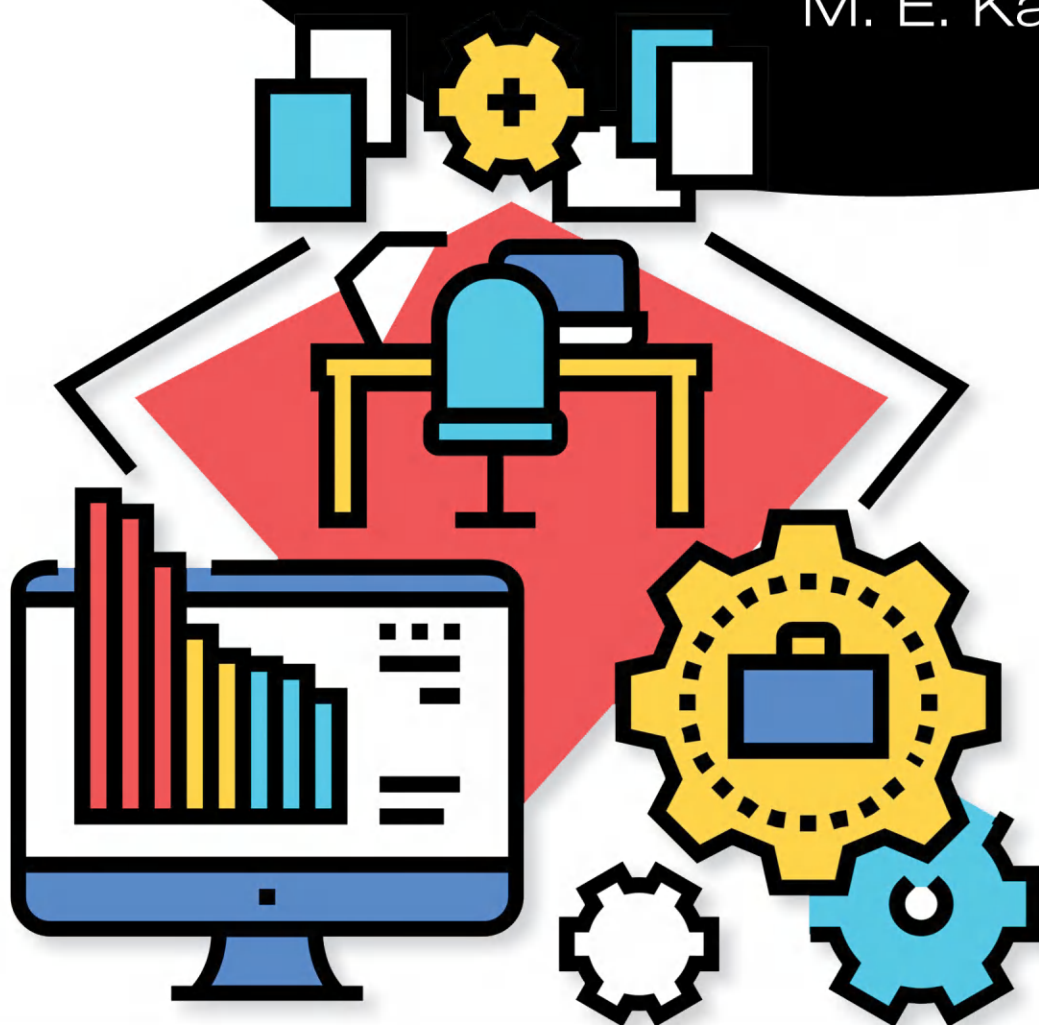


The Expert in the Next Office

Tools for Managing Operations and Security in the Era of Cyberspace

M. E. Kabay



Security, Audit and Leadership Series



CRC Press
Taylor & Francis Group

The Expert in the Next Office

As organizations increasingly depend on electronic information, the lack of systematic training on effective operations and security principles is causing chaos. Stories of data loss, data corruption, fraud, interruptions of service, and poor system design continue to flood our news. This book reviews fundamental concepts and practical recommendations for operations and security managers and staff. The guidelines are based on the author's 40 years of experience in these areas. The text is written in simple English with references for all factual assertions so that readers can explore topics in greater detail.

Security, Audit and Leadership Series

Series Editor: Dan Swanson, Dan Swanson and Associates, Ltd.,

Winnipeg, Manitoba, Canada.

The ***Security, Audit and Leadership Series*** publishes leading-edge books on critical subjects facing security and audit executives as well as business leaders. Key topics addressed include Leadership, Cybersecurity, Security Leadership, Privacy, Strategic Risk Management, Auditing IT, Audit Management and Leadership

Artificial Intelligence Perspective for Smart Cities

Vahap Tecim and Sezer Bozkus Kahyaoglu

Teaching Cybersecurity: A Handbook for Teaching the Cybersecurity Body of Knowledge in a Conventional Classroom

Daniel Shoemaker, Ken Sigler and Tamara Shoemaker

Cognitive Risk

James Bone and Jessie H Lee

Privacy in Practice: Establish and Operationalize a Holistic Data Privacy Program

Alan Tangsss

Leading the Digital Workforce

Jeff Brown

Controlling Privacy and The Use of Data Assets V II: What is the New World Currency – Data or Trust?

Ulf Mattsson

Security Risk Management - The Driving Force for Operational Resilience: The Firefighting Paradox

Jim Seaman and Michael Gioia

Cybersecurity Operations and Fusion Centers: A Comprehensive Guide to SOC and TIC Strategy

Kevin McLaughlin

Seven Deadly Sins of Organizational Culture

L.T. San

The Change Agent: Transforming an Underperforming Internal Audit Department

Hernan Murdock

The Expert in the Next Office: Managing Operations and Security in the Era of Cyberspace

M. E. Kabay

For more information about this series, please visit: <https://www.routledge.com/Internal-Audit-and-IT-Audit/book-series/CRCINTAUDITA>

The Expert in the Next Office

Tools for Managing Operations and Security in the Era of Cyberspace

M. E. Kabay



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First edition published 2025
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© M. E. Kabay

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-1-032-40736-4 (hbk)

ISBN: 978-1-032-40734-0 (pbk)

ISBN: 978-1-003-35453-6 (ebk)

DOI: [10.1201/9781003354536](https://doi.org/10.1201/9781003354536)

Typeset in Times
by KnowledgeWorks Global Ltd.



I dedicate this work to my beloved wife, Dr. Deborah N. Black, light of my life – a source of unfailing encouragement in all my work.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contents

Foreword	xvii
Acknowledgments.....	xix
Author Biography.....	xxi
Introduction.....	xxiii

Chapter 1 The Parkerian Hexad.....	1
Notes.....	2
Works Cited.....	2

Chapter 2 Confidentiality.....	3
Surveillance in the Workplace	4
The Glass-Front Data Center.....	5
LAN Monitors	6
Notes.....	6
Works Cited.....	7

Chapter 3 Control or Possession	8
Facilities Security and Information Assurance.....	8
The Building Location	8
Natural Risks	8
Neighborhood Risks	9
Labeling Facilities	11
Layout	11
Walls.....	12
Doors	12
Windows.....	13
Ceilings and Floors	14
Placing Equipment	14
Electricity	15
UPSs	15
Generators	17
Power Conditioners.....	17
Emergency Lighting	18
Tamper-Proof Enclosures	18
Emergency Power Off	19
Powering Off Every Day?.....	19
Electrical Maintenance.....	19
Electrical Accidents.....	20
Controlling External Factors.....	20
Air Conditioning	20
Controlling Vendor Access to Production Systems.....	21
Stealth-Mode Utilities	22

User Installation of Software.....	24
Unclear on Concept: Anarchy and the Internet.....	25
Unauthorized Vulnerability Scans	26
Responsible Vulnerability Disclosure	28
Responding to Reported Product Flaws	29
Airport-Security Lessons	30
Theft in the Waiting Line	30
Alarms	31
Confidentiality Ignored.....	32
Confidential Garbage.....	32
Reporting Problems.....	33
That Won't Fly.....	33
Flights of Fancy	34
Access and Ego	35
Artificial Stupidity	36
Network Links.....	37
Internet Links Pose Image and Legal Problems	37
Policies for External Links.....	38
Notes.....	40
Works Cited.....	41
 Chapter 4 Data Integrity	45
Criminals Violating Data Integrity as well as Moral Integrity	45
Data Integrity in Voting Machines.....	46
Paper Trails	46
Data Corruption in Medical-Information Systems	49
Quality Control, Data Integrity, and the Silly Season.....	49
The Miracle of the Apostrophes.....	50
The Public-Key Infrastructure Supports Data Integrity and Authenticity	51
Digital Signatures for Authentication.....	52
Overview of PKI.....	53
Certificates.....	54
Issuing, Authenticating and Trusting a Certificate.....	55
Revocation and Expiration of Certificates.....	56
Nonrepudiation and Scalability	57
PKI Services vs. In-House PKIs.....	57
Scumware	58
Scumbody's Changing My Web Page	58
The Ghosts Within	59
Whose Web Page Is It, Anyway?.....	60
Prevention and Removal.....	61
Incompetent Use of Spreadsheets can Cause Production Problems	62
Personal Thoughts on Verification	63
Electronic Truth and Lies	64
Transmission Without Error Correction.....	64
Resources for Verification	66
Disinformation About the COVID-19 Pandemic	66
Social Media and Intermediation	67
Conspiracy Cults	69

Notes.....	70
Works Cited.....	72
 Chapter 5 Authenticity	73
Facial Recognition: Identification and Authentication.....	74
Problems with Passwords	75
Hidden Costs of Passwords	77
Changing Passwords.....	77
Terminating Access.....	78
SPAM	79
The Fake Letter Sticker	80
Kitty Porn	82
Spanish-Bull Fight.....	85
Junk Fax Not What It Seems.....	86
Theft of Identity and the Burden of Proof.....	87
System Defense Against Identity Theft.....	88
Practical Safety Tips to Reduce Identity Theft	88
Prescription for Failure: Side Channels.....	90
CAPTCHA da Flag	91
Easter Eggs and the Trusted Computing Base	92
REDESI Worm Disguised as Security Fix Illustrates Warning Signs of Phishing	94
Hijacking Web Pages.....	96
Misleading Names.....	96
Misleading Links.....	97
Frames Violate Copyright	97
Hidden Text Tricks Users	97
DNS Corruption.....	98
Write-Access Is Dangerous	98
Summary of Countermeasures.....	99
Forged Email Headers and the Law	99
Notes.....	101
Works Cited.....	102
 Chapter 6 Availability	107
Fundamentals of Availability	107
À La Recherche Du Temps Perdu: Eternity in Cyberspace	108
Hardware Obsolescence	108
Software Obsolescence.....	109
Stable URLs and Scholarly References.....	110
The Wayback Machine™	111
Appropriate Guidelines for Data Destruction	111
Lessons from DDoS	114
An Early DDoS Case: “Mafiaboy”	115
Transgressing the Unwritten Law	116
Feedback from Bad Operating Systems	117
Notes.....	118
Works Cited.....	119

Chapter 7	Utility	122
	Organizing and Safeguarding Information on Disk.....	122
	Disks and Partitions	123
	Useful Materials Should be Organized	124
	Finding Files.....	126
	Searching Content.....	126
	Templates.....	127
	The Desktop	128
	System Synchronization.....	129
	System Backups.....	130
	Backups as an Anti-Fraud Tool.....	130
	Notes.....	132
	Works Cited.....	132
 Chapter 8	Threats.....	134
	Threats to Information Security.....	134
	Basic Protection: Safe Hex	134
	Policy, Power, and Position.....	135
	Internal Dangers.....	136
	External Threats	136
	Attractive Targets	137
	Notes.....	138
	Works Cited.....	138
 Chapter 9	Management Principles	140
	Security by Objectives.....	140
	Security by Walking Around	141
	Positive Reinforcement.....	142
	Conflict of Interest.....	142
	Bad Reporting Structure	144
	Quis Custodiet IPSOS Custodies?.....	145
	Employee Preparation for Resisting Social Engineering	146
	Preparing Staff for Social-Engineering Tests	147
	Beware of Unintended Consequences	148
	System Administration.....	148
	Establish Effective Security Configurations	149
	Maintain Software.....	150
	Secure Your Web Transactions.....	150
	Detect Security Breaches	151
	Penetration Testing	152
	Pen-Test Analysis.....	153
	Handling Bad News.....	154
	Use Independent Security Evaluations.....	155
	Working with Consultants.....	155
	Attitudes About Consultants	156
	Goals for Consulting Contracts	157
	Evaluating Potential Consultants.....	157
	Consultants' Code of Ethics	158

Planning for Effective Consultations.....	159
Consulting and Teaching	159
Tools and Techniques for Effective Analysis	160
Real-Time Notes	160
Computer-Aided Consensus	160
Computer-Aided Thematic Analysis	162
Why I Developed CATA	162
Example from Neurological Research Paper	164
Discussion.....	165
Summary	166
Concluding Remarks	166
Notes.....	167
Works Cited.....	168
 Chapter 10 Employment	173
Employment Practices and Policies	173
Evaluating Resumés	174
Selecting Good Candidates for IT.....	175
Avoiding Bad Candidates.....	176
Essential Skills	177
Academic Background	178
Job Experience	179
Administration and Production	179
Probation? Probably Not.....	180
Using College Students as Security Staff.....	180
Poly Want a Hacker?	182
Surfing Brain Waves: fMRI for Lie Detection.....	183
Summary of Hiring Issues	185
Employee Management	185
Redundancy	186
Cross-Training	187
Mandatory Vacations	188
Changes in Behavior and Moods	188
Separation of Duties	190
Job Rotation.....	191
Protecting Privacy	192
Sample Privacy Policy on a Website	193
Controlling Business Partners.....	194
Opting Out.....	195
Who's Actually Requesting My Information?.....	196
The Vulnerable URL.....	197
Termination of Employment	198
Resignations	198
Firings	199
Doing It Wrong.....	200
Cross-Training Again	200
How to Say Goodbye	200
Psychosocial Issues in Firing People.....	201
Style	202
Legal Issues in Firing People	203

Final Comments	205
Notes.....	206
Works Cited.....	207
 Chapter 11 Operations Management in IT	211
Documentation for Less Work	211
The Green Logbook	212
Keep Electronic Records	213
Indexes.....	214
Keeping Time Sheets.....	215
Aleatory ALE	215
Continuity of Operations.....	216
The Capability Matrix	216
Continuity-of-Operations Matrix	218
Stop Information-Hoarding	219
Business Discontinuity	220
VAs and IDSs	221
Deployment.....	222
Response.....	222
Hackback as Revenge	223
False Alarms.....	224
Additional Topics on Operations Security	226
Protecting Public Workstations	226
Locking the Locks.....	227
Data Remanence on Discarded Disk Drives	228
Los Alamos Redux	230
Velocihackers and Tyrannosaurus Superior	233
Notes.....	234
Works Cited.....	235
 Chapter 12 Technical Support.....	238
The Expert in the Next Office	239
TANSTAAFL.....	239
Tools for Tracking TS Incidents	240
Requirements for Problem Solution	241
Problem-Database Analysis.....	241
Solving Technical Problems	242
Set Your Goals.....	242
Get the Global Picture	243
Distinguish Observation from Assumption.....	244
Distinguish Observation from Hearsay	244
Distinguish Observation from Hypothesis	245
Challenge Your Hypothesis	246
Track the Details	247
Don't Prejudge What's Important.....	247
RTFM - Read the ... Fine ... Manual	247
Use Up-to-Date Information	248
Handling Difficult Calls	253

Social Cognition: Forming Judgements About Issues	253
Schemas	253
Weiner's Classification	254
Prejudice	255
Personality Types	255
Driver	256
Analytical	256
Amiable	257
Expressive	257
Incorrect and Dangerous Perceptions	257
Client Support	258
How to Enrage TS Clients	258
Handling Irrate Clients	258
Systematic Responses	259
What if the Problem Still Isn't Solved?	259
Make Users Part of the Tech Support Team	260
Know Your User Community	261
Technical Training	262
The Redundancy Rule	263
Beware the Unbridled Ego	263
Working with Vendor Support	264
Vendor Responsibilities	264
Client Responsibilities	265
Multi-Vendor Problems	265
Teaching and Tech Support	265
Learner Variables	266
Channel Variables	268
Teacher Variables	269
Message Variables	270
Evaluation	271
Notes	271
Works Cited	272
 Chapter 13 Security-Policy Style	 275
The Zen of Network Security?	275
Psycho-Social Factors in INFOSEC Policy	276
Rationality Is Not Enough	277
Writing Down Passwords: Irrationality in Practice	278
Poor Understanding of Risk	279
Practical Psychology	280
Framing Reality	281
Getting Our Security Policies Across	282
Beliefs and Attitudes	282
Changing Attitudes Toward Security	283
Encouraging Initiative	285
Dirty Words: Conformity, Compliance, and Obedience	286
Bringing Security Home	287
Suggestions for Improving Security Education	288

Policy Development.....	289
Phase 1: Preliminary Evaluation	289
Phase 2: Management Sensitization	291
Phase 3: Needs Analysis.....	291
Phase 4: Policies and Procedures	292
Phase 5: Implementation.....	292
Phase 6: Maintenance and Adaptation	293
Writing the Policies	294
Organizing and Presenting the Policies	295
Presenting the Policies	296
Rich Text Format and Proprietary Word-Processor Files	297
Portable Document Format	298
Announcing Changes	298
Notes.....	299
Works Cited.....	299
 Chapter 14 Programming for Security	301
Database Management and Security	303
Chaotic File Structures.....	303
Concurrency and Codd.....	304
The Development of DBMSS.....	305
DBMS Components.....	306
Data Anomalies and Normalization.....	307
Notes.....	308
Works Cited.....	308
 Chapter 15 INFOWAR.....	309
Schwartau's Three Levels of INFOWAR.....	309
Interpersonal Attacks	310
Inter-Corporate Cyberconflicts	310
International INFOWAR.....	311
Russia.....	312
Joint Chiefs: U.S. Behind on INFOWAR Capabilities	313
Industrial Espionage	313
COINTEL Perspective	314
China	315
Blocking IP Traffic from Specific Nations	317
Responding to Chinese Industrial Spam	318
Blocking Porn.....	318
Notes.....	319
Works Cited.....	319
 Chapter 16 Cyberlaw Issues.....	322
Cyberlaw Statutes in the United States	322
European GDPR.....	324
World Wild Web.....	324
Opportunistic Computer Trespass.....	325
Legal Implications of Quality-Assurance Failures	326

Ethical Debate Over Computer Trespass	327
Employee Privacy Rights	329
Privacy at Work	329
Free Speech and Corporate Policy	332
Defamation	333
Trolls	334
Legal Responses to Defamation by Trolls	335
Intellectual Property	336
Copyright	337
Trademarks	337
Patents	340
Legal Dimensions of Spam	342
Picture This: HTML Spam	342
Organizing the Resistance: Fighting Spam Together	343
Not an OPTion	344
Vulnerability Exposure	345
Vulnerability Disclosure Only for a Fee?	346
Managing Vulnerability Disclosure	347
Virus-Writing in Courses	348
Anti-Virus Laws?	349
Viruses Are Not Speech	350
Notes	352
Works Cited	353
 Chapter 17 Protecting Your Organization's Reputation in Cyberspace	 357
Bad Information	357
Violating Netiquette	358
Ill-Advised Email	359
Inappropriate Use of Corporate Identifiers	359
Fraud	360
Spoofing Origination Addresses	361
Chain-Email Pyramid Fraud	362
Frying Pan and Fire: How Not to Handle Spam-Filter	
False Positives	363
Personal Links on a Corporate Website	363
Insulation from External Links	364
Recognizing Hoaxes	365
Using Email Safely and Well	366
Discretion in Email Comments	367
TO and CC + REPLY ALL = Trouble	368
BCC Prevents Email Nuisances	369
Burying Your Email Message	370
Misleading Subject Fields	371
Email Disclaimer Stimulates Expletives	372
Forwarding Corporate Email	373
Emalware	374
Restricting Email to and from the Organization	377
The Keeper of the Lists	378
Mailstorms	379
Delivery Not Guaranteed	380

On Writing.....	381
Summary	382
Notes.....	382
Works Cited.....	383
Index.....	385

Foreword

There are no “perfect solutions”, but almost every previous treatment of computer and network security represents only a small piece of the overall puzzle of trying to achieve trustworthy systems. Such systems inevitably rely on trustworthy hardware, trustworthy operating systems, trustworthy programmers, trustworthy networking, and above all trustworthy administrators. If these systems are built and managed with a comprehensive set of stated requirements (which is seldom the case), those requirements are usually seriously incomplete. Furthermore, the resulting systems are typically built with no deep understanding of realistic threat models. Thus, they fail to honor the second part of the Einstein Principle that “Everything should be made as simple as possible – *but no simpler*.” Failure to adequately consider everything that can possibly go wrong often results in system failures.

This book takes a very significant step forward by considering a wide range of high-level requirements and their impact on overall systems. You might think that 536 pages would be enough to cover everything. For example, needs for trustworthy hardware (which is finally beginning to emerge) and trustworthy people still must be addressed. Nevertheless, Mich Kabay has made considerable inroads to what managers, system developers, and system administrators can do to dramatically improve the existing situation that is becoming increasingly dangerous.

Given the holistic nature of total-system trustworthiness (requiring successful composition and integration that is able to avoid a huge range of risks), the book focuses detailed attention on many of the tricky and psychosocially fundamental practical human issues. That is extremely refreshing, whereas most other authors focus on just a few strictly technical issues or solely operational issues. Remember that the attacker needs to find just a few weak points to exploit, where reality suggests that essentially every topic in this book represents a potential weakness that must be addressed.

Peter G. Neumann

*Chief Scientist, SRI International Computer Science Lab
Moderator of the ACM Risks Forum*



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Acknowledgments

There are so many people I'm grateful to in my career that I cannot reasonably list them here without missing some of them. I am listing a tiny number of those who have been important in my own development in my chosen fields of work.

- Dr Hugh Tyson (z"l) introduced me to applied statistics in 1969 at McGill University and his brilliant teaching made stats a lifelong passion.
- Dr Daphne Trasler (z"l) of McGill University's Human Genetics Sector accepted me in 1970 as a graduate student in teratology and encouraged me in my pursuit of applied statistics in my master's work on homeorhesis in embryonic mice.
- Dr John J. Gilbert was an always-supportive director of my doctoral work at Dartmouth College from 1972 through 1976, hired me as a Teaching & Research Fellow, and allowed me to pursue not only my passion for invertebrate zoology but simultaneously my specialization in applied statistics.
- The *Canadian International Development Agency* (CIDA) sent me to Rwanda from 1976 through 1978 and I will always remember my wonderful colleagues and students and my days teaching statistics and programming at the *Université nationale du Rwanda*.
- Greg Lupfer hired me to write code for statistical functions for his fourth-generation language compiler and allowed me to take advantage of my interest in writing, editing and software quality-assurance by letting me document the system and arrange system testing.
- Larry Luckom was my manager at *Lupfer and Long* and I have always remembered his excellent management style and his sense of humor and intelligence.
- Michel Amesse and Sylvain LeBlanc were my wonderful managers at Hewlett-Packard (Canada) in the early 1980s. They assigned me to socially positive clients such as universities, hospitals, factories, and government agencies (but not tobacco companies).
- Pierre Labelle of Mathema Inc. in Montréal was a brilliant manager who fully supported my efforts for organization of information-technology services operations for 1,000 live terminals from 28 client companies. I learned so much working with him.
- Bob Bales (z"l) and Paul Gates, founders and directors of the National Computer Security Association, allowed me to teach and consult in information security assignments around the world. They encouraged me to write technical articles, some of which are the basis for sections of this textbook.
- David Kennedy of NCSA was one of the colleagues whom I most respect for his intelligence and kindness.
- Security expert and friend Stephen Cobb collaborated on several articles which eventually got incorporated into this collection.
- Security expert Karen Scarfone contributed helpful suggestions for the book.
- Dr Hossein Bidgoli invited me to publish entries in several encyclopedias.
- Alan Freedman, creator of the *Computer Desktop Encyclopedia*, has been a friend and colleague for years and encouraged me to publish this textbook.
- Rebecca Herold, *The Privacy Professor*, has been an inspiration for my desire to share information with a wider public.
- Dean Frank Vanecsek hired me as a professor at Norwich University in 2000 and became a wonderful friend as well as a sterling manager. He gave me the fascinating assignment of creating the undergraduate information-security degree in our department – an enormously stimulating assignment.
- Dean Fred Snow asked me to create and direct the online graduate degree in information security at Norwich, which taught me about online education.

- Dr Peter Stephenson, a world-famous expert in digital forensics, has been my friend and colleague for decades; I particularly enjoyed working with him when he joined me in directing the Master of Science in Information Assurance (MSIA) at Norwich University.
- Director David Blythe took over from Frank Vanecek and was a brilliant director for our department. I am grateful for his continuing friendship.
- Director Matt Bovee of the School of Cybersecurity and Advanced Computing has been one of the best managers I've ever worked with.
- Dean Aron Temkin also became a friend while running the College of Professional Schools so well for us all.
- Dr Peter G. Neumann of SRI International very kindly wrote the Preface; his decades of work in the field have been an inspiration for all of us.
- Former Norwich University student Keeley Eubank provided valuable suggestions for improvement of the manuscript.

Thanks to all of them and my apologies to those I have failed to include!

Author Biography

M. E. Kabay completed high-school math at the age of nine and began tutoring seniors in math and teaching his high-school classmates how to use the slide rule when he was 13 (NOT the ideal way of being popular). He taught himself programming of IBM 1401 computers in assembly language when he was 15 and FORTRAN IV G when he was 16. He completed his BSc in genetics (1970) and his MSc in teratology (1972) at *McGill University*. In 1976, he completed his PhD from *Dartmouth College* in applied statistics and invertebrate zoology and then taught statistics, programming, and biology as a university professor in Canada and overseas.

In 1979, he joined a compiler team for a new fourth-generation programming language (4GL) and relational database management system in the United States and then joined *Hewlett-Packard Canada* in 1980 as an operating-systems and DB-performance specialist, winning the *Systems Engineer of the Year Award* in 1982 and teaching MPE operating system, IMAGE/3000 database and VPLUS/3000 GUI-design courses as well as serving as support engineer to HP's hospital, university and government customers and managing HP's bilingual call center (Phone-In Consulting Service) for Québec and the Maritime provinces.

He served as adjunct faculty in the 1980s in the *University of Ottawa Institute for Government Informatics Professionals*, the *John Abbot College Programmers' Course* and their *Technical Support Program*, and the *McGill University Management Institute* before joining Norwich University in 2001.

He founded his own company, JINBU Corporation, in 1986; much of his consulting work in that firm was database-performance analysis and redesign for optimization. Other assignments included overall operating-system analysis and optimization for improved performance to meet service-level agreements for quality of service; he was assigned 12 such contracts for the *Government of Canada* in 1989. He also completed several contracts in organizational analysis to help improve operations and management processes.

He served as *Director of Education* for the *National Computer Security Association* (later ICSA and then TruSecure) from 1991 to 1999 and taught security courses around the world, including Europe, Asia, and North America. He was the Leader of the *INFOSEC Delegation* to the People's Republic of China in 1993 and provided a 100-page report on his contacts to the *Canadian Security Information Service* (CSIS). He worked with *Adario/AtomicTangerine* where he supported the *International Institute for Information Integrity* (I-4).

He was a member of the committees defining the *Common Body of Knowledge* for the *Certified Information Systems Security Professional* (CISSP) designation in the mid-1990s and earned his CISSP in 1997. The committee used his 1996 textbook, *The NCSA Guide to Enterprise Security* (McGraw-Hill) as one of their resources. His certification as an *Information Systems Security Management Professional* (ISSMP) was granted in 2005. He terminated his use of the CISSP and ISSMP designations in 2021.

Since 1986 (and as of early 2021), he has published over 2,000 articles in operations management and security and served as *Technical Editor* of the 4th (2002), 5th (2009), and 6th (2014) editions of the *Computer Security Handbook* (Wiley). He wrote two security-management columns a week distributed by *Network World* from February 2000 to September 2011 and one per week for *InfoSec Perception* from October 2011 to the end of 2013. His public website has a total of over 2,000 PDF files and over 500 instructional PowerPoint files freely available to anyone for non-commercial use.

He has been an invited lecturer at the *U.S. War College*, the *Pentagon*, and at *NATO Counterintelligence* training in Germany. He was inducted into the *Information Systems Security Association* (ISSA) *Hall of Fame* in December 2004.

From 2002 to 2009, he was the creator and Director of the *Master's Program in Information Assurance* (MSIA) in the *College of Graduate and Continuing Studies* (CGCS) at Norwich

University, Northfield, Vermont where he was also the *Chief Technical Officer* of the CGCS from 2007 to 2009. Returning full time to the *School of Business & Management* in 2009, he was promoted to *Professor of Computer Information Systems* in May 2011 and was appointed *Associate Director* of the *Norwich University Center for Advanced Computing and Digital Forensics* in July 2011.

He retired on 31 December 2020 after teaching at Norwich for 20 years. In May 2021, he was anointed (er, appointed) *Emeritus Professor of Computer Science* in the *School of Cybersecurity, Data Science and Computing, College of Professional Schools, Norwich University*.

Students and everyone else are welcome to *friend* him on *Facebook* for a stream of links to interesting information-security and high-technology articles (mostly from *The Guardian*, *BBC News*, *National Public Radio* and *Washington Post*) with frequent forays into progressive politics, antiracism, LGBTQIA rights, culture, science, cartoons, and puns.

Introduction

Welcome to my anthology of operations and security insights! I wrote and organized the content to help managers and employees improve operations and ensure appropriate security measures to protect information systems (IS). It's also supposed to be fun!

In 50 years of technical writing, I've crystallized my beliefs in how best to communicate with readers interested in learning. To start with, one must determine the target audience. This anthology is aimed primarily at analysts, operations managers, network and security administrators, information-security officers, security consultants, and C-level information executives (e.g., *Chief Information Officers*, or CIOs). However, beginners such as students for whom *information assurance* (IA) is new are warmly welcomed and therefore technical jargon is kept to a minimum; for example, all acronyms are spelled out on first occurrence. Readers unfamiliar with basic concepts will find definitions and articles easily online; more specialized concepts and terms are defined or provided with explicit references. Statements of fact are followed by footnotes to provide additional resources for deeper study. There's also an index for topics; the first entry for each term can serve as the glossary for reminders of terminology because I define acronyms and terms on first use.

The book is organized into chapters:

1. The first substantive section introduces the *Parkerian Hexad*, a fundamental view of the attributes of information that security must protect.
2. Confidentiality refers to restrictions on information sharing.
3. Control discusses limitations on data access and modification.
4. Integrity refers to correctness of data.
5. Authenticity discusses correct attribution and description of data.
6. Availability looks at timely access to information.
7. Utility refers to usability of data for intended purposes.
8. The chapter on threats to information security reviews fundamental issues in the security field.
9. In the section on management principles, I offer managers (new and old) some practical advice on how to work together effectively.
10. The chapter on employment practices and policies reviews ways of hiring, managing, and firing personnel legally and securely.
11. The operations-management section presents insights into getting information-technology work done effectively and efficiently.
12. The next chapter reviews practical issues in the organization and management of technical-support teams.
13. The chapter on security-policy style reviews ways of writing and implementing security policies for effective guidance of personnel.
14. Programming for security includes sections on strengthening programmers' ability to write good code and design DBs for secure access.
15. The information warfare section reviews current issues in cyberconflicts.
16. The cyberlaw review looks at various security issues governed by laws at several levels.
17. The final chapter reviews how organizations should be protecting their reputations by sound management of information and personnel's actions, including professional use of email.

Each chapter ends with the complete list of references cited. There is a detailed index at the end of the book.

Humor can bring to light aspects of any subject that may initially be viewed as plebeian and boring. The collection occasionally features satire and fiction if it makes a point about IA well for the readers. I've included illustrations throughout mostly for fun.

I hope that this book will help improve operations and security. I also hope that readers will enjoy reading it!

1 The Parkerian Hexad

What are the goals of *information assurance* (IA)? We must protect specific attributes of information to the extent required by our system requirements.

The *Classic Triad* of information security refers to attributes of information that have been recognized and named for decades. Now abbreviated *C-I-A*, standing for *confidentiality*, *integrity*, and *availability*, it is still widely used in the field although its precise origin is still a matter of debate and the three elements are not a complete list of what we must protect.¹

The respected scholar Donn B. Parker pointed out decades ago that those three attributes of information are inadequate to describe the goals of information security. The *Parkerian Hexad* adds *control or possession*, *authenticity* and *utility* as essential attributes we must protect.

Parker's introduction to his chapter about the Hexad in the *Computer Security Handbook* summarizes the issues perfectly:

Information security, historically, has been limited by the lack of a comprehensive, complete, and analytically sound framework for analysis and improvement. The persistence of the classic triad of CIA (confidentiality, integrity, availability) is inadequate to describe what security practitioners include and implement when doing their jobs. We need a new information security framework that is complete, correct, and consistent to express, in practical language, the means for information owners to protect their information from any adversaries and vulnerabilities.

The current focus on computer systems security is attributable to the understandable tendency of computer technologists to protect what they know best—the computer and network systems rather than the application of those systems. With a technological hammer in hand, everything looks like a nail. The primary security challenge comes from people misusing or abusing information, and often—but not necessarily—using computers and networks. Yet the individuals who currently dominate the information security folk art are neither criminologists nor computer application specialists.²

In my 40 years of teaching information security in industry and in academia, the Hexad has been an invaluable framework for focusing students' minds on critical aspects of the systems they have to protect. In the following six chapters, I provide examples and discussions of the six fundamental attributes of information that we must protect in the field of information security and as normal requirements for operations management:

- *Confidentiality*: We all know that having someone rifle through our mail without permission is a violation of our privacy. They are violating *confidentiality*.
- *Control*: Those of us who have unlocked mailboxes at home or at work will realize that if someone steals a letter but doesn't open it, they have nonetheless violated security; they have breached our *control* over that information. Similarly, a naïve child who posts nude photos to a friend immediately loses control over what happens to those photos.



FIGURE 1.1 The Parkerian Hexad.

- *Integrity*: When a forger alters the amount on a check we've sent them, they have violated the *integrity* of the document.
- *Authenticity*: When the forger signs our name to a fake check, they're violating the *authenticity* of that signature.
- *Availability*: If a medical practitioner is trying to access information about a new patient arrived in the emergency department, having to wait an hour – or not ever getting the information – is a denial of *availability* and can result in someone's death.
- *Utility*: You arrive at your bank in the United States to discover that your bank account has been converted correctly into Euros – perfectly correctly. In addition, all the documentation for your bank information is now in Egyptian hieroglyphs. For most of us, these conversions, regardless of all the other attributes' being correct, are a violation of *utility*.

NOTES

- 1 Fruhlinger (2020).
- 2 Parker (2014).

WORKS CITED

- Fruhlinger, J. (2020, February 10). *The CIA Triad: Definition, Components and Examples*. Retrieved October 11, 2023 <https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html>
- Parker, D. B. (2014). Toward a New Framework for Information Security. In S. M. Bosworth (Ed.), *Computer Security Handbook* (6th ed., Vol. 1, p. 2000). Hoboken, NJ, USA: Wiley. Retrieved October 11, 2023 <https://www.wiley.com/en-us/Computer+Security+Handbook,+Set,+6th+Edition-p-9781118851746>

2 Confidentiality

Protecting the confidentiality of information involves protecting against unauthorized disclosure of the existence and the details of data. For example, if someone opens a statement from a victim's credit-card company, they have violated confidentiality. If a *counter-intelligence* (COINTEL) agent reveals the mere existence of a file of information about the nefarious activities of a terrorist cell to unauthorized personnel, the error may compromise the operation.

The availability of almost instant publication, distribution, and retrieval of information via the *Internet* (the global internet, sometimes called simply the *Net* and the *World Wide Web* (Web)), which refers to information accessible using *Hypertext Markup Language* (HTML) has transformed communications in the 21st century:



FIGURE 2.1
Confidentiality.

- Information that was once difficult to obtain and that could reach only a few people is now available to billions at the touch of a key.¹
- The wide-scale elimination of professional guardians of accuracy in published materials (editors, publishers) – the process called *disintermediation* – has allowed amateurs and malicious people to spread errors (*misinformation* or MISINFO) and deliberate lies (*disinformation* or DISINFO) freely to many credulous recipients using unregulated channels such as social media and mass distributions of email containing lies.²
- Digital photography editing (sometimes called Photoshopping because of using a well-known program) allows modification of any image to make the most innocent picture look like something horrible if bad people decide to smear someone.³
- Electronic commerce (ecomm) using credit cards and transactions through the Web have allowed criminals to make identity theft one of the fastest growing crimes in the world, with millions of victims losing billions of dollars a year and finding their credit records seriously damaged.⁴
- Computer viruses and worms sometimes spread confidential documents from infected computers to other victims, inadvertently revealing company secrets or embarrassing personal information.⁵
- Special programs called spyware secretly send information about Web usage, email, or other computer information to vendors or outright criminals who track activity of unsuspecting victims.⁶
- Criminal hackers and state and non-state actors break into poorly secured organizations and steal or modify information, including business, medical and operations records, with impunity. Criminal gangs have also increasingly been using ransomware to encrypt victims' data; they demand payment for the decryption key.⁷
- Criminal hackers even break into ordinary people's computers, although they mostly use them as platforms for spreading malware, denial of service (DoS), distributed DoS (DDoS) attacks,⁸ or for sending spam.
- Spam or spam (not SPAM® in uppercase, which is the registered trademark for food products made by Hormel Foods Corporation⁹) is the name applied to unsolicited commercial email, a plague that is clogging the Internet with fraudulent and pornographic appeals for money from gullible and naïve victims. Spam is also used for phishing – email offering links to dangerous sites that often install malware on gullible victims' computers or lead to contacts with scammers).¹⁰

- Chain letters¹¹ and schemes (aka pyramid frauds)¹² play on victims' greed and credulity to extract millions of dollars for help in obviously illegal or impossible plans, many of which involve revealing confidential details of bank accounts to total strangers who have announced that they are crooks. Ponzi schemes work by using received money to pay off earlier "investors" until enough money has accumulated in the criminals' accounts that they can stop the scam and steal the proceeds before disappearing.

SURVEILLANCE IN THE WORKPLACE

One of the many interesting topics of discussion at the *9th Annual Meeting of the European Institute for Computer Anti-virus Research (EICAR)* in March 2000 in Brussels was privacy. In the panel discussion on privacy policies in the European Community, we discussed workplace monitoring.

A key question in any such discussion is the definition of privacy. Most experts see privacy as the result of awareness and control by the data subject. According to the stringent new rules of the *European Community Privacy Directive (ECPD)*,¹³ the subject should know and be able to control what information (s)he is revealing to whom and for what purposes. This principle implies that transmission of data to authorized recipients should be confidential so that unauthorized personnel or organizations do not have access to the information. In addition, once the data are collected and manipulated by an agency, the data subject must have the right to see what has been collected, to correct errors, to determine the ways in which the data may be applied or with whom they may be shared and may remove permission for data storage and distribution.

Although there is relatively little hard evidence based on systematic, scientific investigation of attitudes and beliefs on this question, several speakers on the panel and in the audience thought that the United States and Europe seemed to differ in fundamental attitudes toward privacy.

- People in the United States were more likely to be surprised by the ECPD's requirements than Europeans.
 - U.S. residents seemed to take it for granted that it's acceptable to opt-in by default and opt-out explicitly from data collection; in contrast, the speakers believed, Europeans seem to start from the premise that privacy should be the baseline, with explicit opt-in required to allow data collection and sharing.
 - Europeans had more faith in the privacy protections afforded by government regulations; in contrast, U.S. residents seem to be more skeptical of all government initiatives, including privacy protection.
- In certain European countries such as Germany, employees are guaranteed baseline privacy protection with the workplace unless there are explicit civil contracts with trade unions to override these protections.
 - For example, it is a given that an employee is entitled to privacy of a locker or of a drawer in their desk.
 - Similarly, only if an employee willingly surrenders privacy rights would it be acceptable to monitor corporate email and files on disk.

In general, the panel and audience agreed that there are some very serious consequences of failing to make the ownership of email and files clear to employees when they come on board. The worst situation arises if employees are granted the right to control personal information residing on corporate systems; under the ECPD, such employees would have the right to order the destruction of their "private" email and files on disk and on backup media. The complexity of purging backups



FIGURE 2.2

Surveillance at work.

would be enough to give any system administrator nightmares; the quagmire of deciding which files and messages are legitimately defined as corporate vs private could occasion tremendous costs and quite likely lead to litigation.

Now, as I understand the situation, there is no doubt that organizations should be absolutely clear when hiring staff so everyone understands that all data created by employees of an organization must be the property of that organization and that there is absolutely no right of privacy for such material.

In addition, lawyers tell me that a single signature at time of hiring is insufficient protection for the corporation. The privacy policy must be well known and seen to be enforced.

Warnings at logon may not be sufficient in Europe; I was told in discussions at the EICAR Conference that some EC judges have ruled that logon banners are known to be widely dismissed by employees and therefore cannot be adduced as sufficient evidence of informed consent to full disclosure of email and files on the corporate system.

More problematic is materials that are received from outside the organization. As far as I understand the situation, possession of someone else's copyrighted material cannot in any way extinguish the copyright holder's rights. What this means for email sent to an employee by an outsider will probably have to be settled in the courts.

In 2021, however, more recent studies suggest that U.S. attitudes toward privacy may have shifted toward the European views.¹⁴

THE GLASS-FRONT DATA CENTER

A senior security consultant who preferred not to be identified sent me the following case in response to previous articles I had published.

The new data center cost over \$30 million and was thought to be "state of the art." However, the risk assessment was not done until construction was well underway. The front wall was made of glass, which provided a clear view into the computer room. The access-control system did not work for six months after the center was online, due to problems with a start-up contractor. Two unarmed guards monitored the front door and the computer-room door. They were also supposed to monitor the 30 plus cameras on the perimeter, none with motion sensors, while doing visitor control. A knoll 100 yards for the center provided a clear view of the air conditioners on the roof. Uncontrolled parking was available next to the front glass wall. The *Public Affairs* staff produced a video describing the construction of the center, which was available to anyone who requested it. Pictures from the video were available on its web-site along with a floor plan and network diagrams for many months after the center was completed. The center processes important information for several organizations.

Security by obscurity is not by itself a sound basis for protection, but publishing building details that can help an intruder isn't great either.

Lessons learned:

- Plan for security as you plan your building or data center.
- Perform your risk assessment early in the process when changes can be made.
- Revise the risk assessment as the building is built.
- Don't use materials like glass in critical areas.
- Don't use startup contractors for critical services.
- Don't expect guards to do so many different functions that they don't do any well.
- Do control parking areas.
- Use vehicle barriers (e.g., bollards) to prevent vehicles from accidentally or deliberately crashing into buildings.



FIGURE 2.3 Data center.

- Control the information posted on the corporate website.
- Don't produce videos about critical facilities for public distribution.

LAN MONITORS

Remember Superman, the comic-book hero with X-ray vision? He could look through concrete, but he never looked through people's clothing.

Local area networks (LANs) are threatened by the electronic equivalent of X-ray vision and users of network-monitor programs are looking beyond our electronic underwear. Unencrypted LAN communications are open to inspection by anyone using off-the-shelf software.

Hardware LAN monitors are special-purpose computers that are brought into a network environment by specialists. Anyone can tell that something special is going on when such equipment is connected to the LAN. In contrast, network-monitoring software is invisible because it doesn't alter any data.

Off-the-shelf monitoring programs are difficult or even impossible to detect electronically while they're operating. It's also hard to detect the monitor programs visually. For example, a dishonest employee can easily hide his or her use of a monitor by installing a screen saver that blanks out the tell-tale displays at the touch of keys (e.g., *Windows-L*) or simply switching to another window to appear to be working innocently.

An unauthorized user can decode packets being sent from someone else's workstation to any other node. For example, one could decode the traffic of a network manager using the LAN for connection to a minicomputer or mainframe. The packets could include secure information such as the passwords used for logon/login, and file lockwords. Even worse, the traffic might include the encryption keys used to protect confidential files on servers and hosts or the decrypted contents of such files.

Network monitor software is read-only. It does not interfere in any way with the data stream. There is currently no way for a network supervisor to tell that someone is decoding packets.

X-ray vision indeed.

One solution is to encrypt all the data moving through LAN. Technology exists today to encrypt everything moving across LAN cables or wireless networks. Monitor software can still measure traffic across the network. However, the data in the packets are secure against inspection.

Another solution: Agree on a way for LAN-monitor software to announce itself. There would have to be agreement among manufacturers of LAN *operating systems* (OS) and of LAN-monitor programs to ensure that such software emits standard packets.

The industry could also agree on a standard that enables network managers to forbid unauthorized use of such software on their LANs. The LAN operating systems would then automatically enforce such restrictions by sending appropriate signals to monitor programs that comply with the new security standards.

True, rogue software could still decode unencrypted packets. However, such non-standard software would have poor sales. Ownership and use of such programs on a network would be *prima facie* evidence of dishonest intentions.

I am confident that most of the authors of LAN-monitor software are responsible professionals. Unfortunately, despite their best intentions, they have loosed a monster into the LANs of the world. What happened? This error results from the low importance assigned to information security. Everyone writing software and managing software projects should invest in adequate training in security.

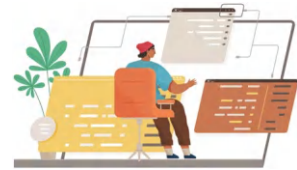


FIGURE 2.4
LAN monitoring.

NOTES

- 1 Johnson (2021).
- 2 Parks (2021).

- 3 Queensland University of Technology (2021).
- 4 Insurance Information Institute (2021).
- 5 NIST (2021).
- 6 Leal (2021).
- 7 Waldman (2021).
- 8 Coble (2021).
- 9 Hormel Corporation (2021).
- 10 Kulikova (2021).
- 11 Gressin (2020).
- 12 U.S. Federal Trade Commission (2021).
- 13 European Commission (2021).
- 14 Future of Privacy Forum (2020).

WORKS CITED

- Callahan, G. (2020, August 10). *Follow These 7 Video Conferencing Security Best Practices*. Retrieved July 7, 2021 <https://www.rev.com/blog/follow-these-7-video-conferencing-security-best-practices>
- Coble, S. (2021, May 18). *Q1 2021 Sees 2.9 Million DDoS Attacks Launched*. Retrieved June 29, 2021 <https://www.infosecurity-magazine.com/news/q1-2021-sees-millions-ddos-attacks/>
- European Commission. (2021, June 4). *Data protection in the EU*. Retrieved June 29, 2021 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- Future of Privacy Forum. (2020, December 13). *Exploring Consumer Attitudes About Privacy*. Retrieved June 29, 2021, from Future of Privacy Forum: <https://fpf.org/blog/exploring-consumer-attitudes-about-privacy/>
- Gressin, S. (2020, May 21). *This “game” is a chain letter scam*. Retrieved June 29, 2021, from US Federal Trade Commission Consumer Advice: <https://www.consumer.ftc.gov/blog/2020/05/game-chain-letter-scam>
- Hormel Corporation. (2021). *What Is SPAM Brand?* Retrieved June 29, 2021 <https://www.spam.com/what-is-spam-brand>
- Insurance Information Institute. (2021, n/a n/a). *Facts + Statistics: Identity Theft and Cybercrime*. Retrieved June 28, 2021, from iii.org: <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
- Johnson, J. (2021, April 4). *Global Digital Population as of January 2021*. Retrieved June 28, 2021, from Statista: <https://www.statista.com/statistics/617136/digital-population-worldwide/>
- Kulikova, T. (2021, May 3). *Spam and phishing in Q1 2021*. Retrieved June 29, 2021 from Securelist by Kaspersky: <https://securelist.com/spam-and-phishing-in-q1-2021/102018/>
- Leal, L. (2021, March 2021). *Trojan Spyware and BEC Attacks*. Retrieved June 28, 2021, from Security Boulevard: <https://securityboulevard.com/2021/03/trojan-spyware-and-bec-attacks/>
- Microsoft. (2021, n/a n/a). *Skype*. Retrieved June 29, 2021, from Skype: <https://www.skype.com/en/>
- NIST. (2021, n/a n/a). *Glossary: Malware*. Retrieved June 28, 2021, from National Institutes of Science and Technology – Information Technology Laboratory – Computer Security Resource Center: <https://csrc.nist.gov/glossary/term/malware>
- Parks, M. (2021, March 5). *Trump Is No Longer Tweeting, But Online Disinformation Isn’t Going Away*. Retrieved June 28, 2021, from NPR: <https://www.npr.org/2021/03/05/971767967/trump-is-no-longer-tweeting-but-online-disinformation-isnt-going-away>
- Queensland University of Technology. (2021, June 28). *Seeing Is No Longer Believing: The Manipulation of Online Images*. Retrieved June 28, 2021, from SciTechDaily: <https://scitechdaily.com/seeing-is-no-longer-believing-the-manipulation-of-online-images/>
- U.S. Federal Trade Commission. (2021, May n/a). *Multi-Level Marketing Businesses and Pyramid Schemes*. Retrieved June 29, 2021, from U.S. Federal Trade Commission Consumer Information: <https://www.consumer.ftc.gov/articles/multi-level-marketing-businesses-and-pyramid-schemes>
- Waldman, A. (2021, January 5). *10 of the Biggest Cyber Attacks of 2020*. Retrieved June 28, 2021, from TechTarget: <https://searchsecurity.techtarget.com/news/252494362/10-of-the-biggest-cyber-attacks>

3 Control or Possession

When someone transmits information to anyone else, the recipient then has possession over that information and control over what will happen to it. For example, if a young person sends a photograph of themselves to a friend, the subject no longer has control over its distribution – which is what has happened too often when the recipients turn nasty and use photographs as weapons.¹ Another example of control violations occurs if someone takes a sealed envelope out of a mailbox (a federal crime in the United States²) but does not open it; they have not *yet* violated confidentiality, but they have already violated *control* because it is now their choice whether or when to violate that confidentiality.

This chapter illustrates key issues involving control:

- Facilities security
- Electricity
- Controlling external factors
- Airport security
- Thoughts on security problems caused by inflated egos
- Early experiences with artificial stupidity
- Network links as a threat

FACILITIES SECURITY AND INFORMATION ASSURANCE

A good example of control issues is physical security, which involves aspects of the environment in which we work and where we place network components.^{3,4}

THE BUILDING LOCATION

If you're planning to build a new computer center or relocate your existing equipment to an existing building, you have an opportunity to make your building work for you instead of against you. By picking the right combination of location, structure and layout, you can decrease your vulnerability while increasing the usability and maintainability of your equipment.

We'll start with cases where we have a choice of placement for our facilities.

NATURAL RISKS

If you're starting from basics, you can consider the geographical location of your new site. Study long-term weather patterns, including frequency of heavy winds (e.g., tornadoes, hurricanes, and monsoons), snow, and lightning. Unless you're devoted to a life of great excitement, the likelihood of earthquakes should play a role when siting a major data center.



FIGURE 3.1 Control.



FIGURE 3.2 Office building.



FIGURE 3.3 Natural risks.

NEIGHBORHOOD RISKS

If it weren't for personal experience, I'd be embarrassed to remind you not to situate your data center in a dangerous place. Sounds like motherhood-and-apple-pie. But consider the following case from my consulting work in the 1980s:

One fine spring day, as I drove to a data center where

I was due to start a security audit, I noticed a field of enormous storage tanks on my left. It looked like a science fiction movie: row upon row of spheres and cylinders holding millions of liters of gasoline, diesel fuel and home heating oil. I was startled to find, upon following my directions, that the data center was directly across the road, no more than 200 meters away.

As I parked my car, I noticed a freight railroad crossing diagonally immediately behind the building. The tracks were still bright (i.e., not rusted), so the railway was still in active use.



Finally, just as I was about to enter the building, I heard a passenger jet screaming across the sky just above, flaps out, heading for a landing at the regional airport.

Now *that* was a poorly situated data center.

FIGURE 3.6

Air traffic.

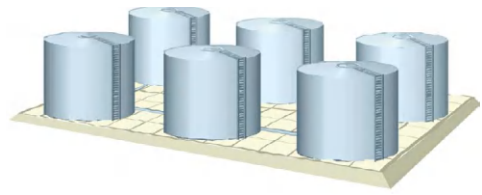


FIGURE 3.4 Oil storage.



FIGURE 3.5

Railway.

Before choosing the building which will hold your corporate offices or data center, examine the neighborhood. Avoid

- Flight paths for the local airport
- Nearby chemical or explosives plants
- Neighboring elevated highways
- Railway freight lines.

Look out for

- Mine shafts
- Toxic waste dumps
- Sources of dust and smoke (e.g., industrial incinerators)
- New or planned building activity (the vibration of pile drivers will harm your systems).

How easy would it be to reach the site in an emergency?

- Is there redundant road access?
- Are there several sources of help to fight fires?
- Is there police support and emergency rescue within easy reach?

Examine the socio-economic profile of the proposed location.

- Are there poor areas around the site?
- What's the crime rate?
- Is it improving or declining?

A participant in one of my courses reported that their corporation decided to move their headquarters one day after the new *Chief Executive Officer* (CEO) took over.

Someone had shot at him in the parking lot on his first day at work.

On the other hand, some corporations and other organizations explicitly include contribution to their community as a goal; for example, *AtomicTangerine* training sessions (“boot camps”) focused on helping selected non-profit organizations to upgrade their websites.⁵ Perhaps instead of running away from a troubled area, we can help improve the socioeconomic conditions there by providing work, support for schools, and volunteer efforts to support other social action.

Whatever you decide, be sure to re-evaluate your physical location periodically and take appropriate action to protect your corporate resources.

In the March 1993 session (Atlanta, GA) of the *Information Systems Security* course I taught as *Director of Education* for the *National Computer Security Association* (NCSA), a participant reported that a major company installed millions of dollars of computer equipment, electrical power conditioners and air conditioners on the 11th floor of an office tower. One Monday morning, the staff arrived to discover no 11th floor – and no 10th floor – and no 9th floor. They had collapsed into rubble. The company had neglected to consult a structural engineer before loading the building with all that equipment. Luckily, no one was hurt in the collapse; however, damages ran over \$100 million.

Access to the computer center should allow easy installation of equipment yet protect that equipment and its operators against physical assault. The ground floor seems too easy to attack; underground is susceptible to flooding. In the 1988 movie “*Die Hard*,” we see a Hollywood conception of a computer center: near the top of an office tower and entirely surrounded by glass.⁶ Since some computer equipment (or support equipment such as large-scale air-conditioning units) is larger than freight elevators can handle, the units have to be lifted into place using building cranes. The higher the computer center, the more expensive the crane. In case of fire, there may be a longer lead time for staff to shut off the equipment and make their way to safety if they’re high up in a sky-scraper.

The second floor seems like a good compromise.

Place the network center or computer room far from hazardous areas. One story circulating in the security field tells of a security auditor in the U.K. who wondered about the vibrations he felt in his feet every now and then. “Oh that?” responded the data-center manager, “That’s just the lorries with the petrol.” The computer room was directly over the passageway through which trucks carrying fuel oil regularly rumbled. Not a low-risk situation.

High security vaults are required by law to have no external walls. That is, they are completely inside their building with corridors completely surrounding them. This design makes it much more difficult to punch holes into the data center without having anyone notice. And in case you doubt that a frontal assault on a computer center is likely, some *automatic-teller machines* (ATMs) have been removed *holus bolus* by thieves operating backhoes and forklifts (it does make one wonder about why no one thought it odd to see a forklift or a tow-truck trundling along with an ATM in the middle of the night).⁷

In the Spring of 1995, one of the participants in an online *Computer Crime and Countermeasures* course told us about how a series of smash-and-grab attacks had been made on a local company known to have installed large numbers of new workstations. The criminals simply crashed through the wall and made off with the equipment in the minutes before the police could respond to building alarms. Maddeningly, the criminals apparently watched and waited until the victims had replaced all the equipment and did it again! They were dissuaded from further repetitions by having a 24 hour guard mounted on the site.

Another dreadful case of foolish placement for computing equipment was in the basement of a building in the *Vermont State Offices Complex* in Waterbury. On August 28, 2011, Tropical Storm Irene raised the water level of the nearby Winooski River above the banks, flooding the entire campus.⁸



FIGURE 3.7
Swamped
computer center.

When I visited the site a few weeks after the storm, the pile of dead computer equipment of all sorts in the middle of a lawn was over 20 feet high. In the building where the data center had been placed in the basement, the water lines on the walls of the *first floor* (not the basement!) showed that the flood had hit about five feet above ground level. Building a new center for the State offices cost an estimated \$125M.⁹

LABELING FACILITIES

One of the perpetual debates in INFOSEC is the value (or worthlessness) of what practitioners call *security through obscurity*. The question is whether one can improve security by hiding information. For example, does it help to hide the details of an encryption product so that no one can easily find the algorithm? *Kerckhoff's Principle* (sometimes spelled *Kerckhoff*) states that the strength of a cryptographic algorithm must not depend on its secrecy.¹⁰ A corollary of this principle is that the validity of an implementation of a strong cryptographic algorithm can best be evaluated when the details of that implementation are accessible. In other words, distrust proprietary implementations of cryptography – there may be mistakes concealed in the object code that would leap out at (and be fixed) if the source code were made available for inspection.

Well, it's a long way from cryptography to building layout and physical security, but there is a connection. Some aspects of the layout may fruitfully be concealed to make the job of the attacker harder; however, some of the information about buildings ought to be available to improve emergency response.

Specifically, once you've built the computer room, be sure the local fire department knows exactly where it is. Keep your plans, including layout, up to date and coordinate with the fire marshals in your municipality.

However, there is no reason to mark the computer room with special neon flashers that read, "THIS WAY TO MILLIONS OF DOLLARS OF VULNERABLE EQUIPMENT." When I led a delegation of Japanese data-center managers to visit the headquarters of EDS Inc. in Dallas in 1991, I was much struck by the anonymity of the equipment rooms. We walked through immense corridors with identical, boring metal doors, each marked with a numbering scheme. They all looked as if they could be broom closets. Then we'd open one up and find vast gleaming, sterile chambers of white tiles with and filled with huge *central processing units* (CPUs) – silent titans standing in rows with blinking red and green eyes. (Today, I suppose, the same processing power would fit onto someone's desk as a notepad computer.) The theory was that anyone who needed to know where the computers were knew where they were; why help anyone else locate such an inviting target?

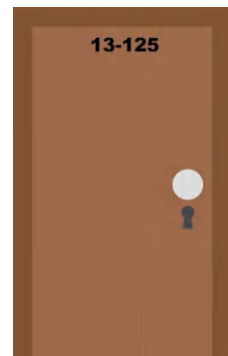


FIGURE 3.8
Numbered door.

LAYOUT

Within your data center, try to put separate functions in different compartments. For example, keep printers away from consoles, disk drives, processors, patch panels and server racks: the paper is a fire hazard and the paper dust gets into your air filters.

To ensure that you don't wipe out your backups if there is a disaster in your *network-operations center* (NOC) or *data center* (DC), put tape vaults and data safes far away from your disk drives. However, you can reasonably have a local fire-proof safe or vault for the convenience of operators as long as the media stored there are not your latest backups.

Put your access-control equipment into a separate, high-security area, not with the rest of the computers. Security measures should reflect the potential *exposure* (consequences) of compromise;



FIGURE 3.9 Layout.

since access to the security equipment compromises everything else, it makes sense to guard it even more strongly than other components of your networks and systems.

Position your phone switches away from the computer room so that a single attack cannot put your entire operation into jeopardy. This suggestion follows the principle of reducing the number of single points of failure – more humbly known as not putting all our eggs in one basket.

The lower the traffic through a secure perimeter, the lower the risk of failure. Accordingly, try to keep your operations personnel comfortable inside the secure areas surrounding your equipment as much as possible; for example, include rest rooms, eating areas and office space for the staff who run your *production systems* (whatever is essential for mission-critical functions) within a tightly controlled space inside the perimeter. This recommendation does not mean that you should forbid staff from leaving the secured area on their off time – that’s their perfect right. However, the availability of such facilities will be convenient for some of the staff some of the time and will contribute to lowering the risk of intrusion and increase the speed of response to emergencies in the NOC or DC.

WALLS

When I was in Africa in 1976-1978 teaching statistics and programming at the *Université nationale du Rwanda*¹¹ in Butare, Rwanda for the *Canadian International Development Agency* (CIDA) – now part of *Global Affairs Canada*¹² – I remember thieves used to enter the houses of the rich *abazungu* (foreigners) by ripping the doors from the walls using pickup trucks and chains. This experience greatly influenced my view of the importance of walls, doors and windows for security: they are weak spots in the perimeter.

When you build an enclosure for expensive and critical equipment, be sure they’re substantial walls, not mere drywall partitions. Reinforced concrete that runs from slab to slab is best.

Check your plans and forbid any closets in the walls of your NOC or DC; they are weak spots and also provide concealment should anyone decide to punch through the wall using drills or explosives.

Finally, if your security needs are usually high (or if you have been watching too many action movies), talk to your architect about the design of the outermost walls of your building. Avoid *chases* (decorative indentations on the sides) and other features such as rusticated stone that could make it easier for assailants to use mountain climbing techniques to climb your building.



FIGURE 3.10
Weak walls.

DOORS

Have as few doors as possible. You must know and obey all the safety regulations which mandate the number of exits you must include for protection of human life. Your architect will know what the law requires. However, only one door should be used for entry and normal exit. All the others should be used as emergency exits only. All doors should be equipped with crash bars and alarms and decorated accordingly. You can even buy or make signs that read, “DOOR IS ALARMED” (which always make me want to pat the door and reassure it that everything will be OK).

Choose heat-resistant doors (solid metal or thick metal with a structurally sound core) and avoid any glass if at all possible. If safety regulations require glass panels to prevent smashed noses, insist on multiply laminated bullet-proof, shatterproof small panels. Glass is a weak point anywhere in the secured area.

Installing a door that would make your local bank proud will be pointless if the frame is so weak that it – and the door – can be pried out of the wall with a crowbar. Door frames should be anchored



FIGURE 3.11 Alarmed door.

solidly in the wall; if possible, bonded to the structural members of the wall. Door hinges should be on the inside of the secure area so they can't be dismantled. Choose hinge pins that are welded into place – not the ones that can be unscrewed and removed by anyone with a home tool kit.

Protect door locks with *astragals* (a lovely word meaning the edge-plates that prevent nasty folk from inserting credit cards, screwdrivers and chisels into the latch and forcing the door open). I have seen many secure sites which use astragals which extend from top to bottom of the door to provide maximum protection.

Don't use motion or simple proximity sensors to unlock or open doors into secure areas. Sliding doors controlled by such sensors – like those used in many public buildings – can generally be opened from the outside simply by pushing a sheet of paper through the rubber gaskets and waving it about.

WINDOWS

Don't put windows in your network and data centers. I've already pointed out that there should be no outer walls in your computer room, let alone windows. Windows are physically weak; their frames are weak; and they let too many people see how you've laid out your equipment – including your security equipment.

I recall one manufacturing site where I stopped next to the floor-to-ceiling windows around the computer console room and stared at the five-meter banner on the wall. It had huge numbers printed on it. I asked, "That's not the main modem number, is it?" Yup. So much for dial-in security.

Unfortunately, many executives who worked with computers in the 1960s and 1970s or who base their standards on Hollywood movies still think that "vision panels" make their data center look more impressive. If you are faced with this retrograde attitude, try a graduated approach to getting rid of these vulnerable spots in your defenses. Offer the decision makers a choice between, say, concrete, brick, or bullet-proof safety glass. Alternatively, you can strap the executives down and force them to watch endless loops of Bruce Willis surviving the destruction of the Glass House in the movie "Die Hard."

If you cannot get approval to remove the windows in your computer room, install vertical blinds and keep them closed all the time except when there are important official visitors pressing their noses to the glass. Install security glazing (shatterproof metal-reinforced glass), and perhaps gratings securely attached to the walls. Install breakage sensors and connect them to the main building alarm systems. Aim motion sensors and closed-circuit television cameras at the windows. Move equipment whose presence should be secret away from the windows. Install a few dummy security cameras and motion sensors just to keep spies and intruders guessing.

There are a couple of other reasons why high-security sites do not permit windows in their NOCs and DCs. An obvious point is that external windows offer opportunities for snipers to attack individuals. More subtly, windows vibrate as people talk; using laser interferometers, it is possible to measure those vibrations and reconstitute the sound waves that caused the vibrations.¹³ Thus an exterior window provides an easy way for industrial or other spies to eavesdrop on conversations from an observation post far away in another building. However, don't try to persuade your top officials to give up their corner offices – some advice is just too unpleasant to bother presenting to upper management when the risks are low. I think that such advice might get you sent to the staff psychiatrist in most organizations.

What might work is to suggest that a window-rich office is perhaps not the best place to discuss top-secret strategic plans with catastrophic consequences of unexpected disclosure. People talking about make-or-break information would do well to do so in sealed rooms with no windows. The key is to be reasonable and not to apply security rules unthinkingly.

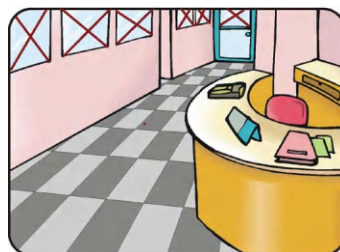


FIGURE 3.12 No windows for data centers.

CEILINGS AND FLOORS

Practically all offices these days have drop ceilings; i.e., acoustic tiles are suspended from the actual ceiling. This design provides for a place where electrical and communications wiring can be laid out of sight. Be sure the design allows for no crawl spaces around the wall above a drop ceiling or below a raised floor. This crawl space must not extend without interruption into the data center. Within the data center, the drop ceiling should include smoke, heat and water sensors. This is especially important when there are other floors above the NOC or DC and there is a possibility of water leakage.



FIGURE 3.13 Ceilings and floors.

The issue of walls that don't go slab-to-slab always reminds me of an incident in the early 1980s when I was a systems engineer for *Hewlett-Packard* (Canada) (HP) in the Kirkland, Québec office. One night after everyone had gone home, I was preparing for a course I had to present the next morning and discovered that the door to the photocopy room was locked. However, the wall for that room extended only about eight feet, leaving a two-foot gap between the top of the wall and the drop ceiling. I cheerfully used my rock-climbing habits to scale the wall and get my copies made. My manager was not pleased.

Most information-processing centers have raised floors because of all the cabling and power cords required for processing equipment and peripherals. The floor tiles are laid on a framework about 18 inches (~50 cm) off the actual floor. These tiles must be fire-resistant, easy to keep clean, and strong enough for the loads that will be placed on them. For access to the under-floor area, the tiles are raised using suction cups. Perforated tiles are part of the air-conditioning and fire-suppression systems and are raised using hooks.

The under-floor area must be kept scrupulously clean. Gas-based fire-suppression systems discharge high-pressure gas through the under-floor. If that area is dusty, the entire computer room will be filled with a cloud of dirt when the gas discharges.

In some cases, operators have used the under-floor as a storage area, sometimes for things that don't belong in the computer room at all (e.g., in one case I personally noted, bottles of soda pop). Such foreign objects may interfere with the air-conditioning system and cause access problems in emergencies.

PLACING EQUIPMENT

In recent years, computer equipment has become increasingly tolerant of environmental conditions. Midrange and many mainframe computers are now air-cooled, survive temperatures from cold to hot, and run on regular 110 V current. Nevertheless, some people abuse their systems. In the early 1980s on a visit to a client, while I was hanging my coat in a hall closet, I noticed blinking green and red lights down among the boots and galoshes. I moved some heavy winter coats out of the way and discovered a network server. Startled, I asked my host what it was doing in an unprotected hall closet. It seems that they ran out of room in the computer center and the server was installed in the hallway. "It doesn't need special conditions," he chirped. "No," I said, "but its on/off switch is open to anyone who wants to try bringing the network down, and I doubt that the engineers planned on seeing their design spattered with mud, water and salt."

A related problem with poor wiring practices is that many users and even some NOC managers don't label their cables. The consequences are most serious when people have to

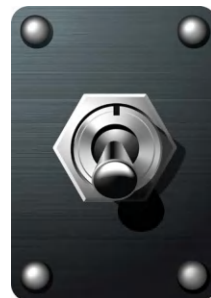


FIGURE 3.14
On-off switch.

move their equipment; either they spend precious time under pressure trying to label their gear or they just unplug everything and hope they get everything right when they reassemble their systems.

Sometimes people plug their computer systems into a power bar in their neighbor's cubicle without informing anyone. When the neighbor innocently cuts the power on their own system by hitting the main switch on the power bar, the electricity-borrower has a power failure too (I've seen it happen). Another problem occurs when people run out of sockets in their cubicles and decide to lay an extension cord out into a hallway to tap into a handy socket there – and naturally, without bothering to label the wires with something like “DO NOT UNPLUG THIS – POWER FOR COMPUTER.” These arrangements inevitably result in what ought to be a predictable loss of power when a building cleaner innocently unplugs the unlabeled power cable to power their floor polisher (happened in an office where I worked). In many smaller organizations, I have noted with dismay that electrical power-cord extensions are looped helter-skelter around the bottoms of desks and partitions. Aside from the problem of tripping over these cords and crashing wildly about one's office, these folks run the risk of unplugging their own computers, causing an occurrence of the notorious *power-cord-out-of-the-socket* “virus” that occasionally amuses technical support staff.

Some common-sense recommendations:

- Don't subject your valuable, sensitive and critical equipment to inappropriate environmental stresses.
- Organize your equipment cables so that they don't tangle each other or passers-by.
- Label your cables clearly using color coded tape or printed labels.
- If you must use electrical outlets outside your immediate control, lock the plugs into place if possible or at least label them clearly so that others don't inadvertently cut power to your systems.

ELECTRICITY

No electricity, no computing.¹⁴ Given that simple principle, it makes sense to have good electrical power and a mechanism for working without external power – at least, long enough to allow a *graceful shutdown* (in contrast with losing everything that was in RAM when the power stopped).



FIGURE 3.15

Electric power.

UPSs

Power outages cause down time, but the more serious threat is that power interruptions during a critical phase of posting data to disk will cause data corruption. If a disk drive goes down while data are being written into a file, one or more records can be damaged. Parity checks or *cyclic redundancy codes* (CRCs) on the disks can usually pick up and sometimes correct errors. However, if the computer is updating a directory structure when the power disappears, there can be serious trouble. Directory structures include *databases* (DBs) or file indexes and system directories such as the *file-allocation table* (FAT). Damaging even a small part of these structures may make large amounts of data inaccessible. Recovery of data may require painstaking retrieval of section (cluster, sector) after section of individual files.

Luckily, in recent years more operations are using fail-safe disks (e.g., *Redundant Arrays of Independent Disks* – RAID) with automatic mirroring and recovery.¹⁵ The occurrence of irrecoverable disk errors is low in such systems.



FIGURE 3.16

Uninterruptable power supply.

Midrange and mainframe computers have long had their own internal electrical-power conditioners and *uninterruptible power supplies* (UPSs). Less powerful, less expensive systems did not. However, users have placed critical applications on servers, workstations and microcomputers; alternative power supplies and line conditioners are now required components for most production systems – and if you depend on your data and your *personal computer* (PC) to accomplish whatever you consider critically important, then your system is a production system.

UPSs run the power from the mains into a transformer which keeps batteries charged; output power comes from *direct current rectifiers* which convert the battery power into alternating current (AC). UPSs provide excellent-quality power and good insulation from power-line fluctuations.

For PCs, work stations and servers, UPS units in the 0.4–1.2 KVA (*kilovolt-ampere*) range are sufficient; they range in cost from about \$50 for a little device about the size of a large surge-suppressor that gives you just enough time to shut a PC down gracefully to over \$1,000 for a sizable unit that can power your entire office.¹⁶ Keep in mind that you have to plan for peak loads, not just the average power drain. Big laser printers, for example, can run at 700 watts while warming up yet function on standby at a mere 100 watts. Older, physically larger disk drives take much more power while spinning up than while running normally. However, modern tiny, ultra-dense drives (e.g., 16-TB on a 3.5" spindle)¹⁷ require so little power anyway that they're no longer an issue of power consumption. Neither are USB drives, which are available in similar capacities.

The less load you put on the UPS, the longer it will last during the power outage. If you're lucky you will not only be able to avoid catastrophic errors but may even keep working productively until the power comes back.

The size of the batteries in your UPS and the drain by your systems determine how long the UPS can keep your system going. At a minimum, you need time for a graceful shutdown; five minutes is ample to allow you and your users to exit from application systems and shut down all peripherals and processors. If there is a reason to continue operating your system during a power failure (e.g., to protect the security computer that controls your physical access control systems), you may have to order extra batteries (for hours of operation) or a generator (for continuous operation as long as the fuel lasts).

Not all UPSs allow for addition of extra batteries, so examine the specifications carefully if you are thinking of providing extended run-times. Some systems are made to be completely customizable, with rack-mounted batteries that you can order and add at any time without fuss.

Just in case anyone reading this has the bright idea of hooking up one UPS to another, don't. The second law of thermodynamics ensures that all you will do is waste the battery power of the first unit as you try to charge the second one. You *can* run two or more UPSs in *parallel* – as when you attach different equipment to different UPSs.

In my office, I run two 0.9 KVA UPSs connected to a power conditioner (see *Power Conditioners* section below) and a third one just for a router and the wireless-phone transceiver. All my essential gear is connected to the UPSs: processor towers, monitor, phone charger, and even desk lamps in case I don't have my phone (with its flashlight app) at hand in the dark. I don't put the printers or the stereo system on the UPS. Many people will deliberately exclude their printers from the calculations for their proposed UPS. They can live without the printer when it loses power. At worst, given the automatic spooling (*Shared Peripheral On Line*) function that's normal on modern operating systems, they may have a single damaged page to reprint when they start the job up from the spool files.

It's a good idea to do a dry run with your new UPS: you really want to have a clear idea of just how long you are going to have once the external power fails. I have timed how long I can run without external power: almost exactly 30 minutes for my setup. At that point, the tolerable repeating beep from the UPS turns into an annoying whine; it's time to start the external electric generator. If for some reason the generator stops and I'm running out of battery power, I save my work to disk, exit from my applications, fire up the file-transfer software and get the current working documents over onto my portable computer or to an external disk so I can resume working once all the power is down. Then I immediately shut down the main system.

GENERATORS

If you use only a portable computer, you already have a UPS: your batteries. If a portable is your only computer, you might want to buy some extra batteries. In my office, though, I don't need to worry much about power failures: I have a 4.5 kW electrical generator that supplies my house and office (but not our electric stove, dishwasher, or laundry equipment). This generator can run about six hours at full load using about six gallons of gasoline – and I always have 30 gallons available (I use it for my tractor as well). Now, you have to understand that this is not a general recommendation for everybody's home or home office; I live out in farmland northeast of Montpelier, Vermont, and we can have power outages lasting days when the ice breaks the power lines. More important to us, we have a 130-gallon tropical fish tank that cannot fall below 75 °F without starting to kill our dozens of beloved fish. The \$2,500 generator¹⁸ and the \$1,000 wiring job to put in a transfer switch just made sense for us. More to the point for this section, I definitely can run our personal computers from the generator power through the power conditioners without problems.

For larger, more critical applications, you should evaluate large-scale UPSs which can be hooked into your office or building electrical system. Systems for loads ranging into the hundreds of KVA can cost from \$2,000 up into the \$100,000 range. Some units include gasoline or diesel generators and heavy-duty flywheels or large isolation transformers to smooth out the rough waveform of the generators' output.

Never run electronic equipment directly from generators without checking the power quality carefully. If you have the gear in-house, you can check power quality directly with the appropriate power-line monitors. Otherwise, see if your friendly neighborhood computer supplier has a power-line monitor they use for site qualification studies. When I worked for HP in the early 1980s, we would routinely install a monitor that printed out reports on the fluctuations in power to determine if we would allow our precious equipment to be installed without an external power conditioner. The reason: long experience had taught HP that bad power equals increased repair calls – and with a fixed-cost service contract, you can understand how seriously we took this kind of environmental report card.

POWER CONDITIONERS

Ordinary household generators of the kind sold in hardware stores for your country cabin can destroy your computer equipment within seconds. In my case, I discovered that the household generator I use has such a jagged (sawtooth) waveform that it could not be used to supply my UPS without a power conditioner.

The manufacturer explained that they have had trouble hooking domestic generators up to their equipment unless the generator is running at no more than one-third its rated capacity. In other words, in order to use their equipment, we are expected to buy a generator three times larger than we would normally expect to need. I was not pleased, but I didn't replace my generator, either.

Keep these problems in mind if you are shopping for a generator and avoid the hassles of trying to hook up incompatible devices.



FIGURE 3.17
Gasoline-powered
small generator.

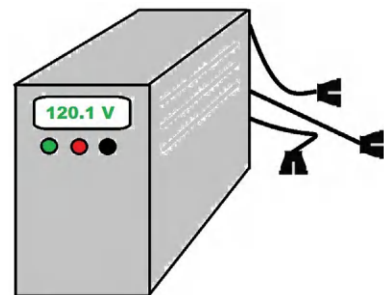


FIGURE 3.18 Power conditioner.

According to research by field service organizations as far back as the 1980s, almost half of all service calls on PCs are related to bad electrical power.¹⁹ Power fluctuations such as brownouts (transient low voltage), spikes (transient over voltage) and *line noise* (waveform deformations) can physically damage sensitive electronic equipment. Even surges on phone lines can damage modems and PC boards. At a very minimum, nobody should be running a computer without a surge suppressor in the power circuit; the cost is negligible compared to the assurance that a fuse wire will melt or a breaker will trip instead of having your precious equipment do the melting and breaking.²⁰

EMERGENCY LIGHTING

Common sense (as well as workplace safety regulations) dictates that you install adequate emergency lighting for all work areas and escape routes. After the bombs exploded in the *World Trade Center* in New York in February 1993, thousands of people had to feel their way through smoke-filled, pitch-black stairwells. It seems the emergency lighting system was controlled by computers that had been blown up by the explosion in the parking garage.²¹ Independent lights with their own batteries would have saved time and reduced injury in that disaster. Portable flashlights supplied to emergency marshals would have helped, too.



FIGURE 3.19
Emergency lighting.

TAMPER-PROOF ENCLOSURES

Now that you've spent all this money on electrical power equipment, how about protecting it all from tampering? Keep all electrical junction boxes, breaker panels and main switches under lock and key. In one hospital information-security evaluation in the 1980s, I recall bringing the head of the *intensive-care unit* (ICU) into the hallway and pointing at a panel on the wall. "What's that?" I asked. She shrugged and said, "I dunno; an electrical panel, I guess." "Open it," I said. Looking irritated, she did (it was unlocked). When she saw the labels on the breakers her pupils dilated and she looked horrified: those breakers controlled the precious equipment in her ICU – respirators, controlled-injection pumps for intravenous drips, heart monitors, external heart pacemakers – the works. If someone had tripped those unguarded, unprotected breakers, some of her patients would have died instantly. I also pointed out that because there is no security check on the people entering a public hospital, some sociopath or idiot could have tripped the breakers for fun. Moral: if you care about your electrical power, you have to protect junction panels just as strongly as any other component in the circuit.



FIGURE 3.20
Protect against tampering.

If you have to install additional power cables, ensure that they're pulled through protective ducts or manifolds, not left lying about in the suspended ceilings where anyone can get at them. And document all the switches and breakers correctly and readably so that people can make intelligent decisions in an emergency.

Label your UPS and power conditioners plainly with warning signs to prevent unauthorized equipment from being added to the circuits. In the May 1993 session of one of my *Information Systems Security* courses, a participant reported that an operator plugged a vacuum cleaner into the nearest electrical outlet, overloaded the UPS, and took down the LAN for a few minutes. That nearest outlet happened to be in the server's UPS, but the staff member had no idea that there was anything special about that unlabeled, unsecured outlet. You can't blame people for errors when you've failed to provide both training and proper labeling.

EMERGENCY POWER OFF

Be sure that there are at least two “panic buttons” (more properly known as the *Emergency Power Off* or EPO) in your computer room: one at each end and both near exits.²² Another EPO could usefully be installed *outside* the main door of the computer room in case smoke chases people out before they can hit the inside EPOs. The EPO cuts off all power to everything in the computer room except the lights. These switches should be protected against accidental use; for example, you can choose switches covered with a spring-loaded flip-top cover or models with the button at the bottom of a one-inch finger-sized tube. Install a phone within reach of each EPO for rapid communications in an emergency. Put a long extension cord on the handset of that phone or provide a cordless phone for use only in an emergency (cordless phones are not secure and should not normally be used for business communications).

It is especially important that the EPO shut down the power to your air conditioning equipment in case of a fire: ventilating an area threatened by fires is a really bad idea.

In one apartment building where I lived many years ago, a visitor had trouble opening the electrically operated door and therefore pulled the nearest handy lever – the fire alarm. To prevent this sort of error, label panic switches clearly; e.g., “MASTER POWER CUTOFF.” In general, my experience running a large data center convinced me that every single switch, electrical receptacle, and data communications plug ought to be labeled understandably and clearly. In addition, critical switches such as fire alarms need to include covers to prevent accidental or impulsive activation.²³



FIGURE 3.21 Emergency power-off.

POWERING OFF EVERY DAY?

It's generally easy to program computers and even other equipment to go to “*sleep*” (low-activity mode) at specific times, such as after the end of the day's shift.²⁴ However, completely shutting off the power to computer equipment is not recommended unless you intend to leave it off for an unusual length of time. An electrical engineer explained to me that the repeated thermal contractions and expansions caused by powering off computer systems actually causes more harm than simply leaving everything on standby. One of the consequences of the shrink/expand cycles seems to be that improperly installed chips with cold-solder joints can actually work themselves loose enough to start causing intermittent problems.



FIGURE 3.22 Don't power off without reason.

ELECTRICAL MAINTENANCE

Keep fuses handy in all the right sizes for all your electrical gear that requires fuses, including the power supplies. Make sure that your staff knows exactly where those fuses are kept and where the fuse-boxes and breaker-panels are. Run drills to make sure that their response to an electrical emergency is exactly what you have decided makes the most sense.

Every time you order modifications to the electrical system or find out that your building is having such modifications, be sure to check that the electrical grounding is correct. Especially when your midrange or mainframe systems use three-phase power, it's crucial that the correct wires



FIGURE 3.23 Maintenance.

carry the ground. While you're at it, verify that your building is properly grounded in case of lightning strikes. This precaution is especially important throughout the great plains of North America but must be studied worldwide now that the climate crisis has been increasing lightning strikes.²⁵

Be sure that your facilities crew are absolutely clear on which circuits may NOT be interrupted for routine work on the power system. Losing power because an electrician tripped a breaker is just as much a problem as any other kind of power loss. And it's worse if some untrained, unaware person shuts off power from your standby power systems.

ELECTRICAL ACCIDENTS

What would you do in case one of your colleagues touched a live 120 V wire and their hand clenched rigidly onto the power source? If you don't know instantly, you have a problem; I suggest you also ask your colleagues to find out if the problem is widespread in your organization. Not knowing what to do in such an emergency could cost one of your friends his or her life.

One hopes that there would be an easy way to cut the power: that's one of the purposes of the panic button we discussed above.

But if someone were in the process of being electrocuted in your computer room and for some reason you didn't have a panic button, what would you use to move them off the live wires? You're supposed to use a non-conductor such as wood or plastic. Some data centers have a wooden cane for this purpose hung on the wall along with fire extinguishers and other emergency equipment. Don't forget to train your staff, though, or the cane will simply sit on the wall while several people electrocute each other in turn.



FIGURE 3.24 Cane for emergency use.

CONTROLLING EXTERNAL FACTORS

Outsiders can be sources of support or of difficulty. The following sections discuss practical issues relating to infrastructure and critical components.

AIR CONDITIONING

Concentrations of computer system equipment (host processors, LAN servers, disk drives, system printers, tape backups, multiplexers, and so on) can use so much energy that regular office *air-conditioning* (A/C) fails to dissipate the heat. Ideally, temperatures in your computer center should be 66–73 °F (19–23 °C). Midrange and mainframe systems still produce so much heat that A/C failure can rapidly lead to high temperatures.²⁶

Each component of your computer system usually has its own temperature sensor that can cut off power at the upper end of the temperature range. In addition, computer rooms have their own global thermostats and cutoff switches.

In the data center where I worked as *Director of Technical Services* in the mid-1980s, an A/C unit failed one day. A new operator noticed the rising temperature but didn't realize the cause. He looked about for the room thermostat and noticed a temperature dial in the ceiling. It was set at 90 °F (32 °C). He turned it down to 70 °F (21 °C) and immediately lost power all over the computer room. He had changed the overtemperature power cutoff.

That day, we labeled every single dial and switch in the computer room.

Relative humidity should be maintained from about 45% to 55% to prevent static electricity buildup (if too dry) and condensation or curling paper (if too humid).

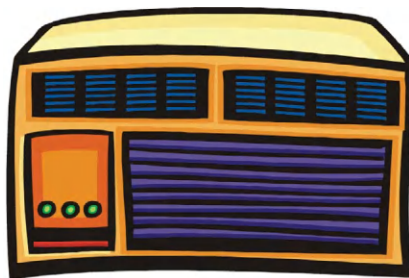


FIGURE 3.25 Air-conditioning.

Air pressure in the computer center should be slightly higher than in surrounding office areas so that air tends to flow out of the equipment area when doors open (especially in an emergency, positive pressure helps keep smoke and dust away from the electronics).

The computer room A/C should be separate from that for the rest of the building. You need to be able to control ambient conditions yourself under normal circumstances.

Protect the external air intakes to reduce the risk of a gas attack or tampering with your A/C. Make sure that the ductwork is non-combustible and that it does not provide a crawlspace for unauthorized access to your computer room. Sometimes it seems that every movie involving penetration of a secured area includes an obligatory scene in which heroes or villains crawl undetected through the A/C ducts. In every case, access to the ducts is relatively easy and is accomplished by removing a flimsy grate without using tools.

Link your A/C units to the fire-suppression control systems. The panic button that cuts power to your computer equipment should include the A/C equipment. In case of a fire, the last thing you need is the A/C continuing to pump fresh air into an enclosed area at risk.

The perforated tiles in your raised floor are part of the A/C system and fire-suppression systems. A/C engineers lay these tiles in patterns that control air flow within the computer room. These tiles must not be displaced at random. In some data centers, operators move the tiles about without considering the effects on air flow; in one case reported by a student in my *Information Systems Security* course, operators decided they didn't like the tiles, so they moved them all over to the far corner of the computer room. This spontaneous redesign of the A/C system produced Arctic conditions in one area and tropical temperatures in the other. The operators were on their way to generating a model of the global atmospheric wind patterns.

Although I've mentioned this in a previous section, I urge you to make sure that the floor under the raised tiles is kept clean and free of extraneous materials. The area next to an A/C outlet is often very cool; however, is not an appropriate cooler for soft-drinks and beer, which I actually saw once on a facilities inspection ☺.

CONTROLLING VENDOR ACCESS TO PRODUCTION SYSTEMS

A reader wrote to me in the 1990s, when modems were still being widely used,

I am at present producing a standard on modem access by suppliers to our control systems. The control systems are used to control the electricity-production process. I have just watched your CD on *Identifying and Managing IT Risk Factors* and the security aspects of this relate to data-collecting office systems. While the CD did help formulate some ideas, it would be ideal to talk with someone who has looked into the security aspects of accessing control systems via a modem.



FIGURE 3.26 Controlling access.

Here is what I answered (with a few additions due to technological changes in the last decades):

Thank you for writing to me. I do not know exactly what kinds of your systems need remote vendor access. For example, some of your infrastructure systems (generators? boilers? environmental controls?) may need access directly; your IT systems (processors, mass storage, communications equipment) almost certainly do.

There are some easy policies and procedures you can define and implement at once. There are others that are difficult and expensive.

- Whatever you do, be sure that you eliminate *canonical* (i.e., uniform default) passwords – that is, passwords that were assigned by the vendor and that are the same across all installations. Such passwords are notorious when users are unaware of the issue and

simply accept what they're given out of the box. This component is essential and easy to accomplish.

- Modems used only for maintenance by suppliers (and thus never for anything else) should be disabled (powered down or even unplugged) unless and until they are required for a specific communication that has been authorized by the appropriate member of the operations team. When the task is over, the modems should be made physically inaccessible again.
- Going one better, use *two* accounts for maintenance: one known to the vendor and used only when access has been authorized; the other, unknown to the vendor, at all other times. Do not use the same access password across these maintenance accounts. Ideally, use stronger authentication (e.g., *two-factor authentication* or 2FA) involving tokens (smart phones can serve that function), or biometrics as additional security for all access to all maintenance accounts.
- Verbal requests for authorization are not normal. In general, suppliers do *not* phone a client or send email asking for access: they respond to client requests.²⁷
- Another useful approach is to use a *remote-access server* (RAS) that provides encryption and access controls for anyone logging into your systems. Such systems are useful for all your employees who need to communicate; you can usually install strong *identification and authentication* (I&A) tools that will help you protect not only against abuse of your vendor access but also access by your employees and other users of your systems.²⁸

Network topology is not always recognized as a potentially strong element of effective security. Details depend very much on the specifics of your functional requirements – i.e., on who needs to access what in your networks. For example, in a real-time process-control system, it is possible that none of your production systems are hooked to any other systems that are in turn accessible through modems (or Internet connections). Secure network topologies should segregate segments of the network that should not normally intercommunicate. Perhaps in your case the example could be that there is no earthly reason why your accounting group should ever have any access whatever to the control systems for your generators. Such partition can be physical segregation (sometimes known as an *air gap*) of the networks – no connection at all. However, there may be practical reasons for allowing limited access across parts of the Internet; in those cases one can use routers and firewalls to limit traffic and allow only specified kinds of communication.

STEALTH-MODE UTILITIES

Some years ago I was looking at privacy-protection software and ran across an interesting note on the webpage of a particular product (the specific product is not the point of this section). The product (let's call it "*MyLittleSecret*") provided the following functions for *Windows* systems:

- *MyLittleSecret*TM can run at an interval of your choosing (every 1 min, 5 min, hour, etc.);
- *MyLittleSecret*TM can destroy specific records from your Web-browsing sessions;
- It can clear browser cache, cookies and toolbar entries;
- Clears browser history;
- Clears out social-media cache/cookies;
- Automatically empties *Recycle Bin* and clears out the *temp* folder (C:\TEMP);
- Clears out *StartMenu->Documents* folder and last *Find/Run* folder;
- Advanced settings let the user customize default directories.



FIGURE 3.27 Spyware.

So far so good. Based solely on the description, it looked like a potentially excellent tool for maintaining confidentiality on one's workstation.

However, my eyebrows rose when I saw the next part of the blurb, which I quote exactly except for the name:

*MyLittleSecret*TM hides in memory so that nobody will know you are using it! Use Stealth Mode to hide the program in memory under a different name. Combine this with Password Protection so that not only will nobody know what you are running, but they won't be able to get to it.

Hmm, this sounded a little alarming for network administrators. Stealth mode? For a utility that prevents tracking of what employees are doing with corporate resources? Didn't sound good to me. Some of the customer testimonials confirmed my fears:

- "My company's computer policy is so strict - now I can visit the sites I want without leaving any trail. *MyLittleSecret* installed in seconds and was incredibly easy to customize!" – Sarah, New York
- "I have recently download [sic] *MyLittleSecret* to find it is an EXCELLENT idea. I find the stealth mode extremely useful – combined with the password facility, it's ingenious! My surfing habits are nobodies business. [sic] Finally a product that understands this" – Sally, United Kingdom
- "I am extremely impressed with your warp drive customer service!!! I also am impressed with the potential for this great little utility! I work for the 'State'. I needed some way to protect my Web experience – AND YOUR most excellent utility is just the Jedi mind trick I have been looking for!!! I have passed this information on to several friends at our office so they too can have a life!!!" – Janet, Michigan

From my perspective in system management, *MyLittleSecret* is not so much "privacy protection" as "consequence avoidance." It seems to me that this product is being praised by people who want to violate corporate appropriate-use policies. For good reason, network managers are concerned about the use of corporate resources for unauthorized Internet browsing: employees are being paid to get useful work done but are visiting sports sites, downloading pornography, and trading large volumes of music and video files. Wiping cache covers dirty tracks for people who are wasting time on unauthorized browsing, but it also eliminates cached copies of legitimate pages and symbols and can significantly slow down the next visit to a particular website.

The activities the stealth-mode software is covering are inherently risky. For example, in a bandwidth-bound organization, the extra load on Internet-connection bandwidth and even local area network bandwidth from unauthorized, heavy-duty browsing can slow response time for everyone on the network. Some of the materials being downloaded may make the employer liable for civil damages or criminal prosecution; trafficking in child pornography, for example, is illegal around the world. Even if these stealth products do try to wipe out traces of incriminating evidence, displaying objectionable material in the first place may itself contribute to what lawyers have called a "hostile work environment" and lead to civil lawsuits by offended or harassed employees.

Stealth mode is designed to help the user avoid detection by duly constituted network authorities; the unexpected consequences are potentially serious. For example, from a support standpoint, if anything goes wrong with the stealth software, or if it interacts badly with other software, tech support may not identify the origin of the problem if the cause is hiding itself and users fail to mention its existence. If the corporate computer is passed on to another user without a thoroughgoing re-installation of the operating system, the stealth software may continue to load without any sign to the new user except for disappearance of cache and cookies – which may not be the desired condition. "Why do I keep having to write in my account information all the time??"

If your security policies do not already include a clause to forbid installation of unauthorized software on corporate computers, include one; here are two examples from my favorite policy source, Charles Cresson Wood's *Information Security Policies Made Easy* (version 9, but the current version is 14).²⁹ These policies were in section 8.03, "Protection against malicious software."

USER INSTALLATION OF SOFTWARE

Here's a control policy I recommend:

Users must not install software on their employer-supplied personal computers, network servers, or other machines without receiving advance authorization to do so from an appropriate information-security coordinator.

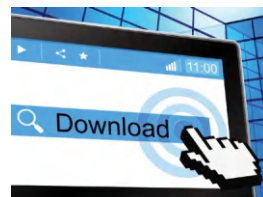


FIGURE 3.28

Downloading software.

Internet access has made many new programs available to the general user population. If users install such programs, or permit an installation process performed by an automatic installation routine, viruses could be propagated, system crashes initiated, and other problems created. This policy explicitly prohibiting users from installing any software unless previously approved by the information-security coordinator. New personal computer software packages are available that will prevent personal computer users from running any software besides the software specifically approved by management. By implication, this policy prohibits the use of Java and ActiveX applets, but some users may not make the connection.

What about downloading software onto work computers using the Internet?

End users must not download software from the Internet under any circumstances.

This policy brings some order to what is often a very chaotic software update environment on end-user personal computers and workstations. End users in many organizations are taking the software update process into their own hands, and in the process they often create problems for the helpdesk and others working in the IS area.

This policy assumes that the organization has a process in place to distribute software and related upgrades. The policy works much better if its implementation includes workstation access-control packages that prevent end users from updating software themselves. Also useful in the implementation of this policy would be an automated software-license management package that periodically takes an automated census to determine what software is installed on each machine.

This policy assumes that all end-user machines are connected to a local area network, a wide area network, an intranet or some other network through which software updates may be pushed. The delay associated with testing software before it is installed across an organization is often desirable because this delay will permit serious bugs to be reported to public forums. Those performing software testing can install patched versions that have corrected these problems.

As for specific technical measures to fight this kind of unauthorized software, I suggest several approaches for network managers faced with the possibility that their users are installing this product or any similar tools for evading corporate Internet-access policy:

- Warn your users that installing software that uses stealth mode is *prima facie* evidence of malicious intent to violate corporate policies and will be viewed as a serious breach of ethics.
- If you find a stealth-mode program on a system, contact your anti-virus and anti-pest vendors and ask that it and any other product with "stealth" capability be added to the list of potentially harmful software so it can be located and expunged from user systems using anti-malware scans.

So I guess you'll agree that if I abuse you by violating your copyright on your own writing, it's your own fault for writing to me. And if thieves steal gasoline, it's the victim's fault for not having better security. And if a torturer harms children, it's their parents' fault for not protecting them. And if, in general, bad people do bad things to others, it's entirely their victims' fault for not being able to prevent those harms.

As for the anarchistic, free-flowing uncontrolled environment, it would be interesting to hear from you why you make that assertion about TCP/IP-connected networks but not about, say, modem-mediated linkups, telephone conversations, letter writing, or face-to-face interactions. Why the special treatment for a particular communications technology? What is so special about a particular communications protocol that forces the implication that we ought to discard normal expectations for civility?

And why not extend your arbitrary rules about breaking down rules of courtesy and honesty when using the Internet to the use of particular languages? For example, how do you defend "the Internet must remain an anarchistic, free-flowing uncontrolled environment" without also supporting the view that "the use of French must remain an anarchistic, free-flowing uncontrolled environment?" Under this extension of your principle, I can hit you over the head with a mallet (assuming I can reach you and you can't defend yourself) as long as I cry, "Merde, espèce de crétin!" but not if I say the same thing in English.

* * *

The correspondent wrote back with the following comments:

>oopsie ... i put my foot in it, eh ... opened the can and jumped in with the worms ... argh ...

your points are valid ... however, using my name and company puts me at risk and i don't need that hassle ... you make the point rather succinctly ... the dialog does show both sides of the issue ... if you feel you must ruin or at least jeopardize my career, so be it ... use this as a column but PLEASE leave my real name and employer out of it

... i will leave the issue there and ponder my further response ...<

* * *

So much for the anarchistic, free-flowing uncontrolled environment of the Internet.

UNAUTHORIZED VULNERABILITY SCANS

Back in April 2000, an 18 year-old honor student at a high school entered the boys' locker room and showered with several of her male schoolmates. For her pains, she was stripped of her position as class valedictorian, lost various privileges, and undoubtedly felt awful about how she was being treated. She initially claimed that her intentions were good: she said she was pointing out a problem that she felt needed to be fixed and she was doing so in a way calculated to draw attention to that problem. She eventually recanted and admitted she was just having fun.³⁰

This youngster initially claimed great enthusiasm for improving security at her school but, alas, she didn't show quite as much judgement as the situation warranted.

So what does this have to do with information security? It is a remarkable parallel to cases that have recurred in our field: well-meaning people sometimes violate protocol by demonstrating security vulnerabilities without authorization.



FIGURE 3.30 Scanning for vulnerabilities.

In perhaps the most notorious case, a jury convicted Randal L. Schwartz of three felony counts under Oregon's *Computer Crime Law* in July 1995 after he tested security at *Intel Corporation* in Beaverton, OR while working there as a consultant. Unfortunately, Mr Schwartz forgot to get permission to test his client's security; he was sentenced to five years of probation, 480 hours of community service, and \$68,000 of damages. His conviction was overturned and his conviction expunged in 2007.³¹ This case evoked considerable head-shaking by people who couldn't believe anyone would be stupid enough to breach security without written authorization from appropriate officials of the target organization.

You would think this would be obvious, but it seems we should spell it out: do not break into your employer's poorly secured systems without written permission from your manager – and better, from your manager's manager too. Think of it as “holding a get-out-of-jail card.”

In a similar case at the university where I worked, a new student arrived in August 2011. Within three days, he hacked the administrative subnet in a misguided attempt to demonstrate his technical knowhow. He was expelled from the university immediately without a refund of his fees.

However, a much more problematic class of unauthorized vulnerability scans is those carried out on unknowing or unwilling participants. Unauthorized scans have caused debates for several decades; for example,

- In late 1996, Dan Farmer, a respected security researcher and creator of the network-vulnerability analysis tool called SATAN, released the results of a real-time security survey on the Internet. It included various classes of attacks against government sites, 660 worldwide banks, credit unions, on-line sex businesses and media organizations – all carried out without authorization from the unknowing participants. Farmer did not release the names of the organizations.³²
- From April 1997 through January 2000, Peter Shipley, a computer security expert in Berkeley, CA, used up to four laptop computers and up to 12 modems to auto-dial 5.7 million telephone numbers, day and night, to count the number of modem lines. He found 46,192 of the numbers to be modems; of course that means he dialed around 5,653,808 phone numbers that didn't have modems connected – but possibly had irate sleepers awakened at odd hours by a phone call consisting of modem-whines and without a human being on the other end.³³
- An uproar broke out in April 1999 when *Singapore Telecom* scanned 200,000 computers belonging to its Internet-service customers — without their knowledge or permission. At first, the company hung tough: “We are merely protecting the interest of our customers,” said Paul Chong, CEO. Staff explained that the non-invasive scans, carried out by anti-hacker personnel from the *Ministry of Home Affairs*, did not penetrate systems but merely noted vulnerabilities visible to any hacker. However, the company announced that 900 virus-infected computers had been found — which hardly seemed non-invasive. The company apologized to its customers within a couple of days after the furor erupted.³⁴
- In 2021, the revelation of *The Pegasus Project* showed that the NSO Group's surveillance software, sold to governments around the world, had been used to spy on thousands of targets.³⁵ The NSO Group developed the remote-access software for smartphones in 2010.³⁶ The spyware can infiltrate both iOS and Android phones and some users infected the targets using spear-phishing. Later versions integrated constant updates to include *zero-day vulnerabilities* (ZDVs); for example,
- “In 2019 WhatsApp revealed that NSO's software had been used to send malware to more than 1,400 phones by exploiting a ZDV. Simply by placing a WhatsApp call to a target device, malicious Pegasus code could be installed on the phone, even if the target never answered the call. More recently NSO has begun exploiting vulnerabilities in Apple's iMessage software, giving it backdoor access to hundreds of millions of iPhones.”³⁷

- A single leak of 50,000 phone numbers of devices infected by the spyware revealed widespread usage by government agencies, including in particular surveillance by authoritarian regimes of journalists and political opponents of the regimes.
- “The phone numbers... spanned more than 45 countries across four continents. There were more than 1,000 numbers in European countries that, the analysis indicated, were selected by NSO clients.”³⁸
- Targets in the sample were located in Algeria, Azerbaijan, Bahrain, France, Hungary, India, Kazakhstan, Mexico, Morocco, Morocco, Pakistan, Qatar, Rwanda, Saudi Arabia, South Africa, Spain, Turkey, United Arab Emirates, United Kingdom, and Yemen.³⁹

In summary, with today’s increasing use of *intrusion-detection systems* (IDSs), scanning for vulnerabilities without authorization looks likely to put people into a whole lot of trouble. In addition, since no one can determine the motivation behind such scans, even a well-meaning scan by honest people can be misinterpreted. This misinterpretation is even more likely now that people know about the *distributed denial-of-service* (DDoS) attacks that depend on installing slave programs on poorly defended systems. Now, as I always point out, *I am not a lawyer* (usually abbreviated using the unfortunate acronym *IANAL*) *and this is not legal advice; for legal advice, consult an attorney*. Nonetheless, it seems to me that in some jurisdictions such as the United States even harmless vulnerability scans might be interpreted as unauthorized use and therefore fall under existing computer crime laws.⁴⁰

Although there is lots of room for debate on this topic, I propose a simple rule:

Obtain written permission for specific types of scan from appropriate authorities such as managers in charge of IT at the target organization before scanning or testing anyone else’s systems.

RESPONSIBLE VULNERABILITY DISCLOSURE

How should security vulnerabilities be disclosed by those who discover them? Should they be broadcast to everyone interested, including criminals? Should they be kept secret and sent only to the software creators? Should there be a time limit on how long product developers can be protected against disclosure? This issue, usually called “full disclosure,” has exercised security specialists, criminal hackers, and those in between for years.

In 2004, the *National Infrastructure Advisory Council* (NIAC)⁴¹ of the *U.S. Cybersecurity & Infrastructure Security Agency* (CISA)⁴² issued their *Vulnerability Disclosure Framework*.⁴³ The 54 distinguished panel members summarized their findings as follows:

- Discoverers and vendors often disagree, but not with respect to the fundamental goal to improve the security of software used in critical processes.
- Common terms and procedures are a fundamental requirement for effective vulnerability management.
- Compatible encryption schemes are necessary to ensure all stakeholders can participate in vulnerability management, and to ensure protection of sensitive information.
- A common threat-scoring method may help facilitate a foundation for the common understanding among stakeholders.
- Robust information-sharing of vulnerabilities, threats, countermeasures, and best practices is key to minimizing threats to critical infrastructure networks.
- Legal and regulatory frameworks at all levels of federal, state, and local government need to be reviewed with the goal of reforming public policy to support the secure sharing of vulnerability information among stakeholders without fear of financial or other liability.



FIGURE 3.31
Vulnerability disclosure.

NIAC published the following recommendations:

- Support development of a common vulnerability management architecture, including common terms and universally compatible procedures to be employed in the public and private sectors for identifying, reporting, scoring, remediating, and resolving vulnerabilities. This includes standardized email addresses for reporting and standardized website locations and content for sharing information effectively.
- Provide policy and funding to ensure that trusted environments are available to protect vulnerability information and ongoing investigations.
- Promote universal use of multiple compatible encryption methods to ensure the U.S. federal government can participate effectively in the global vulnerability management process.
- Conduct a regulatory-framework review. The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities.
- Support robust voluntary information-sharing through policy and funding. The federal government should set up or support neutral clearinghouses for vulnerability management, accessible to researchers, the private sector, and federal agencies.
- Support a robust infrastructure for international coordination.
- Promote and fund advanced university and industry security research and education.

RESPONDING TO REPORTED PRODUCT FLAWS

There's a long-standing discussion about what to do with information about security holes; *full disclosure* supporters cheerfully post the news, including full details of vulnerabilities and exploits, without bothering to notify organizations first to give them a chance to fix the problems. Others, like *GreyMagic Software* security engineers, follow the principle of not publishing details until the bugs have been fixed – or unless they receive no response to their alerts. Their advisories are generally respected and acted upon quickly by the product teams whom they inform. For example, in February 2003, GreyMagic engineers discovered serious problems in (my favorite) browser, *Opera*. [I like *Opera* because of its excellent security, highly customizable user interface, its small size, rapid loading, and responsiveness to the user base.] *Opera* immediately acknowledged the information and issued a revision with fixes within two days.

Individuals also contribute to better security when they inform organizations of security problems. Here's an item from John Gehl's and Suzanne Douglas' long-respected *NewsScan*⁴⁴ in 2020 that illustrates a sound response to flaws:

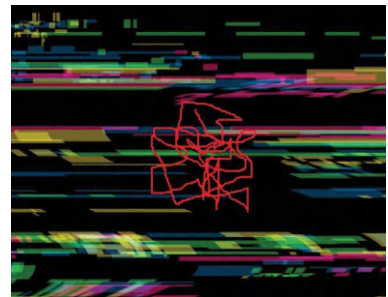


FIGURE 3.32 Flaws.

TRYING TO DENY SECURITY FLAWS “IS ALWAYS THE WRONG ANSWER.”

The website [Anonymizer.com](https://anonymizer.com), which offers a service that protects people's anonymity when they use the Internet, has acknowledged that it has had to fix several security flaws that had been identified by a friendly user, Bennett Haselton. Anonymizer president Lance Cottrell says that Haselton “came up with a new way of exploiting standards. They're pretty subtle.” The company has awarded Haselton a prize for his effort, which is given to anyone who can find security holes in the Anonymizer service. “We are always actively soliciting people to attack it. Trying to hide and keeping your head down is always the wrong answer.”⁴⁵

In contrast, there was another incident in May in which *GreyMagic* informed *Microsoft* of problems in Internet Explorer. *Microsoft* was offering prizes for bug reports but when *GreyMagic* staff reported the problem, there was a delayed response. At that point, the security group decided to post their advisory even though they figured they probably would not receive thanks, let alone the reward, for their work. *Microsoft* issued patches when the vulnerability was reported to the public via the *NTBugtraq*⁴⁶ mailing list.⁴⁷

In my case, in 2011 I wrongly reported the presence of malware in the installation files of a laptop computer to the manufacturer; I sent email to half a dozen executives' addresses on their website. Unfortunately, no one responded, and a few weeks later I stupidly published an article about the problem – which I had to retract because it was a false positive by a specific antimalware company.⁴⁸ In that case, my own stupidity in not trying harder to contact the company or to discuss the issue with the initial anti-malware provider was exacerbated by my unacceptable impatience about the failure of the computer-company to respond promptly.⁴⁹ I was quite rightly fired by the publisher.

Consider the difference between the open vs closed responses described above: the positive, professional response by the software firms not only supported their customers, it also gained them positive publicity. I'm sure that most of us are more confident about the integrity of anyone who immediately admits a mistake and fixes it rather than ignoring the problem or worse, denying it. In contrast, the stonewallers fail to resolve the problem and then make it worse by making people angry.

I think the lesson here is that everyone producing software ought to have an effective incident-response plan for dealing quickly with security flaws. Some simple suggestions:

- Technical-support procedures need an escalation process to deal with problems of high importance; similarly,
- Everyone in a software company should know exactly what to do when they receive any message that claims there's a security flaw in one of their products.
- It should not matter if the message is received by a secretary in the accounting department or by a programmer working on a different product: each employee should know to whom to send the warning and should do so at once.
- In addition, no one should assume that a message has been received by the right people until there's a confirmation from that person or group.
- Ideally, the person receiving the bug notification should personally take the responsibility for passing the message on in person to the right resources and should verify that the person who sent in the bug gets a prompt, courteous response.

AIRPORT-SECURITY LESSONS

As I wrote this essay at 33,000 feet on my way home to Vermont long ago, I was thinking about several security issues that I noticed within a 20-minute period at an airport. I hope that readers will agree that the experiences have lessons for all of who need to protect their information and resources.



FIGURE 3.33 Airport security.

THEFT IN THE WAITING LINE

The first security issue was at the security-inspection station, where the agent tried to get me to put my computer through the X-ray machine before my bag went through. I made a point of putting the bag through and only putting the portable computer on the belt when I was the *very next person* to go through the metal detector. This is a well-established strategy to prevent the notorious



FIGURE 3.34 Waiting in line.

scam by which pairs of criminals steal laptops or other valuables: the person in front of the victim causes an obstruction *after* the portable has entered the X-ray machine by emulating a portable pawn shop and causing repeated alarms on their detector. By the time the victim gets through the detector, the laptop is long gone.

While I'm on the topic of metal detectors, here are some practical suggestions on shortening your security check: put all your metal stuff in your shoulder bag before you get to the security checkpoint; do not carry any questionable sharp objects – I now leave even my relatively harmless computer toolkit in checked baggage or at home instead of clipping it onto my belt as I usually do (geek fashion, you know). In warmer weather, I even make a point of switching to sandals before going to the airport – saves time because they're quick to take off and put on, they don't usually smell bad, and they often don't get checked at all, thus saving time.

ALARMS

As I was packing up my computer after it got swabbed and checked for explosives residues, strobe lights began flashing, horrible grating noises rent the air, and nobody seemed to pay the slightest attention to the ruckus. "What's *THAT*?" I asked the security guard. He shrugged and said casually, "Fire alarm."

Lesson: if you're going to have an alarm in a place where people are not trained to recognize it, make the alarm self-explanatory. Why bright white strobe lights and a low-pitched loud retching noise should automatically be understood as a fire alarm is beyond my comprehension. In my house, the fire alarm shrieks, "FIRE!" over and over at the top of its electronic lungs.

I enquired politely, "Why isn't the terminal being evacuated?" "Oh," replied the bored guard, "it's probably just another false alarm." "So what?" I enquired. "What's the point of having an alarm at all if no one pays any attention to it?" Resentful silence.

I thought about an incident a few years ago where a meeting of about 300 security experts was interrupted by a fire alarm in the hotel. Without a word, all 300 of us collected our laptop computers (minus the power cords and bags) and calmly walked out into the street where we waited for the alarm to end or the building to burn down. When we were informed that everything was safe, we walked back in. Not one person asked, "Is this a test?" or "Do you think it's a false alarm?" The hotel staff were astounded.

Lesson: teach your own staff (and family) that an emergency alarm is not a TV quiz show in which you get points for guessing correctly that it's actually a false alarm. It doesn't matter if it's a false alarm: get out of the building at once. Similarly, in network security, if there's an alert from your *intrusion-detection system* (IDS), your firewall, or your operator, act on the alarm. That doesn't necessarily mean you have to shut down your system, but it does mean that every alarm should be taken seriously and not simply ignored or shut off in the stupid hope that it's a false alarm.

The airport alarm did stop after about 10 minutes, and I enquired at the bookstore (where I picked up the latest novels by P. D. James and Elizabeth Peters, yum) whether such alarms were frequent. "Oh yes," said the attendant, "they happen all the time." She also confirmed that no one paid any attention to the alarms any more.

Lesson: becoming habituated to false alarms will cause a tragedy if delayed reactions cause victims to be trapped in dangerous circumstances. Similarly, in network security, if operations and security staff habitually wait before acting on computer emergency response plans, hackers will succeed, fires will burn things, and water will soak things. Inserting an unnecessary delay in emergency response is just asking for trouble.

The agents at the airport airline club said the same about habituation. I asked them, "How will you distinguish a real alarm from a false alarm?" They explained, "We call the control point and ask them if it's for real."

Lesson: if false alarms happen, fix the system, don't just work around the problem.



FIGURE 3.35
Managing alarms.

CONFIDENTIALITY IGNORED

In the club, I sat down at a cubicle to work on my laptop. The oaf in the next cubicle was talking so loudly on the phone that everyone could hear every word from yards away. Apparently he was angry at his insurance agent because the insurance company had excluded back problems from his medical policy; he explained that his son had jumped on his back and put it out so he'd gone to the chiropractor and gotten it fixed and it wasn't fair to exclude that and he'd like to think about canceling the policy unless they put the back coverage back in and it was making him mad. Then he called a colleague and discussed whether they should fire Henry Foster (not the real name) even though he really liked him and.... The kind of information being bellowed over the phone by this person would be very useful for *social engineering* by a criminal hacker.

We know that social engineering is an important tool for criminal hackers. Social engineering applied by hackers refers to lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can then be used to break into systems. Social engineering is based on deception and on violation of social norms of fairness and honesty.⁵⁰

Names, details of problems – just the kind of issue that lets a criminal sound convincing as they misrepresent themselves. Honest people who don't expect others to lie are prime prospects for these criminals.

Lesson: train your colleagues to keep their voice down in a public place and to *think* about the level of detail appropriate for discussing confidential information where others, possibly competitors, hackers, and extortionists can hear them.



FIGURE 3.36

Indiscretion.

CONFIDENTIAL GARBAGE

Finally, as I threw away an apple core, I noticed a thick wad of papers at the top of the garbage bin. Succumbing to a security-geek's curiosity, I did a bit of scavenging and examined the documents. They consisted of 50 pages of printouts of detailed emails and printed DB records concerning holders of health-insurance policies. The data included full names, dates of birth, and discussions of various problems, including procedural screwups such as refusing policies because no one could find the registration information for the insurance broker who booked a policy. In addition to constituting gross violations of the U.S. *Health Insurance Portability and Accountability Act* (HIPAA),⁵¹ the level of detail and the number of employees named in these documents would be a goldmine for social engineering by criminal hackers. "Hi, I was talking with Jeb Holden over in the San Diego office about this screwup with Mr Watkins and I wondered if you knew who's been taking care of the DB that had problems?" In addition, there was a separate printout from the same company that contained detailed, confidential information about the financial difficulties the publicly traded company was experiencing. The information might be useful for stock manipulation; for example, were it to be released, it could cause a dip in the stock price, allowing a criminal to make a profit by selling futures. Ironically, the airline club had a high-capacity shredder. Too bad the person who discarded the confidential files didn't think to use it.

Lesson: train your colleagues to *think* before discarding (or even printing) confidential information. Destroy what should not be made public.



FIGURE 3.37

Garbage cans aren't shredders.

REPORTING PROBLEMS

I wrote to the U.S. *Federal Aviation Administration* (FAA) and the chief of security at the airport about the alarm debacle. I also sent a polite note to the chief of security at the company whose confidential files were dumped in an open public trash can and returned the confidential documents to them. I hope there was some good from those actions, and I hope that readers will take the lessons from my stroll through the airport and apply them in your own work environments and when traveling.



FIGURE 3.38

Report security failures.

THAT WON'T FLY

On August 10, 2006, British police arrested 24 people suspected of plotting to blow up planes flying from Britain to the United States⁵² In the wake of these police actions, the U.K. *Department of Transport* issued new, stricter regulations limiting what passengers could take into aircraft cabins. The press release of August 10 specifically allowed only the following – and everything had to be placed in a transparent plastic bag, not in pockets (quoting exactly):



FIGURE 3.39 Airport security.

- Pocket-size wallets and pocket-size purses plus contents (for example money, credit cards, identity cards, etc. (not handbags)
- Travel documents essential for the journey (for example passports and travel tickets)
- Prescription medicines and medical items sufficient and essential for the flight (e.g., diabetic kit), except in liquid form unless verified as authentic
- Spectacles and sunglasses, without cases
- Contact lens holders, without bottles of solution
- *For those traveling with an infant:* baby food, milk (the contents of each bottle must be tasted by the accompanying passenger) and sanitary items sufficient and essential for the flight (nappies, wipes, creams and nappy disposal bags)
- Female sanitary items sufficient and essential for the flight, if unboxed (e.g., tampons, pads, towels, and wipes)
- Tissues (unboxed) and/or handkerchiefs
- Keys (but no electrical key fobs)
- All other belongings must be stowed in checked luggage.⁵³

These rules had serious implications for business travelers who needed to fly to Britain and back from the United States.

First of all, nobody was going to be bringing laptop computers, cell phones, personal digital assistants (PDAs) or even watches onto the aircraft. That restriction meant that confidential information stored on such devices could then be exposed to greater threat than if the devices were kept with the passenger. Not having your computer with you on a transatlantic flight may have changed travelers' perspective on the productivity costs of international travel. I recommended they bring a good book, because they sure weren't going to be answering email, writing that management report they intended to finish, or even watching DVDs or listening to CDs. And forget the sound-suppressing earphones: I didn't see those on the approved list, either.

Luckily, good sense prevailed and the restrictions were quickly relaxed a few days later (August 14, 2006).⁵⁴

This overreaction and rapid correction illustrated the importance of weighing risk reduction against costs. Had these restrictions stayed in place, the increased relative value of electronic conferencing might have reduced the use of physical transatlantic meetings, with positive reductions in air travel costs. Such increases would have sped up the implementation of communications security, with *virtual private networks* (VPNs) becoming *standard operating procedures* (SOPs) for any kind of confidential information interchange at such meetings.

(While we're on the topic of virtual meetings, VPNs are considered essential to maintain confidentiality and integrity when using electronic-conferencing tools such as ZOOM.⁵⁵)

FLIGHTS OF FANCY

Putting laptop computers in checked baggage can be a significant risk for the security of confidential information stored on these devices. Other security equipment such as electronic key fobs for automobiles can also be lost or stolen in checked baggage. Luckily, the number of such losses is relatively low; for example, a 2013 review reported that only a fraction of one percent of all checked luggage was lost or misplaced.⁵⁶

To reduce the likelihood that my carry-on bag will be taken by somebody else by mistake, I always strap it with a brightly colored, wide nylon strap that not only makes it more distinguishable but also serves as a safety measure in case the zipper fails. You can also use a microchip luggage tag, which allows immediate identification of luggage and automatic notification of the owner if a misplaced bag is recovered.⁵⁷

Those measures don't change the risk of theft, however, so one should still think carefully about the value of encrypting confidential data and using strong I&A measures on electronic gear stored in checked luggage.

Assuming that you have encrypted your data, you'll also want to think about insuring the value of your hardware. You may have to evaluate several options to find an insurance policy that ensures against both damage and loss at reasonable cost.⁵⁸



FIGURE 3.40 Luggage at airports.

ACCESS AND EGO

One of the principles I teach is that access to computer systems or information is a privilege, not a right. It is unwise to grant access privileges to managers who don't need it – there's a risk that access will become a status symbol instead of a tool tied to specific job requirements. One of the incidents that I recall with amusement occurred around 1985 when the president of the company I worked for brought a visitor from Toronto to our Montreal data center on a Saturday night and asked the operator to let them into the computer-operations room. The operator politely refused because the president was not on the list of approved unaccompanied visitors. The young man offered to call me for permission, but the president took the snub in good spirits. Indeed, he wrote a letter of commendation for the operator on the following Monday. The president was demonstrating *egoless work*.⁵⁹

In contrast to the case above, I was sitting with a colleague in a class years ago and heard a story that may send shivers up the back of any network-security administrator.

My colleague – let's call her Amy – was the security manager at a major financial institution. She discovered that one of the managers from the accounting department had root access on the production systems for which Amy was responsible. No production systems should be accessible to anyone who does not need total control over that system as part of their official responsibilities. Even within the production department, only a few people should ever have root access. In addition, one of the fundamental principles of security, whether for financial systems or for computers and networks, is the separation of duties. An accounting-department manager with root access could easily initiate transactions and force them through production DBs without supervision or detection.

Amy immediately went to talk to the accounting manager. Her normal strategy when dealing with anomalies was to assume that there must be a good reason for the situation and to investigate with an open mind. In contrast to some security managers I have known, Amy knew that adopting a hostile or authoritarian attitude would only cause resistance and resentment among her colleagues. Unfortunately, resistance and resentment were the immediate responses from the accounting manager. This man believed that having access to root was symbolic of his importance and power within the organization. He instantly took umbrage at Amy's questions and told her that he had no intention of giving up his root access or even of discussing the question further with her. Worse still, it turned out that this manager was the son of the CEO. He said that he would have Amy fired if she took away his root privilege.

If Amy succumbed to the threat, she would lose all credibility within the organization. If she challenged the abuse of power, she might get fired. Amy did the best thing she could under the circumstances: she removed the unwarranted root privileges at once and went directly to the CEO to discuss the situation. To her relief, the CEO supported her 100 percent. She never had any further conflict with the CEO's son; one can only imagine what the conversation was like between father and son.

This story illustrates an important principle: one must not confuse access with status or personal worth. The CEO's son, for psychological reasons unknown to the security manager, seemed to believe that his personal worth was bound up with his unnecessary access to system resources. Anytime this confusion occurs, it presents the potential for danger to the organization and conflict with fundamental principles of security.



FIGURE 3.41 Egotistical boss.

I hope that these anecdotes will help network managers reach their colleagues who still think that carrying the modern equivalent of a universal master key announces how valuable they are to the organization.

It's time to shred the illusions about worth, ego and access.

ARTIFICIAL STUPIDITY

I was struck in 2002 by the kind of blooper that Peter G. Neumann's *RISKS Digest*⁶⁰ has been highlighting for decades: automated responses based on faulty assumptions.

One of the themes illustrating the dangers of stupidly defined rules rigidly applied is anti-spam measures based on absurdly clumsy methods of identifying unsolicited commercial email. Many correspondents have reported on simple-minded filters that block email based on, say, the presence of particular alphanumeric sequences. Such discussions usually have to dance circles around the actual target strings for fear that the anti-spam measures will block the issue of *RISKS*. For the same reason, I dared not write the sequence consisting of three instances of the third-to-last letter of the English alphabet (you know, the one between W and Y) in the original published article on which this section is based because so many filters identify any text containing that particular sequence as if they are inevitably pornographic messages.

Another example of a stupid rule instantiated into code is from an old version of *MS-Outlook*, where at one point years ago, the presence of the string “begin” followed by two spaces at the start of a line in an email message was interpreted as the start of MIME-encoded text.⁶¹ All the rest of the message was therefore converted to an attachment. Microsoft's proposed workaround was to use some other word than “begin” in one's text: they suggested “start” or “commence.”

Back in 2001, my old *CompuServe*⁶² email account (75300@compuserve.com) dating back to 1984 was blocked because the password was changed. I called technical support; they informed me that my account had been flagged as being involved in spam. Tech support could do nothing further to help me, they said; only the *Community Action Center* could do so. The *Action Center's* logs showed that my account had been frozen because I sent an announcement about an upcoming security lecture in our college's monthly series to 70 recipients (all students) and then immediately sent another (actually the same) message to about 40 faculty members. It seemed that *CompuServe* had very strict rules which automatically froze any account that was identified as sending spam – what a good thing, right? Well maybe not.

When I asked what the rules were so that I could avoid any further difficulties, I was categorically told that it is impossible to give the rules. The rules involve a combination of message size, number of recipients, and interval between messages with more than an indeterminate number of recipients.

I spent a while looking for any information about these (now practically mythical) rules in the *Terms of Service* and *Spam* sections of *CompuServe*, but I found nothing whatsoever to help me avoid future blockages.

The specific example is not particularly important. The significant problem is the blind, Philistine pig-ignorance (to quote the *Monty Python Architect Sketch*⁶³) that presupposes an absolute identity between email with lots of recipients and email that qualifies as spam. If one of my programming students had designed a system with this degree of stupidity I'd have assigned a zero for the design.



FIGURE 3.42 Bad AI.

Remind your programmers to test their assumptions before they engage in automated DoS to paying customers.

As for me, after 17 years with *CompuServe*, I switched to a different email system with clearer rules.

NETWORK LINKS

A reader from South Africa asked me about the security implications of having hyperlinks on a company intranet that point to (a) an Internet server owned by the same company or (b) to a server controlled by some other organization. In the following discussion, I focus on organizations such as government agencies and businesses but explicitly exclude academic institutions, which have their own peculiar policies related to principles of academic freedom.

Both questions revolve around crossing domains. The *Computer Desktop Encyclopedia* defines a network domain as “all resources under the control of a single computer system.”⁶⁴

Pointing from an intranet server to an Internet server, even if under the control of the same organization, increases the risk of the following security breaches:

- *Integrity*: risk that the contents of a document in an external link will change in ways that affect the functionality of the intranet page. What if an external agent (another department in the corporation, say) unilaterally changes the content of a page on which the intranet users have been depending? It may be difficult for the owner of the original document on an Internet server to keep track of all the users expecting to see specific content on a page accessed through the intranet servers.
- *Availability*: risk that a link for an important document will go bad. When I planned the links for curriculum pages on our university’s teaching extranet, all *required* readings point to materials residing on the extranet servers. Although this policy means that we must obtain permissions from all the copyright holders and sometimes pay royalties, it’s too great a risk to depend on URLs out of our control. In contrast, *optional* readings usually do use external links, but we check every one of those for currency before each repetition of a course module goes live for the next group of students.

INTERNET LINKS POSE IMAGE AND LEGAL PROBLEMS

A related question is about the risks of pointing to external non-organizational websites from a corporate Internet server.

In addition to the issues of integrity and availability mentioned in the previous section, there’s always the problem of lack of control over where users – especially customers or potential customers – will end up when they follow a link from a corporate site into the greater Internet. What may have been an inoffensive, useful page or document last week may be a salacious, tendentious, pornographic, libelous, or otherwise embarrassing destination this week. The public-relations department will surely be concerned about the implications of external linkages on any corporate webpage.

Does linking to another site imply approval or endorsement of whatever is on that site? In 1997, the German government filed charges against Angela Marquardt, the 25-year-old, blue-and-purple-haired deputy leader of the *Party of Democratic Socialism*, for linking from her webpage to a banned magazine called *Radikal*.



FIGURE 3.43 Links.



FIGURE 3.44 Bad links.

The issue of *Radikal* was banned because it included detailed instructions on how to sabotage railway lines. According to the public prosecutor, “It has nothing to do with censorship. Criminally relevant materials are subject to classification by the district attorney or criminal prosecutors.”⁶⁵ The court hearing opened and adjourned after an hour so the magistrates could arrange for expert testimony to explain the Net and the Web when the case reconvened. The German court ultimately ruled that maintaining a hyperlink to objectionable material is not tantamount to publication of that material.⁶⁶

Even just linking to another organization’s webpages (a practice now known as *deep linking*) can open one to a lawsuit from nitwits. In a startling display of anhistorical cluelessness about the history and even the *definition* of the Web, *Ticketmaster Group* sued *Microsoft* in April 1997 for including a link from *Microsoft* webpages to *Ticketmaster* webpages without a formal agreement granting permission for such links. The problem apparently stemmed from *Ticketmaster’s* perceptions that *Microsoft* was deriving benefit from the linkage but bypassing *Ticketmaster’s* advertising.⁶⁷ A few weeks later, *Ticketmaster* programmed its webpages to lead all *Sidewalk* users trying to follow unauthorized links to a dead end, where they were confronted with the statement,

This is an unauthorized link and a dead end for *Sidewalk*. *Ticketmaster* does not have a business relationship with *Sidewalk* and you do not need them to visit us. They want to traffic on our good name and your desire for information on live entertainment events to sell advertising for their sole benefit while offering nothing in return.⁶⁸

In another case of almost Pythonesque absurdity, Hollywood photographer Gary Bernstein sued several Web operators in September 1998 for having links – even indirect links – to a site that contained pirated copies of his works:

Bernstein discovered during his visit to the *J.C. Penney* site that by clicking on a series of hyperlinks to get additional information on Elizabeth Taylor, he was taken from *J.C. Penney’s* “Passion” subpage to a site called the *Internet Movie Database* (IMDb) – which is not affiliated with J.C. Penney or the makers of “Passion” – and then to a site in Sweden called SUNET, for the *Swedish University Network*. The site contains a large collection of celebrity photos, apparently placed on the Internet by fans. It included two images of Ms. Taylor – the Pink Lady Image and the Lavender Image.⁶⁹

In other words, his lawyers argued that the contamination spread along Web links: from the bad site to all those that linked to it and then to all the sites that linked to the sites that linked to the copyright infringer. By this reasoning presumably every owner of a website on the planet could be liable for any violation of copyright laws anywhere else on the planet. Luckily, *Los Angeles Federal District Court* Judge Manuel A. Real dismissed the indirect-linkage lawsuit and Bernstein withdrew his entire suit. I still think we could create an amusing satirical skit about this case.

POLICIES FOR EXTERNAL LINKS

Although a link to another document may be intended solely as a useful contribution to users of a website, corporate public relations, marketing and legal personnel are justifiably concerned about the tacit assumptions of some of their customers or users. For many technologically unsophisticated people, the concept of the *World Wide Web* is vague; it may not be obvious to a novice that they have moved from one Web server to another. If they click on a link on one site, they may erroneously



FIGURE 3.45 Global linkages.

assume that the page they are viewing belongs to the site they began visiting. If they don't like what they see, they may transfer their dislike to the original website and its owners.

Dislike of linked material boiled over into the public arena in July 2004, when South Dakota Governor Mike Rounds went ballistic over a link to *Planned Parenthood*:

South Dakota's Republican governor, Mike Rounds, shut down the teen section of the state library's Website, *eSchoolNews* reports. Though the *State Library Board* last spring rejected a request to remove a link to *Planned Parenthood* in the section, on July 9 the board reversed itself and agreed to remove the link. "Rounds opposes abortion; *Planned Parenthood* lobbies to keep abortion legal," according to *eSchoolNews*. Governor Rounds "said the removal of the Web links does not amount to censorship, because Internet users still can go directly to those organizations' sites. State government sites should not feature links to advocacy groups that are politically active, he said." *ESchoolNews* adds that most of the links in the section were related to teen culture, but there were links to *Columbia University's Go Ask Alice!*, "which provides answers to health concerns and some explicit sexual questions" and to "*It's Your (Sex) Life*," which includes information on pregnancy, birth control, and sexually transmitted diseases."⁷⁰

Some organizations explicitly display a disclaimer when a visitor clicks on an external link and then provide the link itself after the warning. For example, the *National Institute of Standards and Technology* (NIST) website uses a *Common Gateway Interface* (CGI) script that includes the following text:

Thank you for visiting. We hope your visit was informative and enjoyable.

We have provided a link to this site because it has information that may be of interest to our users. *NIST* does not necessarily endorse the views expressed or the facts presented on this site. Further, *NIST* does not endorse any commercial products that may be advertised or available on this site.⁷¹

Most organizations' security policies also forbid employees to put personal, non-business-related links on corporate webpages. It may be fun for an employee to add a link to a model-airplane club in her biographical notes on the "About Us" page on the corporate website, but if someone else working at *Acme Corporation* puts a link in his bio to a highly politicized site (e.g., supporting or opposing a particular political ideology or party) there may be repercussions for Acme's reputation or acceptance by customers. To avoid having to argue about which personally chosen external links are acceptable, it makes sense to restrict all personal links from a corporate website.

The most surprising case of an inappropriate external link I have ever encountered in my security practice concerned a law firm (all details are obscured to protect confidentiality) in which the network administrator was a pleasant and popular staff member who happened to be a transvestite with two identities. *Jim* showed up on Mondays, Wednesdays and Fridays and *Jan* showed up on Tuesdays and Thursdays. Nobody at the law firm minded at all (an admirable attitude I fully support) – until it was pointed out that their home page on the Web included a link to an association promoting transsexuality – which in turn had links to all kinds of, ah, vivid pictorial material. The lawyers were astounded to discover that the link had been on their home page for quite some time and immediately asked for it to be removed.

You never know what you might be linking to out there.

I do want to emphasize that the law firm would have been perfectly justified and indeed admirable for posting the link *knowingly*. The problem in this case is that the link was posted without consulting the organization's management.

I have many links to external sites on my *personal* webpages, but I always check the content to make sure I'm not going to be sorry for adding those helpful pages. And I am *very* careful about external links in teaching materials regardless of the principles of academic freedom: every link must be justifiable as relevant to learning about a specific topic.

NOTES

- 1 [Matte \(2021\)](#).
- 2 [U.S. Congress \(1948\)](#).
- 3 Platt, Physical Threats to the Information Infrastructure (2014).
- 4 Platt, Protecting the Physical Information Infrastructure (2014).
- 5 Kabay, M. E. (2023). Personal memory of AtomicTangerine training.
- 6 [Thorp, Stuart, and de Souza \(1988\)](#).
- 7 [Tamashiro \(2021\)](#).
- 8 [Daniels \(2011\)](#).
- 9 [Stein \(2013\)](#).
- 10 [Manoske \(2019\)](#).
- 11 [University of Rwanda \(2020\)](#).
- 12 [Government of Canada \(2021\)](#).
- 13 [Zhong et al. \(2021\)](#).
- 14 [Foster Fuels \(2018\)](#).
- 15 [Prepressure \(2021\)](#).
- 16 [Google Search \(2021\)](#).
- 17 [Google Search \(2021\)](#).
- 18 [Electric Generators Direct \(n/a\)](#).
- 19 [Bolton \(2019\)](#).
- 20 [Connell \(2017\)](#).
- 21 [U.S. Department of State \(2019\)](#).
- 22 [Culverhouse \(2017\)](#).
- 23 [Safety Technology International \(n/a\)](#).
- 24 [Colburn \(2019\)](#).
- 25 [Thompson \(2014\)](#).
- 26 [Digital Reality \(2019\)](#).
- 27 [Capterra \(2021\)](#).
- 28 [Remote Access \(2021\)](#).
- 29 Wood, Information Security Policies Made Easy, version 14 (2021).
- 30 [CBSNEWS Staff \(2000\)](#).
- 31 [Espiner \(2007\)](#).
- 32 [O'Hearn \(1997\)](#).
- 33 [Shipley and Garfinkel \(2001\)](#).
- 34 [Sesser \(1999\)](#).
- 35 Kirchgaessner et al., The Pegasus project part 1: an invitation to Paris, (2020).
- 36 Kirchgaessner et al., The Pegasus Project part 2: cat and mouse, (2021).
- 37 [Pegg and Cutler \(2021\)](#).
- 38 Kirchgaessner et al. (2021).
- 39 [Priest, Timberg, and Mekhennet \(2021\)](#).
- 40 [U.S. Code \(2020\)](#).
- 41 NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC) (2021).
- 42 U.S. Cybersecurity & Infrastructure Security Agency (CISA) (2021).
- 43 [Chambers and Thompson \(2004\)](#).
- 44 [Living Internet \(2020\)](#).
- 45 [The Mercury News \(2002\)](#).
- 46 [Sullivan \(2000\)](#).
- 47 [Sliwa \(2002\)](#).
- 48 Kabay, Apology to Samsung: We blew it, (2011).
- 49 [Stephenson P. R. \(2011\)](#).
- 50 [Fruhlinger \(2021\)](#).
- 51 U.S. Department of Health & Human Services (2020).
- 52 [Cowell and Filkins \(2006\)](#).
- 53 [BBC NEWS \(2006\)](#).
- 54 [U.K. Department of Transport \(2006\)](#).
- 55 [ZOOM \(2020\)](#).
- 56 [Hill \(2013\)](#).

- 57 Manuell (2017).
- 58 insuranceQnA (2021).
- 59 Kabay, On Writing, (2018).
- 60 ACM Committee on Computers and Public Policy (2021).
- 61 IBM (2013).
- 62 CompuServe (2021).
- 63 Chapman et al. (1989).
- 64 ComputerLanguage.com (2021).
- 65 Walker (1997).
- 66 Andrews (1997).
- 67 Brown (1997).
- 68 Wired News Staff (1997).
- 69 Kaplan (1998).
- 70 Collier (2004).
- 71 Standards Coordination Office USA WTO TBT Enquiry Point (2021).

WORKS CITED

- ACM Committee on Computers and Public Policy. (2021, July 22). *The Risks Digest: Forum on Risks to the Public in Computers and Related Systems*. (P. G. Neumann, Ed.) Retrieved July 27, 2021, from CATLESS: <https://catless.ncl.ac.uk/risks/>
- Andrews, E. L. (1997, July 1). *German Judge Dismisses Criminal Charge Over Internet Link*. Retrieved July 27, 2021, from The New York Times: <https://www.nytimes.com/1997/07/01/business/german-judge-dismisses-criminal-charge-over-internet-link.html>
- BBC NEWS. (2006, August 12). *Baggage advice for UK passengers*. Retrieved July 25, 2021 http://news.bbc.co.uk/2/hi/uk_news/4778615.stm
- Bolton, N. (2019, January 11). *Are Power Outages Bad for Your Computer?* Retrieved July 8, 2021, from CHRON: <https://smallbusiness.chron.com/computer-just-suddenly-power-off-67117.html>
- Brown, J. (1997, April 29). *Ticketmaster Sues Microsoft over Sidewalk Links*. Retrieved July 27, 2021, from WIRED: <https://www.wired.com/1997/04/ticketmaster-sues-microsoft-over-sidewalk-links/>
- Capterra. (2021, n/a n/a). *Digital Signature Software*. Retrieved July 9, 2021, from Capterra: <https://www.capterra.com/digital-signature-software/>
- CBSNEWS Staff. (2000, May 11). *School, Girl Battle Over Coed Shower*. Retrieved July 9, 2021, from CBSNEWS: <https://www.cbsnews.com/news/school-girl-battle-over-coed-shower/>
- Chambers, J. T., & Thompson, J. W. (2004, January 13). *Vulnerability Disclosure Framework: Final Report and Recommendations by the Council*. Retrieved July 23, 2021, from Cybersecurity & Infrastructure Security Agency (CISA): <https://www.cisa.gov/publication/niac-vulnerability-framework-final-report>
- Chapman, G., Cleese, J., Gilliam, T., Idle, E., Jones, T., Palin, M., ... Innes, N. (1989, October 20). *The Complete Monty Python's Flying Circus: All the Words* (First ed., Vol. 1). New York, New York, USA: Pantheon Books. Retrieved July 25, 2021, <https://www.youtube.com/watch?v=QfArEGCm7yM>
- Colburn, K. (2019, May 24). *Should You Turn Off Your Computer Every Night or Leave It On?* Retrieved July 8, 2021, from wtopnews: <https://wtop.com/tech/2019/05/should-you-turn-off-your-computer-every-night-or-leave-it-on/>
- Collier, A. (2004, July 29). *SD gov yanks teen site*. Retrieved July 27, 2021, from Net Family News: <https://www.netfamilynews.org/sd-gov-yanks-teen-site>
- CompuServe. (2021, n/a n/a). *About CompuServe*. Retrieved July 27, 2021, from CompuServe: <https://www.compuserve.com/home/about.jsp>
- ComputerLanguage.com. (2021, n/a n/a). *Definition: Domain*. Retrieved July 27, 2021, from Computer Desktop Encyclopedia: <https://www.computerlanguage.com/results.php?definition=domain>
- Connell, M. (2017, February 6). *Power Conditioners: Affordable Insurance or Waste of Money?* Retrieved July 8, 2021, from Computerworld: <https://www.computerworld.com/article/3163522/power-conditioners-affordable-insurance-or-waste-of-money.html>
- Cowell, A., & Filkins, D. (2006, August 10). *British Authorities Say Plot to Blow Up Airlines Was Foiled*. Retrieved July 25, 2021, from The New York Times: <https://www.nytimes.com/2006/08/10/world/europe/11terrorcnd.html>
- Culverhouse, T. (2017, August n/a). *Emergency Power Off (EPO) button*. Retrieved July 8, 2021, from TechTarget: <https://searchdatacenter.techtarget.com/definition/Emergency-Power-Off-EPO-button>

- Daniels, P. (2011, August 29). *Emergency Officials Concerned About State Office Complexes*. Retrieved July 7, 2021, from VPR Archive: <https://archive.vpr.org/vpr-news/emergency-officials-concerned-about-state-office-complexes/>
- Digital Reality. (2019, n/a n/a). *Data Center Cooling Technologies and Best Practices*. Retrieved July 9, 2021, from Digital Reality: <https://www.digitalreality.com/data-center-cooling>
- Electric Generators Direct. (n/a, n/a n/a). *Honda EM5000SX - 4500 Watt Electric Start Portable Generator*. Retrieved July 8, 2021, from Electric Generators Direct: <https://www.electricgeneratorsdirect.com/Honda-EM5000SXX3AN-Portable-Generator/p112647.html>
- Espiner, T. (2007, March 5). *Intel 'Hacker' Sentence Expunged*. Retrieved July 9, 2021, from cnet: <https://www.cnet.com/news/intel-hacker-sentence-expunged/>
- Foster Fuels. (2018, February 8). *The Effects of a Power Outage on a Business*. Retrieved July 8, 2021, from Foster Mission Critical: <https://fosterfuelsmissioncritical.com/power-outage-effects-businesses/>
- Fruhlinger, J. (2021, September 16). *Social Engineering Explained: How Criminals Exploit Human Behavior*. Retrieved September 21, 2021, from CSO U.S. | Security | Social Engineering: <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>
- Google Search. (2021, July 8). *Search "16tb Disk Drive"*. Retrieved July 8, 2021, from Google Search: <https://www.google.com/search?client=opera&q=16tb+disk+drive>
- Google Search. (2021, November 30). *Shop Uninterruptable Power Supply*. Retrieved November 30, 2021, from Google Search: <https://www.google.com/search?q=uninterruptible+power+supply>
- Government of Canada. (2021, November 5). *Global Affairs Canada*. Retrieved December 6, 2021, from International GC CA: <https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=eng>
- Hill, M. (2013, September 16). *The Odds of Losing Luggage*. Retrieved July 25, 2021, from USA TODAY: <https://traveltips.usatoday.com/odds-losing-luggage-109295.html>
- IBM. (2013, n/a n/a). *MIME Multipart Message Overview*. Retrieved December 1, 2021, from IBM | Documentation | IBM B2B Advanced Communications: <https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=concepts-mime-multipart-message-overview>
- insuranceQnA. (2021, n/a n/a). *Is There Travel Insurance That Will Cover My Laptop and Camera?* Retrieved July 25, 2021, from insuranceQnA: <http://www.insuranceqna.com/travel-insurance/will-travel-insurance-cover-laptop-and-camera.html>
- Kabay, M. E. (2011, April 4). *Apology to Samsung: We blew it*. Retrieved December 6, 2021, from NetworkWorld: <https://www.networkworld.com/article/2201735/apology-to-samsung-we-blew-it.html>
- Kabay, M. E. (2018, May 18). *On Writing*. Retrieved December 1, 2021, from M. E. Kabay | Methods: <http://www.mekabay.com/methodology/writing.pdf>
- Kaplan, C. S. (1998, September 25). *Can a Web Link Break Copyright Laws?* Retrieved July 27, 2021, from CyberLaw Journal – The New York Times: <https://archive.nytimes.com/www.nytimes.com/library/tech/98/09/cyber/cyberlaw/25law.html>
- Kirchgaessner, K., Lewis, P., Pegg, D., Sabbagh, D., Cutler, S., Lakhani, N., ... Safi, M. (2020, July 19). *The Pegasus Project Part 1: An Invitation to Paris*. Retrieved July 21, 2021, from The Guardian: <https://www.theguardian.com/news/audio/2021/jul/19/the-pegasus-project-part-1-an-invitation-to-paris>
- Kirchgaessner, K., Lewis, P., Pegg, D., Sabbagh, D., Cutler, S., Lakhani, N., ... Safi, M. (2021, July 19). *The Pegasus Project Part 2: Cat and Mouse*. Retrieved July 21, 2021, from The Guardian: <https://www.theguardian.com/news/audio/2021/jul/20/the-pegasus-project-part-2-cat-and-mouse>
- Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N., & Safi, M. (2021, July 18). *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon: Spyware Sold to Authoritarian Regimes Used to Target Activists, Politicians and Journalists, Data Suggests*. Retrieved July 21, 2021, from The Guardian: <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>
- Living Internet. (2020, November 24). *Well Known Mailing Lists – NewsScan*. Retrieved July 25, 2021, from Living Internet: https://www.livinginternet.com/l/la_known_newsscan.htm
- Manoske, A. (2019, April 4). *No Security in Obscurity*. Retrieved July 7, 2021, from medium.com: <https://a2d2.medium.com/no-security-in-obscurity-b36d878dead8>
- Manuell, R. (2017, February 22). *RFID Microchip Luggage Tag Technology and the Baggage Tech Revolution*. Retrieved July 25, 2021, from International Airport Review: <https://www.internationalairportreview.com/article/32144/reboundtag-baggage-handling/>
- Matte, C. (2021, June 24). *Why Is Sexting a Problem for Teens?* Retrieved July 7, 2021, from very well family: <https://www.verywellfamily.com/what-is-sexting-problem-1258921>

- National Infrastructure Advisory Council (NIAC). (2021, n/a n/a). *National Infrastructure Advisory Council (NIAC)*. Retrieved July 23, 2021, from U.S. Cybersecurity & Infrastructure Security Agency: <https://www.cisa.gov/niac>
- O'Hearn, B. (1997, January 7). *Dan Farmer Releases Real-Time Security Survey*. Retrieved July 9, 2021, from Risks Digest: <https://catless.ncl.ac.uk/Risks/18.74.html#subj10>
- Pegg, D., & Cutler, S. (2021, July 18). *What is Pegasus Spyware and How Does It Hack Phones?* Retrieved July 21, 2021, from The Guardian: <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>
- Platt, F. (2014). Physical Threats to the Information Infrastructure. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6 ed., Vol. 1). Wiley. Retrieved July 7, 2021, <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Platt, F. (2014). Protecting the Physical Information Infrastructure. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6 ed., Vol. 1). Wiley. Retrieved July 7, 2021, <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Prepressure. (2021, n/a n/a). *RAID*. Retrieved July 8, 2021, from Prepressure: <https://www.prepressure.com/library/technology/raid>
- Priest, D., Timberg, C., & Mekhennet, S. (2021, July 18). *Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide; NSO Group's Pegasus spyware, Licensed to Governments Around the Globe, Can Infect Phones Without a Click*. Retrieved July 21, 2021, from The Washington Post.
- Remote Access. (2021, n/a n/a). *A Beginner's Guide to Remote Access Software*. Retrieved July 9, 2021, from Remote Access: <http://www.remoteaccess.org/>
- Safety Technology International. (n/a, n/a n/a). *Stopper II: Helps Prevent False Fire Alarms*. Retrieved July 9, 2021, from Safety Technology International: <https://www.sti-usa.com/series/stopper-ii/>
- Sesser, S. (1999, May 7). *SingNet Issues Public Apology for Secret Virus Scanning*. Retrieved July 21, 2021, from The Wall Street Journal: <https://www.wsj.com/articles/SB926015638975623105>
- Shipley, P., & Garfinkel, S. L. (2001, n/a n/a). *An Analysis of Dial-Up Modems and Vulnerabilities*. Retrieved July 9, 2021, from simson.net: <https://simson.net/clips/academic/2001.Wardial.pdf>
- Sliwa, C. (2002, May 20). *MS Says Flaws in Patch May Be a New Vulnerability*. Retrieved July 25, 2021, from PC World: https://www.pcworld.idg.com.au/article/22357/ms_says_flaws_patch_may_new_vulnerability/
- Standards Coordination Office USA WTO TBT Enquiry Point. (2021, n/a n/a). Retrieved July 27, 2021, from NIST.GOV: https://tsapps.nist.gov/notifyus/data/leaving_nist/leaving_nist.cfm
- Stein, A. (2013, August 29). *New Waterbury State Office Complex gets \$42 million boost from FEMA*. Retrieved July 7, 2021, from VTDigger: <https://vtdigger.org/2013/08/29/new-waterbury-state-office-complex-gets-42-million-boost-from-fema/>
- Stephenson, P. R. (2011, April 4). *Samsung Laptops Clean: No Keylogger or Spyware of Any Kind Found*. Retrieved December 6, 2021, from NetworkWorld | Security: <https://www.networkworld.com/article/2201733/samsung-laptops-clean-no-keylogger-or-spyware-of-any-kind-found.html>
- Sullivan, B. (2000, September 20). *NTBugTraQ goes corporate*. Retrieved July 25, 2021, from ZDNet: <https://www.zdnet.com/article/ntbugtraq-goes-corporate/>
- Tamashiro, K. (2021, November 22). *Thieves Target Multiple Local Businesses in Brazen ATM Thefts*. Retrieved November 30, 2021, from KHON | Local News: <https://www.khon2.com/local-news/thieves-target-multiple-local-businesses-in-brazen-atm-thefts/>
- The Mercury News. (2002, May 21). *Security Holes Found in Popular Privacy Program*. Retrieved July 25, 2021, from Internet Archive – WayBack Machine: <https://web.archive.org/web/20020614074111/http://www.siliconvalley.com/mld/siliconvalley/3306644.htm>
- Thompson, A. (2014, November 13). *Lightning May Increase with Global Warming*. Retrieved July 8, 2021, from Scientific American: <https://www.scientificamerican.com/article/lightning-may-increase-with-global-warming/>
- Thorp, R., Stuart, J., de Souza, S. E. (Writers), & McTiernan, J. (Director). (1988). *Die Hard* [Motion Picture]. United States. Retrieved July 7, 2021, <https://www.imdb.com/title/tt0095016/>
- U.K. Department of Transport. (2006, August 14). *Airline Security*. Retrieved July 25, 2021, from Internet Archive - WayBack Machine: https://web.archive.org/web/20060812035241/http://www.dft.gov.uk/stellent/groups/dft_about/documents/page/dft_about_612280.hcsp
- U.S. Code. (2020, October 20). *18 U.S. Code §1030 - Fraud and Related Activity in Connection with Computers*. Retrieved July 23, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/18/1030>
- U.S. Congress. (1948, June 25). *18 U.S. Code § 1708 - Theft or Receipt of Stolen Mail Matter Generally*. Retrieved December 5, 2021, from Legal Information Institute | U.S. Code.

- U.S. Cybersecurity & Infrastructure Security Agency (CISA). (2021, n/a n/a). *U.S. Cybersecurity & Infrastructure Security Agency (CISA)*. Retrieved July 23, 2021, from U.S. Cybersecurity & Infrastructure Security Agency (CISA): <https://www.cisa.gov/>
- U.S. Department of Health & Human Services. (2020, November 2). *Your Rights Under HIPAA*. Retrieved September 14, 2021 from HHS | Health Information Privacy | For Individuals: <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html>
- U.S. Department of State. (2019, February 21). *1993 World Trade Center Bombing*. Retrieved July 8, 2021 from U.S. Department of State: <https://www.state.gov/1993-world-trade-center-bombing/>
- University of Rwanda. (2020, n/a n/a). *Why Choose UR?* Retrieved November 30, 2021, from Université nationale du Rwanda: <https://ur.ac.rw/>
- Walker, R. (1997, June 27). *In Germany, Policing the Net Brings Troubling Legal Issues*. Retrieved July 27, 2021 from The Christian Science Monitor: <https://www.csmonitor.com/1997/0627/062797.intl.intl.4.html>
- Wired News Staff. (1997, May 5). *Ticketmaster Blocks Sidewalk Users: Clicking from Microsoft's Seattle Site Now Leads to a "Dead End."*. Retrieved July 27, 2021, from WIRED: <https://www.wired.com/1997/05/ticketmaster-blocks-sidewalk-users/>
- Wood, C. C. (2021, n/a n/a). *Information Security Policies Made Easy, version 14*. Retrieved July 9, 2021 from InformationShield: <https://informationshield.com/products/information-security-policies-made-easy/>
- Zhong, X., Jiyang, L., Shulian, Z., Yidong, T., Xiliang, Z., Xuling, L., ... Songlin, Z. (2021, June n/a). Remote eavesdropping at 200 meters distance based on laser feedback interferometry with single-photon sensitivity. *Optics and Lasers in Engineering*, 141. <https://doi.org/10.1016/j.optlaseng.2021.106562>
- ZOOM. (2020, December 17). *VPN Split Tunneling Recommendations*. Retrieved December 1, 2021, from ZOOM | Help Center | Network and Firewall: <https://support.zoom.us/hc/en-us/articles/360053610731-VPN-Split-Tunneling-Recommendations>

4 Data Integrity

Correctness of data is essential for all of our work with information. This chapter looks at a variety of issues involving data integrity:

- Practical examples of the need for data integrity
- Basics of the Public Key Cryptosystem for protecting integrity
- Scumware violates data integrity
- Errors in spreadsheets that destroy integrity
- Verification to prevent and identify violations of integrity.

CRIMINALS VIOLATING DATA INTEGRITY AS WELL AS MORAL INTEGRITY

Data *integrity* includes correctness of information and stability of stored information regardless of correctness. Thus, if someone enters their birth year incorrectly, they've caused an integrity problem. If the actual weight of an athlete is stored on a computer hard drive but gets modified by a hardware or software glitch, that error is a violation of data integrity.

One of the enraging scams being perpetrated on (mostly) elderly victims is the *refund scam* (also called an *overpayment scam*). My wife's 92-year-old aunt, limited to getting about in a wheelchair, called me up a year before she died to announce in a panic that I absolutely had to go to her bank to sign a money order for a "poor Indian clerk" who had "inadvertently" "refunded" thousands of dollars into her bank account while supposedly trying to refund an erroneous PayPal charge.

The criminal had persuaded our aunt to allow him to access her computer and told her to access her checking account so he could deposit \$3,000 to refund the (nonexistent) withdrawal. Within moments, her screen showed that there had indeed been a \$3,000 debit followed by – gasp! – a \$30,000 deposit! Weeping in panic, the criminal said that he would be fired and his family would starve to death unless our aunt sent him a wire transfer for \$27,000 to correct the "error."

What actually happened is that the criminal got a screenshot of the bank record, inserted the fake entries, and then posted the modified screenshot on the compromised computer's screen. The image shown demonstrated a *violation of data integrity*.

I'm glad our aunt called me! She was horrified when I explained what happened.

The email messages many of us receive from a paypal4265@gmail.com (just an example) account claiming that we have been billed, say, \$440 for the purchase of Bitcoins or congratulating us on opening a new PayPal account illustrate how violations of integrity can be used to breach authenticity. A similar GMAIL message often comes (falsely) from "GeekSquad" for a license toor support contract for some useful product such as an antivirus tool – often an order of magnitude more than the actual cost of a license.

These scams depend on the ignorance or stupidity of the recipients to work (that is, to have the victims send money to the criminals as part of refund scams): it is out of the question for PayPal, Bank of America, and so on to be notifying victims of unauthorized charges using GMAIL, HOTMAIL, AOL, or email from (for example) the RU (Russian) domain. Another clue (duh) is that the criminals use a serial or transaction number in the scam email but *send the same message to a*



FIGURE 4.1 Data integrity.

BCC list. Finally, some of the criminals send fake checks in the mail that gullible people deposit and then pay back before their bank notifies them that the checks are indeed fake.

Readers may want to remind (or more likely, inform) gullible, unsophisticated users of email about these warning signs.¹

DATA INTEGRITY IN VOTING MACHINES

The explosive disagreements over the validity of vote counts reported by voting machines in the USA were brought to international attention in November 2020 when the losing candidate and his supporters accused state agencies across the country of having misrepresented the vote counts and allowed the election of Joe Biden and other non-Republican candidates for political office. The losing candidates and their media supporters accused the manufacturers of voting machines of having skewed the vote counts. Courts of law determined that the accusations were baseless in over 60 legal cases and there were severe financial consequences for some of the conspiracy theorists.²



FIGURE 4.2 Voting machines.

PAPER TRAILS

Vermont has a tiny population; we had about 645,000 people in the entire state in 2021.³ Because of this small population, people there have many ways of becoming involved in civic affairs. Our state house in Montpelier (the smallest state-capital city in the United States, with about 8,000 people)⁴ is open to the public, as are committee meetings. State officials such as the governor often walk about in town where ordinary citizens can chat with them in a friendly and very personal way.⁵

I was invited to address the *Vermont House Committee on Government Operations and Military Affairs*⁶ in 2004 as they discussed a pending bill which would require any wholly electronic voting mechanism to be equipped with a means of producing a paper ballot that could be inspected by the voter and which would then be stored safely for official recounts. Given the importance of safeguarding the vote in our nation, I thought it might interest readers to step outside the confines of network security for a moment to consider the security implications of wholly electronic voting.

Today, there are three different forms of voting in place in use in the USA (I won't discuss remote, Internet-based voting in this section): one can mark a piece of paper by hand and have it read by people; one can mark a piece of paper by hand or machine and have it read by an optical-mark reader which tallies the results automatically; or one can use a wholly electronic system with an input device such as a touch-sensitive screen which stores the results in a *database* (DB) and produces automatic tallies.

Normally, paper ballots, whether read by people or tallied by machines, are stored in sealed containers and can be opened with a court order in cases of judicially approved recounts when election results are challenged.

In Vermont, the *Secretary of State's* office allows optical-mark readers to be used for elections; only one such machine is required per voting location, most of which have at most a few thousand voters registered per location. However, most locations still use manual counting of ballots under the supervision of representatives of the various political parties involved in the election.



FIGURE 4.3 Paper trails.

In my testimony before the *Government Operations Committee*, I stressed the following points:

- Any system of vote counting that relies on completely proprietary (secret) programs is potentially vulnerable to abuse. The underlying computer programs controlling how marks on ballots are counted in Vermont are proprietary (they were originally owned by *Diebold Corporation* but eventually purchased by *Dominion Voting Systems* in 2010⁷), but the technicians who prepares the configuration tables relating a position on a ballot to a particular name worked for an independent consultancy in Massachusetts and their configuration tables were open for inspection.
- Every optical tabulator is tested to see if it reads ballots correctly before the election begins.
- Passing a law that allows the *Secretary of State* to order a random check on the accuracy of machine tallies in any voting district would help prevent systematic fraud. The tallies in a manual recount must match the machine tallies to within an acceptable error rate (to allow for the inherent difference between machine tallies and human counting methods: machine reject incorrectly marked ballots whereas people can agree on the intention of the voter).
- Wholly computer-based voting systems have far more vulnerabilities to tampering than optical-mark sensors.
 - We know that even companies such as *Microsoft* have allowed *Easter Eggs* (unauthorized, undocumented code such as flight simulators⁸) to escape quality assurance and be delivered to customers in software such as *MS-Excel*.
 - We know that microprocessors have been tampered with to cheat clients and evade testing (e.g., gas-pump meters in the Los Angeles district were designed to overcharge customers by 10% – unless they were set for one- or five-gallon deliveries, which were the volumes typically used by inspectors when checking accuracy).⁹
 - We know that production code has been profoundly flawed for years without being caught (e.g., the Colorado lottery's not-very-random-number generator that produced only numbers from zero to eight but never any nines).¹⁰
 - We know that data stored in DBs without careful attention to chained cryptographic checksums involving timestamps, sequence numbers and the previous record's checksum can be modified to misrepresent election results.
- For all these reasons, we should resist the use of wholly computerized voting machines until there is software that is entirely open to inspection.
- Any wholly electronic voting machine should be required to produce a paper ballot showing the voter's choices for inspection by that voter (only). The voter should then be required to place the ballot in a ballot box for use in judicial recounts and random testing of the accuracy of the computerized voting system.

At the time I was due to testify before the government committee, one of my colleagues who enjoys vigorous discussions and I got into a discussion of electronic voting systems. One of our (good-humored) verbal battles (which could cause those listening to turn pale and back off in fear that we would come to blows) practically cleared out the Faculty/Staff dining room in the Mess Hall at our university. My colleague blew a gasket when I suggested that electronic voting systems should produce a paper ballot to be verified by the voter and then dropped into a secured ballot box in case there was a recount to validate the electronic records.

What fascinated me was my colleague's attitude toward the trustworthiness of electronic systems:

That's ridiculous. Surely you should be able to devise a foolproof electronic system impervious to tampering? Otherwise, we're all in deep trouble, because we've been replacing manual systems by electronic systems for years now in all aspects of business. Why should we go to the expense of keeping old manual systems such as ballot boxes and hand recounts – which are vulnerable to abuses anyway – when we can – or ought to be able to – implement completely secure electronic systems?

This charming confidence in the power of software engineering is undermined by several well-established principles of the field:

- Security is an emergent property (much like usability or performance) and cannot be localized to specific lines of code.¹¹
- Security failures can come from design errors (e.g., failing to include I&A measures to restrict access to confidential or critical data).
 - Programming errors (e.g., failing to implement a security measure because the source code uses the wrong comparison operator in a comparison).
 - Run-time errors resulting from poor programming practice (e.g., failing to prevent bounds violations that result in buffer overflows and the consequent execution of data as instructions).
 - Malicious misprogramming (e.g., Trojan horses, logic bombs, and back doors).
 - Failure to patch code errors quickly.¹²
- Testing for security is one of the most difficult kinds of quality assurance procedures known; it is inherently difficult because failures can occur from such a wide range of sources.¹³
 - Worse, quality assurance is often sloppy, with poorly trained people who don't want to be doing the work assigned to the job in spite of their protests.
 - These folks often believe that manual testing (entering data in via a keyboard) is an acceptable method for challenging software (it isn't).
 - They focus on showing that the software works (instead of trying to show that it doesn't).
 - They don't know how to identify the input domains and boundaries for data (and thus fail to test below, at and above boundaries as well as in the middle of input ranges); and
 - They have no systematic plan for ensuring that all possible paths through the code are exercised (thus allowing many ways of using the program to be wholly untested).
- The principles of provably correct program design¹⁴ have not yet been applied successfully to most of the complex programming systems in the real world. Perhaps someday we will see methods for defining production code as provably secure, but we haven't gotten there yet.

Having independent measures to enforce security is a foundation principle in preventing abuse. Involving skeptical and intelligent people to keep an eye on voting machines is just one example of that principle, and it's worth the money to prevent our democracy (and other critical systems) from being hijacked.¹⁵

In 2006, a study from the *Center for Information Technology Policy at Princeton University* released a paper reporting on an independent study of the Diebold *AccuVote* e-voting machine.¹⁶ The abstract was alarming:

This paper presents a fully independent security study of a Diebold AccuVote-TS voting machine, including its hardware and software. We obtained the machine from a private party. Analysis of the machine, in light of real election procedures, shows that it is vulnerable to extremely serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could also create malicious code that spreads automatically and silently from machine to machine during normal election activities — a voting-machine virus. We have constructed working demonstrations of these attacks in our lab. Mitigating these threats will require changes to the voting machine's hardware and software and the adoption of more rigorous election procedures.

Diebold's response attacked the study on specious grounds¹⁷ and was soundly refuted by Ed Felten in a blistering riposte.¹⁸ Felten also appeared on the *Weekend Edition* program of *National Public Radio* in a discussion of the issues with host Scott Simon.¹⁹

I think that we in the United States should be following the example of the Australian government. There, e-voting machine code has been open for inspection by all and has continued to be improved over the years since its introduction and implementation in voting machines.²⁰ Programmers and security experts interesting in supporting an open-source model for secure e-voting in the United States (and elsewhere) can volunteer for or simply follow the *Trust the Vote* project.²¹

Let's make our votes count; let's not allow proprietary, secret software to undermine what little democracy we still have left – and let's ensure that the disinformation being spread by opponents of democracy doesn't disrupt voting across the country.²²

DATA CORRUPTION IN MEDICAL-INFORMATION SYSTEMS

When data are mission critical, errors or deliberate corruption can lead to serious consequences for patients and staff:

Physicians and computer scientists at the *University of California San Diego* have shown that medical results can be easily modified remotely by attacking the connections between hospital laboratory devices and medical-record systems.

The researchers suggest that these unsecured medical record systems and unsecured medical devices could be putting patient lives at risk.... “As a physician, I aim to educate my colleagues that the implicit trust we place in the technologies and infrastructure we use to care for our patients may be misplaced, and that an awareness of and vigilance for these threat models is critical for the practice of medicine in the 21st century,” Jeffrey Tully, an anesthesiology resident at UC Davis Medical Center, said.²³

An episode of *Law & Order* that I used for several years in my *Cyberlaw & Cybercrime* course²⁴ concerned an angry hacker who kills two patients in a diabetes clinic by tampering with the control systems of their insulin pumps.²⁵ Just to be clear: this was a *fictional* TV show, not a documentary; however, such an attack was perfectly feasible: in 2018, white-hat hackers demonstrated that poorly designed insulin pumps were susceptible to hacks that could potentially kill users; their presentation at a *Black Hat* security conference was instrumental in pushing the manufacturer into fixing the problem even in their older models.²⁶ Ironically, hacking into medical devices became a way for users to save money by improving older insulin pumps to adjust the insulin as a function of blood-sugar levels.²⁷



FIGURE 4.4 Medical informatics.

QUALITY CONTROL, DATA INTEGRITY, AND THE SILLY SEASON

Every now and then we read about errors that we just have to laugh at.

Back in 2009, I received an advertising flier from a major company (politeness accounts for my suppressing the name) that had me in stitches. Here are the bargains advertised in the flier:

- 640 GB internal hard drive: was \$14999; now only \$7999
- 640 GB external hard drive: only \$9999 – Limited time. Limited supply.
- 250 GB external hard drive: was \$14494, now only \$7899
- Super DVD 22X Writer: only \$9999



FIGURE 4.5 Wrong prices.

Amazing what happens when you leave out decimal points, eh? This is a classic example of a failure of data integrity: the figures that went out online were not the data that the sales department

wanted to advertise! What on earth possessed the operations team to allow public display of information without proper vetting?

I wonder how many thousands of customers thought that they had received a blast from the past? When I started work at HP in 1980, our largest disk drive was the HP7925²⁸ which had a staggering capacity of ... [wait for it]... 120 MB. It cost U\$25,000, which in 2023 U.S. dollars would be around \$92,000.²⁹

One of my favorite examples of a spectacular data-integrity blooper occurred in 1999 when for unknown reasons, the BUY.COM online store website listed a \$588 (roughly \$1,000 in 2023 U.S. dollars) *Hitachi* monitor at only \$164.50 — and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The company filled 163 orders using its stock on hand but cancelled the other orders. The potential cost was estimated by the company at \$320,000 (1999 dollars)³⁰ or about \$580,000 in 2023 dollars. The company told all the rest of the eager clients that they were out of luck. They also posted new language on their website addressing the non-validity of erroneous prices.³¹ In October 2000, the company settled a class-action lawsuit by frustrated buyers by paying \$50 to each of the complainants and \$190,000 to the plaintiffs' attorneys for a total of \$575,000 (not counting the cost of the corporation's own legal fees)³² or about \$1,000,000 in 2023 dollars.

Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store had a policy of *underbidding any price on the Net* for particular products and may possibly have used *knowbots* (automated scanning programs) to scour the Web looking for prices of products it was selling. The company's computer seemed to post its lowered price on its website automatically to underbid what it had found — perhaps without human supervision. Talk about a *deadly embrace*!³³

Worse, if any two or more competitors used such automatic price-lowering algorithms, the unsupervised knowbots could very well poison each other's website DBs by repeatedly underbidding each other.³⁴ The same technique could be used deliberately in an information-warfare attack to ruin a competitor. Speculation had it that if the BUY.COM was using an automatic response, then a nasty competitor might deliberately have underbid the BUY.COM price to force it downwards, at least temporarily. A similar attack could drive a posted price higher by allowing the victim's knowbot to define new prices only slightly lower than ridiculously high fake prices posted online.

This example of data corruption from failing to verify the performance of programs should warn everyone involved about the necessity for thorough analysis and thorough real-world testing of new software before it goes into production.

THE MIRACLE OF THE APOSTROPHES

One aspect of data integrity is *consistency* with the originally stored data. When someone goes to the trouble of producing an elegantly formatted memorandum or other document and sends it out to recipients, everyone would like to preserve data integrity by seeing the same appearance on all the systems sharing that document.

Unfortunately, sending formatted messages as the body of emails (as distinct from as attachments) does not guarantee preservation of the exact *appearance* of the source material.

Attractive, well-formatted email messages with boldface, italics, different point sizes and the like usually get transmitted as *HTML* to recipients' mailboxes, where most people's email clients allow the funny-looking code to be reconstituted into something similar to the original.

I say "similar" rather than "exactly like" because *HTML* does not control the final appearance of text on a recipient's system. The codes refer to types, not exact matches, of fonts; thus a sender might want to use, say, 24-point *Arial* as a *Heading 1* display but a particular recipient might have defined *Heading 1* as, say, *Times Roman* 14 point. A two-page original document may appear to be a three-page document to one recipient and a one-page document to another recipient.

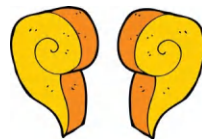


FIGURE 4.6
Apostrophes.

More significantly, though, many people turn off *HTML* email for security reasons. They can automatically convert all such formatted email into plain-text *ASCII* text. The fragment of message below is in plain text as I received it:

Note: The on-line course evaluation system may be used from room, lab and home? anywhere Internet access is available.

Overview: Failure to complete a course evaluation will result in a? hold? being placed on the students? final grades.

When this message was auto-converted to *ASCII*, the apostrophes turned into question marks – probably because the writer was using “curly” characters instead of the straight ones in plain *ASCII*. If you care to prevent this peculiarity if you’re using *MS-Word*, turn off the option in the {*TOOLS* | *AUTOCORRECT* | *AutoFormat As You Type*} screen: uncheck the box labeled {“*Straight quotes*” with “*smart quotes*”}.

In addition, it looks like a dash character may have been in the text in the first line (labeled “Note”) between “home” and “anywhere.” One can turn that conversion off in the same menu referenced in the last paragraph above by unchecking {*Hyphens (–) with dash...*}.

Some people try to send files that should look the same on a recipient system and the originating system by attaching word-processing documents, e.g., *MS-Word DOCX* files, *WordPerfect WPD* files, *Rich Text Format (RTF)* files and so on. Unfortunately, even these attempts don’t necessarily work as planned, since lack of shared fonts, different default paper sizes (different countries may use different sizes) and different printing margins (resulting from installation of different printers) may cause the documents not to look precisely the same on all systems.

So if the exact appearance of a message you are sending via email is critically important to you, you can send the content and its format in a way that is (largely) platform-independent: *Acrobat PDF (Portable Document Format)* files. *PDF* files can include all the characters in the document that are formatted in a particular font.³⁵

Although even they don’t necessarily result in perfect rendition of the author’s intentions across systems, *PDF* files are far more likely to succeed than the other methods mentioned above. You can create *PDF* files in a number of ways; some systems have *Adobe Acrobat* installed so that you can either “print” to an *Acrobat* driver to create the *PDF* files or even just click a toolbar button to do so from within your word processor. Other packages exist that are less expensive (and generally less feature-rich) than the full *Adobe Acrobat* software but nonetheless allow users to create *PDF* files easily. Type “create *PDF*” into a Web search engine to find lots of choices.

If you don’t have access to *Acrobat*, you can always take screenshots and save them as standard image files (e.g., *JPG*, *PNG* and so on) as a last resort for guaranteeing that you are showing exactly how you want the material to appear.

THE PUBLIC-KEY INFRASTRUCTURE SUPPORTS DATA INTEGRITY AND AUTHENTICITY

Electronic mail and electronic documents have become a normal part of today’s business. Unfortunately, signing those documents using *digital signatures* is still relatively rare.

Why should everyone sign operationally critical or sensitive email and other forms of electronic communication?

The problem is that forging messages is ridiculously easy in today’s technical environment. Take word-processing documents, for example. The properties sheet can be filled out anyway you want; it is simple to enter somebody else’s name or somebody else’s company in the appropriate fields. Send such a document to a recipient who assumes that the identification of the author must be correct, and you can have a real problem.

DIGITAL SIGNATURES FOR AUTHENTICATION

In a famous case from the 1990s, a secretary complained of sexual harassment in a large firm. As evidence of systematic discrimination, she presented electronic mail from the company email system showing that her boss had fired her to protect the CEO against her claims of sexual harassment. The email was convincing enough to win a \$100,000 settlement from the company. However, a few months later, records of her boss's cellular phone calls suggested strongly that he had not been in the office when the incriminating email had been written. It turned out that the secretary possessed her boss's email password; she was convicted of perjury for having forged that incriminating message using her boss's email account.³⁶



FIGURE 4.8 Forger.

One obvious lesson is that absolutely nobody should have anyone else's email account password. If one of your users needs to let someone else read and answer their email, you should arrange for proxy privileges so that the colleague can help without being able to forge email pretending to be the normal user of that account.

Another problem that facilitates forgery is the ease with which anyone can forge email headers for Internet delivery. Spammers do this all the time; junk email arrives from countries all over the world – at least, so the headers would sometimes fraudulently indicate. Some criminals use easy forgery to cause trouble for their victims; they insert someone else's reply addresses in offensive or annoying email so that recipients effectively mail-bomb innocent people. The following annotated screenshot

from a spam message I received illustrates the problem (the image is what I posted on Facebook for my students and readers):

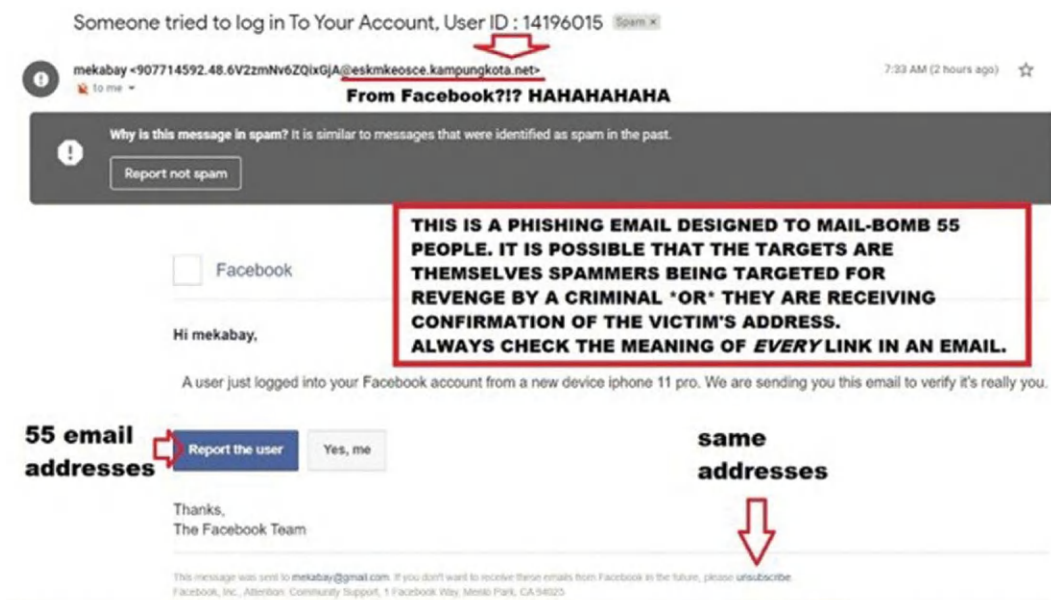


FIGURE 4.9 Spam for mail-bombing.



FIGURE 4.7 Digital signatures.

There was a case in Texas years ago where a clueless junk emailer called Craig Nowak stupidly used the reply address “flowers.com” in his junk email. As a result, the legitimate firm flowers.com received over 5,000 email messages complaining about the junk. The angry CEO of the company, Tracy LaQuey Parker, sued Nowak and won a \$19,000 judgment against him for damage to her company’s good name.³⁷

Until we see authentication integrated into *TCP/IP*, it will be difficult to prevent criminals from forging email sent through the Net. However, with little effort, it is possible to make life harder for forgers. Wherever possible, everyone should sign their electronic messages using a digital signature.

There are many products available that allow every message to be signed so that its integrity and authenticity can be confirmed. Using digital signatures consistently allows an accused reasonably to *repudiate* (deny their authorship of) any message that is not digitally signed with their private key. The sender will not be able to repudiate authorship of these messages unless they claim their key has been compromised. However, honest people need have no fear of *nonrepudiation*. As long as no one has compromised the pass phrase of the private key, no one will successfully forge communications in the user’s name.

One of the free software packages that support encryption and digital signatures is *Gnu Privacy Guard* (GnuPG),³⁸ a successor to the famous *Pretty Good Privacy* (PGP)³⁹ software dating back to its creation in 1991 by the famous computer scientist Phil Zimmerman.⁴⁰ The current version of PGP is *OpenPGP*.⁴¹

At the time of writing, there are (literally) a hundred services already available for signing shared documents without having to sign email; *DocuSign*, *HelloSign*, *PandaDoc* and *eversign* are among the well-established choices.⁴²

There are still problems preventing widespread acceptance of digital signatures. For one thing, most signature software tools do not successfully interoperate with each other. For another, the tools don’t support all commonly used electronic-mail packages. I urge producers of popular cryptographic software to ensure that their digital signatures can be verified by competing products. I also hope that digital signature will become completely automatic for users of popular email and document-preparation software.

OVERVIEW OF PKI

Public key infrastructures (PKI) are the foundation on which the digital signatures and secure Internet transactions are built. The PKI depends on the *Public Key Cryptosystem* (PKC),⁴³ which uses *asymmetric encryption* to provide secure encryption of confidential messages and transactions, to authenticate the origin of such data, and to guarantee data integrity.

For each user, two keys are generated at a time; each can decrypt only what the other encrypts; that is, each key cannot decrypt what it encrypts. One key is kept secret (the *private key*); the other becomes a *public key* known to anyone who wants to use the PKC. To send a message readable only by a specific PKC user, we can encrypt the cleartext with the recipient’s public key; only the corresponding private key can decrypt the ciphertext. Similarly, to *authenticate* the origin of a message, the sender encrypts the cleartext or a randomized extract of the text (a *hash*) using their own secret key. Anyone can then decrypt the message using the sender’s public key – and only that key.

Both of these methods also guarantee the integrity of the cleartext while the ciphertext is in transit, since any tampering with the ciphertext causes errors during verification of the digital signature or decryption of the ciphertext.

However, a PKC depends on trust. For example, in the case of a digital signature, the PKC provides proof only of which *secret key* used to sign a given document. What if a signing key were actually issued to an imposter? What if a person’s secret key were compromised? The PKC can



FIGURE 4.10 Two complementary keys created.

be trusted only if there is a trusted link from a public key to a known individual, organization, or device. It is the chief function of a PKI to document a trustworthy linkage between the ostensible owner of a secret key and that key.⁴⁴

There are many questions raised when discussing the PKI. For example,

- What should a certificate that links identity to a key pair contain?
- How should we validate a public key to prevent spoofing (impersonation)?
- How should we handle revocation (cancellation) of certificates?
- What happens to documents signed with keys that have been revoked?
- Should organizations build their own PKI or use third-party certificate authorities to handle the details of key creation, trust and revocation?
- Can proprietary formats for certificates lead to successful interoperability?
- What are the costs and benefits of third-party PKIs versus in-house PKIs?

CERTIFICATES

In the real world, we are used to many different kinds of *certificates*. For example, we carry passports, drivers' licenses, car registration, employee cards, membership cards, and credit cards.

What is certified by a certificate? Certificates attest to a linkage or an association, an origin or ownership. For example:

- A passport links a person to citizenship.
- A driver's license links a person to the right to drive in a given state.
- The car registration links and automobile, an owner, and the payment of appropriate fees to the states.
- An employee covered links person, and employer, and confers authority.
- A membership card relates a person to an organization and associates that person with a member's rights.
- A credit card links a person, a financial institution, a credit limit, and the right to buy services or products up to that credit limit.
- Similarly, a certificate in a PKI links a person or device to a key pair through the signature of a certificate authority (CA).



FIGURE 4.11 Certificate.

In cyberspace, we accomplish the same purposes as those of real-world certificates using the electronic equivalent. Ford and Baum write,

A PKC certificate is a collection of information to which a digital signature has been affixed by some authority who is recognized and trusted by some community of certificate users.⁴⁵

Any user of a certificate, whether electronic or physical, must be able to answer at least the following questions:

- Whom does the certificate identify?
- What is it certifying?
- Who certified the bearer's identity and the object certified?
- How is the authenticity of the certificate established?

The *Telecommunication Standardization Sector* of the *International Telecommunications Union* (ITU-T) defined the X.500 standard in 1988 for identifying individuals and other entities (e.g., companies, government departments, and even devices such as routers or printers).⁴⁶ This standard used a simple scheme involving the country, organization, and common name to

identify entities; e.g., C=U.S., O=ICSA, CN=Mich Kabay. However, this structure did not guarantee uniqueness. For example, a different person with the same common name (e.g., John Smith) could easily end up working for the same organization at the same time or in the future. More recent versions of the X.500 standard include unique identifiers; organizations can use these fields to insert such elements as employee numbers, Internet email address, Internet domain name, X.400 email address, X.500 directory name, Internet IP address, or any other unique, unambiguous name registered as an object.

The *X.509 version 3* certificate goes beyond the X.500 standard by its provisions for unique identifiers; organizations can use these fields to insert such elements as employee numbers, Internet email address, Internet domain name, X.400 email address, X.500 directory name, Internet IP address, or any other unique, unambiguous name registered as an object.⁴⁷ The *X.509* certificate consists of the following fields:

- Version of certificate format
- Certificate serial number
- Signature algorithm identifier
- Certificate authority (CA) X.500 name
- Validity period (start, expiration)
- Subject X.500 name
- Subject public key info (algorithm, public key)
- Issuer unique identifier (optional)
- Subject unique identifier (optional)
- Extensions
- Certificate Authority's digital signature.

ISSUING, AUTHENTICATING AND TRUSTING A CERTIFICATE

The functional requirements for a PKI include the following:

- Issuing a certificate
- Locating a certificate
- Trusting a certificate
- Renewing a certificate
- Relations among CAs
- Revoking a certificate
- Supporting nonrepudiation of signatures by PKIs
- Scalability
- Interoperability (sometimes)



FIGURE 4.12 Certification.

When a CA issues a certificate, the CA must gather all necessary information, verify the accuracy of that information, create and sign a certificate with the CA's private signing key, send the certificate to its owner, optionally deposit a copy of the new certificate in a public repository, archive the certificate, and record an entry in an audit trail.

What defines the authenticity of a certificate? Users of any certificate must trust the procedures used to authenticate the identity of the certificate. For example, passport offices demand other documents, photographs signed by a photographer and salon. This kind of procedure implies a *chain of trust*; for example, a passport official must trust the signature of the photographer and must trust the authenticity of a birth certificate. The chain of trust assumes that authenticate documents are difficult to forge; in the real world, documents are printed in special formats on recognizable unique paper, have serial numbers that can be verified and a variety of stamps that are presumed to be difficult to duplicate without authorization. In cyberspace, a PKC guarantees strong authentication as

long as the confidentiality of the signing key is protected. However, there is always a possibility of fraud; for example, a stolen passport can be modified by criminals. In the PKC, all confidence in a certificate is lost if the signing key used to authenticate the certificate is divulged.

Authenticating a certificate in a PKI requires access to the signer's public key. The user can either store all public keys needed in a single list or – more likely when documents from strangers have to be authenticated – there has to be a system of *key servers* that can provide public keys securely on demand. As the number of users grows, managing public keys becomes more onerous; therefore, a fully developed PKI naturally involves a directory structure for locating the right keys.

Trusting a certificate always involves following a chain of authentication. For example, suppose Alice and Charlie do not know each other but both know and trust Bob. If Bob signs Alice's public key, Charlie can verify Bob's digital signature on Alice's key; if Charlie assumes that Bob took proper precautions before signing Alice's key, then Charlie can trust Alice's public key. The same principle applies to trusting a passport, a driver's license, and so on.

The chain of trusted signatures can be arbitrarily long. Suppose Dave's key were signed by Alice. Would Charlie trust Dave's key? Yes, since Dave's key was signed by Alice and Alice's key was signed by Bob, and Charlie trusts Bob. This process is known as following the *chain of trust*. It occurs regardless of the particular structure of a PKI hierarchy of signers.

REVOCATION AND EXPIRATION OF CERTIFICATES

There are several models for the relationships among CAs. The most common thus far is the top-down hierarchical structure. Certification flows only downward in this structure; all certificate users must know and trust the top-level CA public key. The main advantages of this model are that there is one and only one certification path for each entity; it is easy to locate these paths; and the structure is consistent with naturally hierarchical organizations and systems. Examples of top-down hierarchical CA structures include:

- SET (*Secure Electronic Transactions*) for VISA & Mastercard
- U.S. Department of Defense MISSI (Multilevel Information Systems Security Initiative)
- PEM (*Privacy Enhanced Mail*), which failed to be accepted as a standard)

A major implication of the top-down hierarchy is that protection of the signing keys becomes increasingly important at higher levels of the hierarchy. A compromised high-level key could destroy trust in a very large number of certificates.

In practice, the top-down hierarchy will likely not be implemented worldwide – or at least, not soon (some say, not without a world revolution); because of national sovereignty considerations, few governments would accept a single root certificate authority that would certify national CAs. Because of the reluctance to have national root CAs certified by a single international authority, it is likely that the global PKI will consist of many independent hierarchies. To enable interoperation, it is likely that national CAs cross-certify — that is, will mutually sign — each other's public keys.

Another model for strengthening trust in public keys is the *Web of trust* (for example, used by PGP and GPG users). PGP and GPG users depend on a manual process for signing each other's public keys. In this model, there is no centralized signing function. The software allows keys to be marked with four different levels of trust. However, there is no formal accountability for bad decisions. A single careless certification of a public key could allow malefactors to hijack other people's identities by signing false public keys.

In yet another function for a PKI, *it may be necessary to stop trusting a certificate*; for example, the secret signing key might be compromised or there could be a change of relationship between the



FIGURE 4.13 Expiration.

certificate bearer and the CA. Announcing that a data certificate is no longer valid is called *revocation*. In addition to revocation for cause, most certificates have a limited period of validity as defined by policy; typically, the longevity of a certificate is measured in months to years and is indicated in a field of the certificate itself.

NONREPUDIATION AND SCALABILITY

Nonrepudiation is familiar from the legal arena; we are used to the legal requirement of accepting responsibility for contracts that we have signed. Similarly, a PKI provides a basis for insisting that a document signed using a particular private key represents acknowledgement by the private-key owner. Repudiation of such a signature necessarily implies immediate revocation of the corresponding public key. So, nonrepudiation depends entirely on the security of the private key; if anyone else has a copy of the private signing key, the owner can legitimately repudiate her signature. Therefore, no one should make a copy of a signing key unless its safety is as strongly protected as that of the original key.

Scalability is the capacity for acceptable performance regardless of size. One of the problems of growth for a PKI is finding a way of verifying a certificate sent by another user; another problem is trusting an increasing number of CAs to follow strict certification policies. In particular, with many governments in the world today consisting of the equivalent of armed criminal conspiracies, national signing authorities cannot automatically be trusted. Scalability is supported by an effective directory structure permitting verification of any public key or certificate and by effective standards enforced by complete records and meticulous audits.

Worldwide interoperability is a long-term goal for e-commerce and communications. However, some PKI hierarchies are deliberately kept from interoperating to make it harder for subversion of their certificates.

PKI SERVICES VS. IN-HOUSE PKIS

One of the biggest questions PKI managers have to answer is whether to use a certification system implemented within their organizations or to use its third-party verification instead.

An external certificate authority has some advantages. The commercial company typically claims to provide 100% availability of operations with high scalability. Certificates are purchased, with volume-based pricing available. The CA functions reside largely in secure facilities with disaster recovery plans, bonded personnel, and independent auditing of the certification procedure. The commercial PKI can offer key backup and recovery, support for *key escrow* (secure storage) of encryption keys (if users choose to trust such escrow), revocation management, multiple directory standards, and interoperability (assuming customers push for this feature). Costs vary widely⁴⁸ with some firms offering individual users services at about \$7 a year and others ranging into the \$100s/year per user. All of these estimates need to factor in the costs of I&A technology, which can run from dozens to hundreds of dollars per user in initial costs (with lower on-going costs) depending on the technology used.

The alternative is to create and manage one's own PKI. The purchaser is responsible for buying software for every client or system. There is a potentially heavy investment in special hardware and



FIGURE 4.14 Non-repudiation.



FIGURE 4.15 PKI certificate.

software. According to some analysts, rolling your own PKI is suitable for organizations who are sure of their direction and do not want to pay per-user fees to a third-party. Costs of in-house PKI are more difficult to estimate; some published studies have found costs of about \$7 per year per user for 500,000 users and up to around \$70 per year per user for 5,000 users. On the other hand, the costs of I&A for in-house access to the PKI are integrated into I&A that the organization has to provide anyway for controlled access to its other IS.⁴⁹

SCUMWARE

In recent years, a new way of abusing computer users has spread like a disease through the Web: *scumware*. In this section, I will describe the functions of scumware; examples of software labeled by this unappealing term; legal issues raised by scumware; and defenses against scumware.

Scumware (sometimes known as *thiefware*) is any software that significantly changes the appearance and functions of web-pages on *users'* computers without permission of Webmasters or copyright holders.⁵⁰ For example, a number of products overlay banner advertisements with other ads, sometimes for competing products. Scumware may add unauthorized hyperlinks to a user's view of a webpage – sometimes using links to possibly objectionable sites. Such programs can interfere with existing hyperlinks by adding other destinations to the intended target. In addition, some products install themselves without warning users of these functions; others bury the details of their Web-page modifications in the extensive legal detail of end-user license agreements. Some scumware is difficult or impossible to control; for example, the programs may be difficult to uninstall, can introduce instability into the operating system, and sometimes conflict with other applications.⁵¹

One of the best-known instances of scumware was better documented than most: the *Microsoft XP Smart Tags*® “feature” was announced as an improvement for *MS-Office* products.⁵² Using *Smart Tags*, specific words in lists could have pop-up menus; these menus could offer options for useful functions such as choosing the style of pasting wanted for text (e.g., formatted, unformatted and so on). *Smart Tags* were also planned for the *MS Internet Explorer* (IE) v6 Web browser; however, many critics argued that the way *Smart Tags* were to be implemented, there would be an opportunity to hijack Web content by showing extra hyperlinks. These extra links would direct users to MS-related sites or to sites which had bought entries in the *Smart Tag* space. There were waves of outrage all over the industry and MS withdrew its proposal for *Smart Tags* in *XP* a few months after the initial proposal.⁵³

SCUMBODY'S CHANGING MY WEB PAGE

Surf and Keep® is an example of a product that adds unauthorized embellishments to webpages:

The *Surf and Keep* browser plugin promises to save time and money whilst shopping online. This browser add-on automatically scans for coupons, deals, and promotions, providing online shoppers with the benefit of comparison and enabling them to purchase products and services that suit their budgets. Note that while such functionality may seem legitimate, many Internet users refer to *Surf and Keep* as a virus or malware. These negative associations are because this browser plugin installs on users' Internet browsers (*Internet Explorer*, *Google Chrome*, and *Mozilla Firefox*) without their consent, and furthermore,



FIGURE 4.16 Scumware.

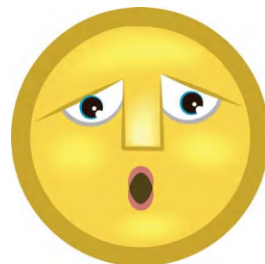


FIGURE 4.17 Who changed my page??

the add-on generates intrusive coupon and deals ads. Unwilling installation of this extension is caused by deceptive free software download websites, which employ ‘download clients’ to monetize their free services.⁵⁴

TopText (also known as *ContextPro*) from eZula was bundled with other software (e.g., the *KaZaa* peer-to-peer file sharing software). This toolkit was a browser plug-in that gave *Internet Explorer* the ability to show additional links in yellow text. The makers defended their product by pointing out that surfers knew what they were getting into if they read the end-user license agreements; that their service successfully provided a legal method for increasing business to their clients; and that their system helped to pay for free services for which users would otherwise have to pay. One commentator labeled this kind of product *foistware*.⁵⁵

Greg Searle reported in RISKS 21.47 on yet another way of annoying Web users. A company called *Fastclick* provided code that hid pop-up windows behind the windows already on screen. These pop-ups remained in place and were revealed only after the victim minimized or closed the other windows on screen – by which time it was difficult to determine where the pop-ups came from. The solution, such as it was, was to disable *JavaScript*; alternatively, if one could locate the offending sites, one could put them on a firewall’s or browser’s exclusion list.⁵⁶

So here’s the essential problem: a Webmaster creates a webpage and includes links and advertisements. Some other company or person provides software to a user that alters the functions and appearance of the webpage before the user can see the intended webpage. Many vendors and users say that it’s the user’s own business what they do to the webpage once it reaches the user’s own computer; however, many Webmasters and other content providers argue that their work is being modified without their permission, violating their author rights.

THE GHOSTS WITHIN

In addition to Web-page modifiers, another variant of scumware makes unauthorized changes in the system registry to alter a user’s home page. For example, there was a pornographic website (now a dead URL) called mycpworld.com that exploited typing errors by people trying to reach mycpworld.com. The rogue webpage forwarded browsers to an offshore website that included a JavaScript module which inserted an undocumented change in the system registry at every system bootup to alter the browser’s home page to the porn site.⁵⁷

I leave the reader to contemplate the consequences if this interference were to occur on an employee’s work computer.

Some forms of scumware intercepted email:

Melbourne-based online marketing company, *Reva Networks*, is currently promoting a new email technology – *Admail* – that allows online advertisers to intercept email messages as they enter the mail server and “wrap” them in advertising content tailored to the recipient’s demographic profile. Unlike conventional unsolicited email, where advertising arrives in the users’ inbox as separate email, *Admail* fuses advertising with the body message regardless of its origin.... Charles Britton, IT policy officer for the *Australian Consumer Association*, is critical of any electronic advertising that places consumers in a reactive position.... Britton doesn’t believe that consumers will passively accept the new form of online advertising. “Without some incentive why would you want advertising in your email?” he said.... Observing the negative reception that spam receives from the Internet community, Britton believes that advertisers may ultimately decide the fate of the technology. “Advertisers are reluctant to be associated with anything that irritates consumers,” he said. “There’s not many successful business models based on annoying people.”⁵⁸

The revanetworks.com domain was last recorded online in the *Internet Archive* in January 2016⁵⁹ and was put up for sale by March 2016.⁶⁰



FIGURE 4.18
Nasty.

Back in 2002, yet another weird data-integrity bug was reported.⁶¹ If you open two *MS-Excel* files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, close file A, and then paste the number into a new file B, you get a value that is identical to what was visible rather than to what was entered in the original cell. Thus, in the example above, if 1.2345 in the source were visible as 1.23, the copy would become 1.23 in the destination worksheet. This can be described as an undocumented, unauthorized data modification, but since it was documented in 2002 and yet was still the case in 2023 (I checked), one can no longer interpret it as an error. It is now an unfortunate feature.

WHOSE WEB PAGE IS IT, ANYWAY?

In this section, I review some of the ethical and legal issues underlying the trouble over scumware. In particular, the question comes down to who owns the image of a webpage when it's in a browser window?

In an interview with Stephanie Olsen in September 2001,⁶² *Gator* chief Jeff McFadden discussed his view of the ad overlays. First of all, said McFadden, *Gator* ads can be moved away from the ad they overlay, and they are clearly labeled as coming from *Gator*. They are no different from any other window that might obscure part of another window. Asked about a popup ad for a credit card that overlay an identically sized ad for a competing credit card, McFadden assured the interviewer that the overlay was popped up because the product deduced that the viewer might be interested in credit cards; the product does not “know” that its ad is overlaying the banner from a competing product.

Why did McFadden launch a lawsuit against the *Interactive Advertising Bureau* (IAB) in August 2001? McFadden told Olsen:

Some IAB representatives made some egregious statements about the company – a little bit of name calling, but mainly telling people that they thought that our ad model was illegal. I spoke to the IAB and they said they weren't interested in retracting those statements. And that can have a pretty substantial impact on our business. We have 200 advertisers, many of them Fortune 500 and Fortune 50 companies, and I just can't have them saying that what they're buying from us is illegal. So we filed the action (last) Monday.⁶³

But how is what scumware does any different from, say, having a user put a *Post-It*TM note on her monitor that obscures part of a webpage? Surely users can do what they want with webpages that have been copied to their own cache?

Well, no, not really.

A look at the IAB's 28 August 2001 press release shows an uncompromising title (caps are in the original):

“INTERACTIVE ADVERTISING BUREAU (IAB) ASSERTS GATOR.COM'S BUSINESS PRACTICES VIOLATE THE CONTRACT, TRADEMARK AND COPYRIGHT INTERESTS OF WEB PUBLISHERS AND ADVERTISERS: UNFAIR COMPETITION AND DECEPTIVE PRACTICES IN VIOLATION OF FEDERAL LAWS.”⁶⁴

Before we go any further, let me warn readers again using the mandatory disclosure that IANAL.⁶⁵

From my point of view as a lay observer, the arguments presented by the IAB and other opponents of scumware boil down to the following (and I am using the generic “scumware” instead of focusing only on *Gator*'s products):

- Scumware makes unauthorized changes in the appearance and content of webpages that can affect more than a single user.

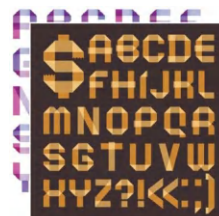


FIGURE 4.19
Overlays.

- The changes imposed by scumware may interfere with contractual relationships between Web content providers and advertisers.
- The introduced advertisements and links may convey a false impression implying relationships and possibly endorsements that do not exist.
- The modifications may be creating an unauthorized derivative work.

From an international perspective, European laws are more restrictive than U.S. laws in defining what are called the *moral rights* of not only a copyright holder but also the rights of the creators of intellectual property. Scumware, under this doctrine, may violate the content-creator's rights of integrity, disclosure, retraction, and replies to criticism. Unauthorized modification of what users see on a webpage may violate all of these rights.⁶⁶

Those opposing scumware will have to articulate why they don't also go after firewalls and ad-blockers that speed up Web access by reducing the amount of graphical data transmitted to a browser. Perhaps one factor reducing the outrage over *blocking* ads is that few seem to be offended by *not* seeing an ad; although the advertisers may not like the idea, at least there is no chance of casting the website in a false light (an important element of the concept of defamation in U.S. jurisprudence).⁶⁷

From a purely ethical (as opposed to narrowly legal) standpoint, it seems to me that scumware is a bad idea on several grounds:

- The people who benefit from the introduced materials (links and ads) are not the people who invested time and money in creating the underlying content; this situation seems unfair.
- If everyone engaged in such behavior, webpages could become cluttered with extraneous matter and obscure the underlying content entirely – just imagine running several different scumware programs at once to see what might result.
- Obscuring other people's messages and adding unauthorized linkages seems disrespectful of the human beings who created the original webpage; such behavior seems to me to be disregarding the Web designers' feelings and intentions.

PREVENTION AND REMOVAL

How do we prevent and remove infestations of scumware?

First, you must decide if you approve of having advertisements and hyperlinks inserted into the views of webpages that appear on your screen. If you do, there's no problem and you can stop reading this section.

For those who don't like the idea of extraneous links and ads, the most obvious measure for preventing infestation is not to install scumware at all. Unfortunately, this is not as easy as one would like. As we have seen in previous sections, scumware can infest other software and be installed with little or no notice to the user. Nonetheless, before installing freeware, shareware, or adware (products that offer services in return for sending the user targeted ads), everyone would do well to read about the product using an Internet search engine.

Check the lists of known scumware to see if the product you are thinking of installing is a known offender.⁶⁸ Without gritting your teeth too hard, read the *end-user license agreement* (EULA). Look for language, no matter



FIGURE 4.20 Removing scumware.

how convoluted or how tiny the point size, that indicates that the product is likely to add to or modify the appearance of webpages you download. In addition, look for language that threatens to delete or inhibit any of your *other* programs.

Back in 2002, we got a fascinating glimpse of the mindset of some adware makers. The *RadLight*® adware product came with a EULA that read in part,

You are not allowed to use any third party program (e.g *Ad-aware*) to uninstall application bundled with *RadLight*. Such programs will be removed.⁶⁹

On *your* computer, you give up the right to apply your choice of *antimalware*?? It sounds like a sick joke.

While you are installing *any* software, from no matter what source, always keep your firewall active if at all possible. Be sure to configure your firewall to alert you to any attempt to contact an external address from inside your system; although such attempts may occasionally be necessary (e.g., for updates to critical components), in many cases they can be blocked safely. You can always study the issue more closely if necessary, by examining the *TCP address* of the target and doing a *reverse IP-block lookup* to find out where the critter is trying to connect. Once you know the name of the registrant and the *Domain Name System* (DNS) entry for the target, block the transmission without hesitation if you don't know why a module on your system is trying to communicate with a site you know nothing about. You can always reverse your decision later if you determine that the connection is in your interest.

To identify and remove undocumented or forgotten adware, spyware and scumware, most anti-malware products today can protect us effectively.

INCOMPETENT USE OF SPREADSHEETS CAN CAUSE PRODUCTION PROBLEMS

A long-standing problem with end-user computing is that tools such as simple DBs and spreadsheets are so easy to use that people with no background or training in computing can apply them to *production* problems (applications on which an organization depends for mission-critical functions or decisions).

The *European Spreadsheet Risks Interest Group* (EuSpRIG) reports on many aspects of spreadsheet usage, including what they call *Horror Stories*; their description reads,

These stories illustrate common problems that occur with the uncontrolled use of spreadsheets. In many cases, we identify the area of risk involved and then say how we think the problem might have been avoided.⁷⁰

An example from October 2020 reported on how the erroneous use of *XLS* files – an old *Microsoft Excel* format – caused errors in processing 16,000 Covid-19 test results in the UK. The unsophisticated users failed to note that *XLS* files could handle only 65,000 rows, in contrast to the million-row capacity of the current *XLSX* format. When they imported valid data in *comma-separated-values* (CSV) files, they lost all but about 1,400 case results. Had they checked their data right away after importing, they would not have lost a week in reporting the results of the tests.⁷¹

A classic example of how failure to verify one's work after making spreadsheet errors occurred in March 2000. Mark Lutton reported in *RISKS* 20.84 on a week-long kerfuffle at the *Massachusetts Institute of Technology* (MIT), when the grades of 22 students in a cell-biology class were randomly altered. Initial suspicions focused on hacking, and the teacher, Harvey Lodish, told his class on March 2, 2000, that he had uncovered a cheating scandal. On March 10, the *Boston Globe* reported



FIGURE 4.21 Spreadsheets.

that in fact a teaching assistant had sorted the student-name column but not all the other ones, thus failing to carry all the data through the sort. Lutton suggested, “It seems to me that bound paper ledger books would be a much better tool for keeping grade records, at least for this teacher and his assistants.”⁷² Some other ideas:

- Enable the *audit-trail* feature (can create large files but does record all changes);
- Keep daily backups with version numbers so that a good version of the data can be located and used quickly.”

In a later issue of the *RISKS Forum Digest*, correspondents Tony Lima and John Pearson both pointed out that the fundamental problem was that the teaching team was using a spreadsheet to do a DB’s job.⁷³ Any DB would have prevented detaching the name field from the other information during a sort.

Unfortunately, beginners rarely think about quality assurance in a systematic way. When I taught beginners how to use office products in the first-year non-majors’ computing course at *Norwich University*, I emphasized the importance of documenting and testing spreadsheets before relying on them. Professor Raymond R. Panko of the *University of Hawai’i* studied the frequency of errors in spreadsheets in real-world applications. His paper, “What We Know About Spreadsheet Errors” provides a statistical *meta-analysis* (aggregating probabilities of the null hypothesis for several experiments) of 13 studies of spreadsheet errors from 1987 through 2004. Prof Panko’s abstract was as follows:

Although spreadsheet programs are used for small ‘scratchpad’ applications, they are also used to develop many large applications. In recent years, we have learned a good deal about the errors that people make when they develop spreadsheets. In general, errors seem to occur in a few percent of all cells, meaning that for large spreadsheets, the issue is how many errors there are, not whether an error exists. These error rates, although troubling, are in line with those in programming and other human cognitive domains. In programming, we have learned to follow strict development disciplines to eliminate most errors. Surveys of spreadsheet developers indicate that spreadsheet creation, in contrast, is informal, and few organizations have comprehensive policies for spreadsheet development. Although prescriptive articles have focused on such disciplines as modularization and having assumptions sections, these may be far less important than other innovations, especially cell-by-cell code inspection after the development phase.⁷⁴

It makes sense to identify *all* production spreadsheets in your organization and to review (or establish) quality-assurance processes to ensure that errors don’t creep into operational data and decisions.

PERSONAL THOUGHTS ON VERIFICATION

When I was a child, I was raised by a demanding father who punished me for making mistakes while he was forcing me to learn math that was years ahead of what my little buddies were studying (e.g., algebra when I was six) – not conducive to popularity among the primary-school crowd, especially when I spoke English with a strong French accent while attending English-language schools. One consequence of my father’s, ah, teaching style was that I learned – the hard way – to check my work before I turned it in to him.

When I reached *McGill University* in 1966, I carried on as I had learned and I remember my astonishment at finding out that other people did not do the same. One day in a chemistry class, for example, I nearly caused a heart attack in another student who was sitting behind me. She said, “You’ve been punching in a lot of numbers on that calculator, haven’t you? How many numbers are you dealing with?” “Oh,” I answered, “I’m summing 1,200 numbers.” “You are adding 1,200 numbers?!?” “Yes – in groups of 100 – and each group twice (once forward and once backward) to be sure I’m entering them right.” She practically fainted. We did become good friends, though!

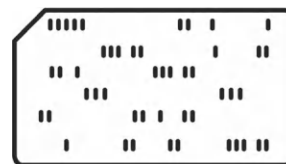


FIGURE 4.22
Hollerith card.

It was shortly after that that I turned to the *FORTRAN* compiler and Hollerith (punched) cards to replace the calculator for that kind of work. In particular, I always numbered the cards using columns 73 to 80, in contrast to some of the less-organized students who discovered how much work it was to sort unnumbered program cards when they dropped their box of cards on the floor. Numbered cards were sortable using the sorting machines, although it was still a nuisance: we had to put the cards in the hopper, sort on column 80, collect the cards from the 10 output stacks, put them back in the hopper, turn a crank to sort by column 79, sort again, and so on. Incidentally, I used to allow for 100 numbers between cards (e.g., 00002700, 00002800) to allow for insertions of additional code.

Turned out that attention to detail and verification proved of immense value to me as a research scientist, programmer, statistician, and teacher. I kept detailed lab notebooks (still have them) with numbered pages (to prevent removal of any records) showing details written in India ink (non-erasable) for every single experiment in my four years of PhD research. Unlike my fellow students, for each experiment I wrote an introduction (with references), materials-and-methods (including diagrams as appropriate), results, analysis and discussion (including ideas for follow-up experiments). When I finished the lab work in my fourth year at Dartmouth, writing the thesis took only a few months and I finished the degree in four years as well as publishing three papers. In contrast, less organized grad students were stuck in the program for five, six or more years.

Strangely, I think that my father's cruel response to mistakes is one of the reasons that I have *never* embarrassed or humiliated students who made mistakes in my courses – I just helped and encouraged them to figure out the roots of their difficulties and solve the problems.

Anyway, enough of this airy persiflage. Could we just all agree to apply some simple quality control for all aspects of our work? Especially the stuff that affects the stakeholders??

ELECTRONIC TRUTH AND LIES

Thanks to unschooled, naïve users who forward anything they receive without even *thinking* about checking for correctness, amateurs and network users often report *false news* or *misinformation* (MISINFO) or deliberate falsehoods (DISINFO) they have received to their friends and colleagues.

As shown in the 2001 outbreak of the *SULFNBK hoax*⁷⁵ (where messages convinced some people to delete a perfectly harmless and useful file out of fear that it carried a virus), hoaxes can convert gullible users into agents of destruction.

In common with most other security specialists, I recommend that every organization explicitly ban distribution of warnings concerning any sort of technical matters to employees except through an authorized channel such as a network-operations center, security team, technical-support group or helpdesk. The policy should also ban circulation of astonishing news and ridiculous offers for instant wealth.⁷⁶ The more astonishing the news, the greater should be our skepticism.

TRANSMISSION WITHOUT ERROR CORRECTION

The *telephone game*⁷⁷ familiar to children from early grade school consists of whispering a phrase to the next person in a chain without verification. It was originally offensively named by racists:

“Chinese whispers” stems from a racist idea in the 1800s that Chinese people spoke in a way that was deliberately unintelligible. It associates the Chinese language with “confusion” and “incomprehensibility.” Now, the game is more commonly referred to as “the telephone game” in the United States.⁷⁸



FIGURE 4.23
False information.



FIGURE 4.24 Telephone game in cyberspace.

The results of never checking what is transmitted include ending up with wildly distorted information reaching later members of the chain— funny for children in an innocent game, but not so funny in real life when it leads to victimization by criminals.

One of the classic hoaxes that did not involve money transfers was the *Good Times Virus*, which surfaced in December 1994:

Here is some important information. Beware of a file called Goodtimes.

Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.⁷⁹

A hilarious spoof of the hoax appeared quickly online from Donald Watrous of Rutgers University and had geeks chortling around the world:

Subject: "Very dangerous" computer virus

Goodtimes will re-write your hard drive. Not only that, but it will scramble any disks that are even close to your computer. It will recalibrate your refrigerator's coolness setting so all your ice cream goes melty. It will demagnetize the strips on all your credit cards, screw up the tracking on your television and use subspace field harmonics to scratch any CD's you try to play.

It will give your ex-girlfriend your new phone number. It will mix Kool-aid into your fishtank. It will drink all your beer and leave its socks out on the coffee table when there's company coming over. It will put a dead kitten in the back pocket of your good suit pants and hide your car keys when you are late for work.

Goodtimes will make you fall in love with a penguin. It will give you nightmares about circus midgets. It will pour sugar in your gas tank and shave off both your eyebrows while dating your girlfriend behind your back and billing the dinner and hotel room to your Discover card.

It will seduce your grandmother. It does not matter if she is dead, such is the power of Goodtimes, it reaches out beyond the grave to sully those things we hold most dear.

It moves your car randomly around parking lots so you can't find it. It will kick your dog. It will leave libidinous messages on your boss's voice mail in your voice! It is insidious and subtle. It is dangerous and terrifying to behold. It is also a rather interesting shade of mauve.

Goodtimes will give you Dutch Elm disease. It will leave the toilet seat up. It will make a batch of Methanphedime in your bathtub and then leave bacon cooking on the stove while it goes out to chase gradeschoolers with your new snowblower.

Listen to me. Goodtimes does not exist.

It cannot do anything to you. But I can. I am sending this message to everyone in the world. Tell your friends, tell your family. If anyone else sends me another E-mail about this fake Goodtimes Virus, I will turn hating them into a religion. I will do things to them that would make a horsehead in your bed look like Easter Sunday brunch.⁸⁰

RESOURCES FOR VERIFICATION

One of the best resources for checking on the veracity of startling information and warnings circulating on the Internet and even in popular news media is [SNOPES.COM](https://snopes.com). The description summarizes its history and mission:

Snopes is the Internet's definitive fact-checking resource.

When misinformation obscures the truth and readers don't know what to trust, Snopes' fact-checking and original, investigative reporting lights the way to evidence-based and contextualized analysis. We always link to and document our sources, so readers are empowered to do independent research and make up their own minds.

Snopes got its start in 1994, investigating urban legends, hoaxes, and folklore. Founder David Mikkelsen, later joined by his wife, was publishing online before most people were connected to the Internet. As demand for reliable fact checks grew, so did Snopes. Now it's the oldest and largest fact-checking site online, widely regarded by journalists, folklorists, and readers as an invaluable research companion.⁸¹

Everyone from children to employees to elders *must* be educated to *check for fraud* before forwarding terrifying information about anything computer related.

DISINFORMATION ABOUT THE COVID-19 PANDEMIC

As the COVID-19 pandemic spread throughout the world, two kinds of bad information became widespread:

- Misinformation (MISINFO) – mistakes honestly believed by the originators;⁸²
- Disinformation (DISINFO) – lies promulgated deliberately for ulterior purposes.⁸³

According to the World Health Organization, misinformation can be life-threatening:

Acting on the wrong information can kill. In the first 3 months of 2020, nearly 6 000 people around the globe were hospitalized because of coronavirus misinformation, recent research suggests. During this period, researchers say at least 800 people may have died due to misinformation related to COVID-19.

At its extreme, death can be the tragic outcome of what the *World Health Organization* (WHO) has termed the *infodemic*, an overabundance of information — some accurate, some not — that spreads alongside a disease outbreak. False information runs the gamut, from discrediting the threat of COVID-19 to conspiracy theories that vaccines could alter human DNA.

Though they aren't new, in our digital age infodemics spread like wildfire. They create a breeding ground for uncertainty. Uncertainty in turn fuels skepticism and distrust, which is the perfect environment for fear, anxiety, finger-pointing, stigma, violent aggression and dismissal of proven public-health measures – which can lead to loss of life.⁸⁴

One of the best sources of accurate information countering COVID-19 DISINFO⁸⁵ is from the CISA DHS.



FIGURE 4.25

Fact-checking resource.

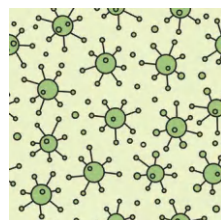


FIGURE 4.26

COVID-19 virus.

SOCIAL MEDIA AND INTERMEDIATION

As the spread of MISINFO and DISINFO about vaccination spread during the COVID-19 pandemic, an increasing number of voices joined a growing movement focusing on the role of social media. A shocking analysis of the sources of anti-vaccination lies and distortions revealed the main sources for the false news: a mere dozen people were found to have posted thousands of instances of dangerous incorrect information on major social media (Facebook, Instagram, and Twitter).

Spreading unfounded claims without controls is an example of *disintermediation*: the essence of gossip.

One researcher, Imran Ahmed, CEO of the *Center for Countering Digital Hate* said, “The ‘Disinformation Dozen’ produce 65% of the shares of anti-vaccine misinformation on social media platforms. These agents are opposed to vaccination and some sell products and literature. Some of the claims included denial that COVID is real; others attacked the medical establishment as peddlers of fake treatments for profit. Ahmed said, “Many of the 12...have been spreading scientifically disproven medical claims and conspiracies for years.”⁸⁶

Controlling content on private communications resources is called *intermediation*:

...[D]igital intermediation incorporates the agency of platforms, social media influencers and increasingly algorithms.... Digital intermediation that combines both social influencers and algorithms... acts as a visibility process for media content across emerging networked platforms.⁸⁷

The U.S. Administration voiced concerns in July 2021 about the lack of intermediation on social media to restrict pandemic DISINFO and argued for stricter legal consequences for uncontrolled distribution of lies and distortions:

Social media giants should be held accountable for publishing misinformation, the White House’s communications director said Tuesday.

The comments are the latest from the Biden administration in a tiff over whether or not social media companies, specifically *Facebook*, are harming users by showing COVID-19 vaccine misinformation.

When asked by MSNBC’s Mika Brzezinski whether these companies should be held liable for publishing false information that causes people harm, Kate Bedingfield said the administration is reviewing policies. That could include amending the *Communications Decency Act*, or Section 230 of the act.

“We’re reviewing that, and certainly they should be held accountable,” Bedingfield said. “And I think you’ve heard the president speak very aggressively about this. He understands this is an important piece of the ecosystem.”⁸⁸

In July 2023, Republicans managed to convince a rightwing federal judge to block federal agencies such as the DHS, the FBI, and the CISA from communicating directly with social-media companies to warn them of MISINFO or outright DISINFO. The ruling, quickly challenged by the federal government, claimed explicitly that having government agencies *identify lies* by reporting them to social media is a violation of the free-speech guarantees of the First Amendment of the US Constitution.⁸⁹

The notion that DISINFO and MISINFO are to be protected under the First Amendment has a complex history. The distinguished Professor of cyberlaw Eugene Volokh of the UCLA School of Law published a thorough analysis in October 2022 about the issues. The introduction to his article⁹⁰ (minus his references) summarizes the issues:



“I decided to stop complaining and start gossiping.”

FIGURE 4.27 Spreading lies without intermediation.

Sometimes lies are constitutionally punishable: Consider libel, false statements to government investigators, fraudulent charitable fundraising, and more.... (I speak here of lies in the sense of knowing or reckless falsehoods, rather than honest mistakes.).... This, of course, borrows from the Supreme Court's formulation, treating "deliberate or reckless falsehood" or "the knowingly false statement and the false statement made with reckless disregard of the truth" as interchangeable with "calculated falsehood," "the known lie," and "the lie, knowingly and deliberately published."

But sometimes even deliberate lies are constitutionally protected. In *New York Times v. Sullivan*, the Court held that even deliberate lies (said with "actual malice") about the government are constitutionally protected.... This is separate from the more famous holding of *Sullivan*, which is that honest errors (but not deliberate lies) about government officials are constitutionally protected.... And in *United States v. Alvarez*, five of the justices agreed that lies "about philosophy, religion, history, the social sciences, the arts, and the like" are generally protected....

The Supreme Court hasn't explained where the line is drawn, and that leaves unclear where important areas of controversy—such as laws punishing lies in election campaigns—should fall....

Professor Volokh explicitly discusses the assertions by the courts that allowing governments to challenge what *they* define as falsehoods – even in matters of science – is dangerous:

What makes this categorical immunity as to science and history, though, is precisely that there is an institutional academic system with the ability and the incentive to deal with these questions. On one hand, this system benefits from the freedom to make false statements, since that freedom also frees people to make claims that are true but appear at first to be incorrect; or to make claims that prove to be partly false but partly true; or even to make claims that are entirely false but for which the process of disproving them produces important insights—all of which have been familiar phenomena in the history of science.

It is important to understand that publishers, including social media, are in *no way* restricted in determining whether to remove erroneous information, hate speech, or any other material that violates their explicit terms of service. Indeed, when anyone asks to "friend" me on Facebook, I send them my rules of behavior:

Hi!

Delighted to welcome you to my Facebook page!

Rules for participating in my Facebook page:

- I encourage well-written postings even when I disagree with their content; however, I do not tolerate postings that express bigotry such as racism, misogyny, homophobia and other prejudices.
- Stick to the topic in discussions of a posting.
- Provide evidence where possible to support your position.
- Don't post disinformation (claims that aren't true such as anti-vaxxer propaganda or Trumpist lies).
- Don't use ad hominem attacks on other posters on the page when you disagree with them.
- Don't use obscenities and vulgarities.
- I delete offensive posts and send a warning about them to the writer.
- I block people who persist in violating the rules for MY page.

Have fun!

Mich

Finally, even with judicial rulings preventing government agencies from communicating with social media and publishers directly, nothing is preventing those agencies from distributing their

corrective information to the public at large. And if the social media executives and publishers have any sense, they will be reading that information carefully and acting responsibly.

CONSPIRACY CULTS

Outlandish claims can generate acolytes who reinforce each other's beliefs in defiance of countervailing evidence. Conspiracy-cult members can switch from one outlandish belief to a contradictory one, tolerate, welcome and praise abuse, and commit crimes in obedience to or worship of their leaders. Many (not all) cult members are impervious to fact or logic that challenge their beliefs, and some kill others or themselves as a result of their delusions.⁹¹



FIGURE 4.28 Cultists.

One of the dangerous cults that developed into a significant political force in the United States during the reign of the Fascist Orange Narcissistic Sociopath and his deluded acolytes (2016–2020) was *QAnon*. Popularized on the *4chan*⁹² unrestricted communications site, the bizarre and evolving set of lies apparently started modestly. NBC News published a report in 2018 with details of the history:

In November 2017, a small-time YouTube video creator and two moderators of the *4chan* website, one of the most extreme message boards on the Internet, banded together and plucked out of obscurity an anonymous and cryptic post from the many conspiracy theories that populated the website's message board.

Over the next several months, they would create videos, a *Reddit* community, a business and an entire mythology based off the *4chan* posts of “Q,” the pseudonym of a person claiming to be a high-ranking military officer. The theory they espoused would become *QAnon*, and it would eventually make its way from those message boards to national media stories and the rallies of President Donald T****.

....

QAnon is a convoluted conspiracy theory with no apparent foundation in reality. The heart of it asserts that for the last year [2017] the anonymous “Q” has taken to the fringe Internet message boards of *4chan* and *8chan* to leak intelligence about T****’s top-secret war with a cabal of criminals run by politicians like Hillary Clinton and the Hollywood elite. There is no evidence for these claims.

In addition..., the theory has been increasingly linked to real-world violence. ...*QAnon* followers have allegedly been involved in a foiled presidential assassination plot, a devastating California wildfire, and an armed standoff with local law-enforcement officers in Arizona.

Now [2018], the people behind that effort are at the center of a fractious debate among conspiracy enthusiasts, some of whom believe the three people who first popularized the *QAnon* theory are promoting it in order to make a living. Others suggest that these original followers actually wrote Q’s mysterious posts.”⁹³

It may be easy to dismiss and ridicule the nonsense peddled by followers of *QAnon*, but by May of 2021, the cult had definitely penetrated mainstream politics. Researchers found that

About one-quarter of Republicans, 23%, agree with a set of conspiratorial beliefs linked to the *QAnon* movement, according to a PRRI [*Public Religion Research Institute*] report.... These believers said they mostly or completely agreed that “the government, media, and financial worlds in the U.S. are controlled by a group of Satan-worshipping pedophiles who run a global child sex trafficking operation,” that “there is a storm coming soon that will sweep away the elites in power and restore the right-ful leaders,” and, finally, that “because things have gotten so far off track, true American patriots may have to resort to violence in order to save our country.” Among the full American public, 14% mostly or completely agree with all those statements, with a broad majority saying they disagree.⁹⁴

In the public sphere, our educational systems must increase their focus on critical thinking if we are to escape the mental pollution of MISINFO and DISINFO:

...[A] study exposed thousands of young people to some true messages and some false ones, similar to those they may see on social media. The study confirmed that greater knowledge about the topic of a message did not in itself improve judgments of accuracy However, participants who had many prior media-literacy learning experiences provided more accurate responses when they were exposed to a post containing misinformation and an evidence-based post. This means that media literacy education helps people reject misinformation.⁹⁵

A funny set of interviews from 2024 by the *Jimmy Kimmel* crew demonstrated that some people can hold contradictory views of behavior depending on whom they think is being referenced.⁹⁶

NOTES

- 1 [Government of Australia Competition and Consumer Commission \(2018\)](#).
- 2 [Brennan Center for Justice \(2023\)](#).
- 3 [Vermont Legislative Joint Fiscal Office \(2023\)](#).
- 4 [City of Montpelier \(2023\)](#).
- 5 [City of Montpelier \(2023\)](#).
- 6 [Government of Vermont \(2023\)](#).
- 7 Benzinga (2010).
- 8 Tideman (2001).
- 9 Anderson (2006).
- 10 Hamilton (1998).
- 11 Nichols, Kabay, and Braithwaite, *Writing Secure Code* (2014).
- 12 Scarfone, Mell, and Souppaya (2014).
- 13 Levine, Mason, and Hadley (2014).
- 14 Linders (2015).
- 15 For a hilarious commentary on e-voting machines, readers can watch a video from 2006 (Wright, 2006).
- 16 Feldman, Halderman, and Felten (2006).
- 17 Byrd (2006).
- 18 Felten (2006).
- 19 Simon (2006).
- 20 Zetter (2003).
- 21 Macharyas (2019).
- 22 [Sanchez \(2022\)](#).
- 23 Kirsh (2018).
- 24 Kabay, CJ3341/IA241 Cyber and Cybercrime course (2014).
- 25 Wolf, Chernuchin, and Balcer (1993).
- 26 Newman (2019).
- 27 Brown (2019).
- 28 Hewlett-Packard Company (1983).
- 29 [CoinNews Media Group Company \(2023\)](#).
- 30 Huffstutter (1999).
- 31 Sprenger (1999).
- 32 Computerworld (2000).
- 33 Meehan (2001).
- 34 Adar (1999).
- 35 Vlahos (2020).
- 36 Associated Press (1997).
- 37 Craddock (1997).
- 38 GnuPG Project (2021).
- 39 Petters (2020).
- 40 Zimmermann (n/a).
- 41 OpenPGP Working Group (n/a).

- 42 Software Advice (2021).
- 43 Cobb and LeFrançois (2014).
- 44 Chokhani, Peterson, and Lovaas (2014).
- 45 Ford and Baum (1997).
- 46 International Telecommunications Union (2019).
- 47 Cooper et al. (2008).
- 48 Pickavance (2021).
- 49 Olenski (2015).
- 50 Rouse, M. (2013). "Scumware." Techopedia. Available at: <https://www.techopedia.com/definition/13253/scumware>
- 51 Gibbs, What to do about scumware? (2003).
- 52 Microsoft (2001).
- 53 ZDNet Editors (2001).
- 54 Meskauskas (2015).
- 55 [CEXX.ORG](#) (n/a).
- 56 Searle (2001).
- 57 Spector (2002).
- 58 Colley (2001).
- 59 REVA Networks (2016).
- 60 [revanetworks.com](#) (2016).
- 61 Brent (2002).
- 62 Olsen, Nobody's going to skin this Gator (2001).
- 63 Featherly (2001).
- 64 Interactive Advertising Bureau (2001).
- 65 I am not a lawyer and this is not legal advice. For legal advice, seek an attorney specializing in the particular aspect of the law that is relevant to your needs.
- 66 Fasoldt (2001).
- 67 [Cornell Law School](#) (2022).
- 68 [SCUMWARE.ORG](#) (2021).
- 69 McWilliams (2002).
- 70 EuSpRiG (2020).
- 71 Kelion (2020).
- 72 Lutton (2020).
- 73 Lima and Pearson (2000).
- 74 Panko (1998).
- 75 Mikkelsen (2008).
- 76 HTML Blog (2020).
- 77 McIlroy (2021).
- 78 Fernando (2018).
- 79 U.S. Department of Energy Computer Incident Advisory Capability (1995).
- 80 Watrous (nd).
- 81 Snopes Media Group (2021).
- 82 Merriam-Webster (n/a).
- 83 Merriam-Webster (n/a).
- 84 World Health Organization (2021).
- 85 U.S. Cybersecurity and Infrastructure Security Agency (2021).
- 86 Bond (2021).
- 87 Huthinson (2018).
- 88 Bursztynsky (2021).
- 89 [Reuters](#) (2023).
- 90 [Volokh](#) (2022).
- 91 Heller (2021).
- 92 Dewey (2014).
- 93 Zadrozny and Collins (2018).
- 94 Edwards-Levy (2021).
- 95 Zucker (2019).
- 96 Kimmel (2024).

WORKS CITED

- Brennan Center for Justice. (2023, n/a n/a). *The Myth of Voter Fraud*. Retrieved May 1, 2023 from Brennan Center | Issues: <https://www.brennancenter.org/issues/ensure-every-american-can-vote/vote-suppression/myth-voter-fraud>
- City of Montpelier. (2023, nd). *Home Page*. Retrieved July 9, 2023 <https://www.montpelier-vt.org/>
- City of Montpelier. (2023, nd). *Welcome to Montpelier*. Retrieved July 9, 2023 <https://www.montpelier-vt.org/551/Welcome-to-Montpelier>
- CoinNews Media Group Company. (2023, n/a n/a). *US Inflation Calculator*. Retrieved May 1, 2023 <https://www.usinflationcalculator.com/>
- Cornell Law School. (2022, December nd). *False Light*. Retrieved July 9, 2023 https://www.law.cornell.edu/wex/false_light
- Government of Australia Competition and Consumer Commission. (2018, January 04). *Overpayment Scams*. Retrieved July 9, 2023 <https://www.scamwatch.gov.au/types-of-scams/product-and-service-scams/overpayment-scams>
- Government of Vermont. (2023, May 8). *House Committee on Government Operations & Military Affairs*. Retrieved July 9, 2023 <https://legislature.vermont.gov/committee/detail/2024/14>
- Kimmel, J. (2024). *Marjorie Taylor Greene Begs Christian Women to Stop Sexualizing Themselves & We Prank Trumpers!* Starts at 8:39. Retrieved February 24, 2024 <https://www.youtube.com/watch?v=FAFbOK0luE4&t=1s>
- Reuters. (2023, July 4). *Judge restricts White House Communications with Social Media Companies*. Retrieved July 11, 2023 <https://www.theguardian.com/us-news/2023/jul/04/judge-restricts-white-house-communications-with-social-media-companies>
- Sanchez, G. R. (2022, July 26). *Misinformation is Eroding the Public's Confidence in Democracy*. Retrieved July 9, 2023 <https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/>
- Vermont Legislative Joint Fiscal Office. (2023, January 12). *Vermont's Population Estimates by Age Group: 2021 Compared with 2010*. Retrieved from Government of Vermont: https://ljfo.vermont.gov/assets/Subjects/Demographics/a9239392f8/VT_population_2021_vs_2010.pdf
- Volokh, E. (2022, October 19). *When Are Lies Constitutionally Protected?* Retrieved July 11, 2023 from Knight First Amendment Institute at Columbia University: <https://knightcolumbia.org/content/when-are-lies-constitutionally-protected>
- Watrous, D. (nd, nd nd). *WWW Page of Donald Watrous*. Retrieved July 9, 2023 <https://people.cs.rutgers.edu/~watrous/goodtimes-spoof.html>

5 Authenticity

Authenticity of data refers to correct attribution of the origin and nature of the data. Thus if a thief forges a false signature on a stolen check, that's a violation of authenticity. If data are stored in a DB in a field called "tax owed" but are actually about tax *paid*, that's a violation of authenticity too.

This chapter looks at the following aspects of authentication:

- Fundamental principles
- Spam as a key example of violations of authenticity
- Theft of identity including frauds using fake identities
- Hijacking Web pages using false authentication
- Legal aspects of forged email headers



FIGURE 5.1
Avoiding fakes.

A common abuse of authenticity is products using fake trademarks. One of the most egregious is the companies selling counterfeit US stamps; I worked on a project to collect and report hundreds of Websites advertising on Facebook about such forgeries, which are illegal to make, sell or use.¹

The most common issue involving authenticity is using a victim's identification as the source of information. Criminals who send imaginary invoices from PayPal from GMAIL addresses are violating authenticity by pretending to work for PayPal.

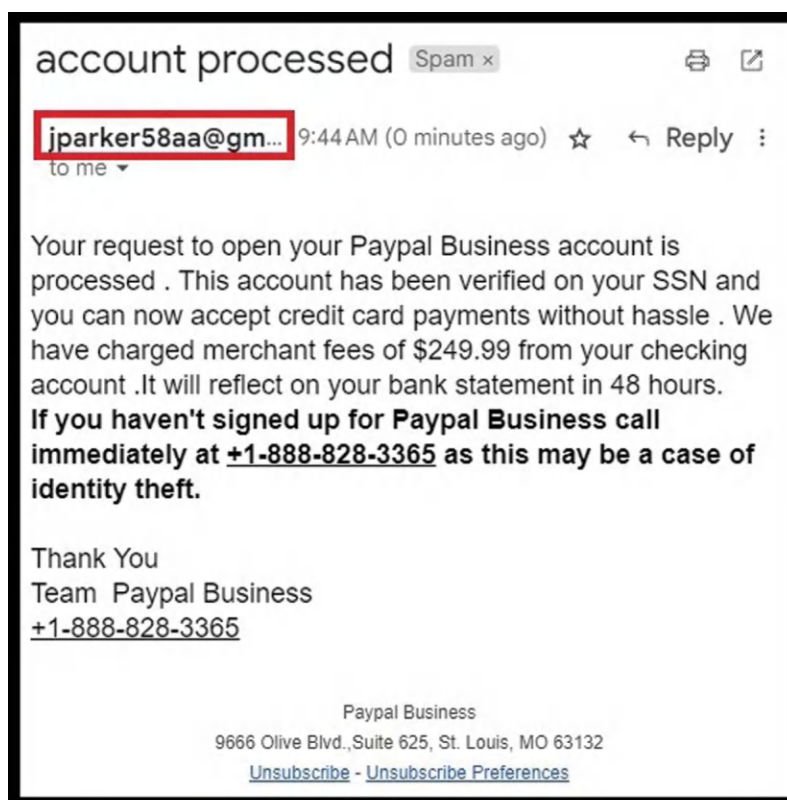


FIGURE 5.2 Fake invoice.

Practically everyone already knows that the four fundamental mechanisms for binding social identity to user identifier (ID) are as follows:

- *What you know that no one else knows*: Passwords or passphrases such as nonsense strings or supposedly private information (e.g., your first love's pet name).
- *What you are that no one else is (static biometrics)*: Characteristics of your body such as retinal patterns, iris patterns, hand geometry, fingerprints, facial features, height-to-weight ratio.
- *What you do that no one else does the same way (dynamic biometrics)*: For example, dynamics of voice, speech, signatures and typing.
- *What you have that no one else has (tokens)*: For example, your mobile phone, keys, passcards, badges, photo IDs, or anything unique or nearly unique that is difficult to obtain or counterfeit.

I'm not going to go into the details of these systems in this section. There are plenty of reviews^{2,3} available summarizing the features and benefits of systems using these approaches to authentication. Estimates of costs are variable, and some of the reports are produced by companies selling the solutions.^{4,5}

Passwords don't work very well for crowds. Tokens are used all the time – consider airline tickets and passports – but in today's digital scanning and printing world, they are easy to counterfeit. Biometrics are particularly useful because under normal circumstances, people don't alter their fingerprints, iris patterns, and ear shapes very often. Faces are also useful, but as anyone my age knows, those *do* change over time!

For increased security, systems can implement *multi-factor authentication* to make breaches less likely. A common method these days is to use codes sent to a registered mobile phone in addition to user-ID and password.



FIGURE 5.3 Multi-factor authentication.

FACIAL RECOGNITION: IDENTIFICATION AND AUTHENTICATION

One problematic biometric technology that allows automatic session initiation *and* termination is face recognition. Some camera-based facial-recognition systems can correctly detect not only the arrival but also the *departure* of an authorized user:

To enhance security when a user is logged on and the lock is unlocked, NeoFace Monitor® is also equipped with a continuous surveillance function that periodically performs facial recognition during use and automatically activates the lock when necessary.⁶

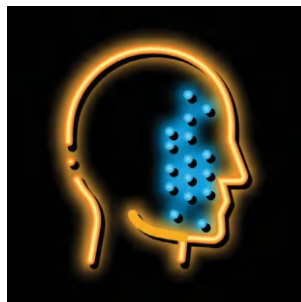


FIGURE 5.4 Facial recognition.

Unfortunately, a report in 2004 by Jonathan Krim of the *Washington Post* pointed out that facial recognition systems using photographs can have serious problems:

... [F]ederal researchers who have tested face-recognition technology say its error rate is unacceptably high – up to 50 percent if photographs are taken without proper lighting.⁷

An *American Civil Liberties Union* (ACLU) report from 2002 revealed that in face-recognition trials at the Palm Beach Airport,

...the system failed to match volunteer employees who had been entered into the DB fully 503 out of 958 times, or 53 percent of the time.⁸

In addition, facial-recognition systems have unfortunately been trained using racially skewed test populations, resulting in significant differences in accuracy of recognition applied to people of different races and genders:

Face recognition algorithms boast high classification accuracy (over 90%), but these outcomes are not universal. A growing body of research exposes divergent error rates across demographic groups, with the poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old. In the landmark 2018 “Gender Shades” project, an intersectional approach was applied to appraise three gender classification algorithms, including those developed by *IBM* and *Microsoft*. Subjects were grouped into four categories: darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males. All three algorithms performed the worst on darker-skinned females, with error rates up to 34% higher than for lighter-skinned males.... Independent assessment by the ... NIST has confirmed these studies, finding that face recognition technologies across 189 algorithms are least accurate on women of color.⁹

Iris recognition is another biometric technology that has required some cooperation by the subject. However, the technique’s accuracy is almost perfect:

New iris recognition accuracy benchmarking from NIST is out, and NEC has claimed the top accuracy rate, at 99.59 percent for 1:N identification for images with both eyes from 500,000 people.¹⁰

Ear biometrics are also being studied as a possible basis for authentication; recent studies suggest accuracy can be in the same range as that of iris recognition:

A paper written by the three researchers claims that a deep network model can accurately recognize people by their ears at least 96.99 percent of the time.¹¹

So unfortunately for us in the snow belt, earmuffs may eventually be seen as threats to security.

PROBLEMS WITH PASSWORDS

I detest passwords. Why do I loathe passwords as a method for authentication? Let me count the ways:

1. Most systems allow users to choose their own passwords. Most users have no clue how to choose passwords that will resist even the mildest guessing based on elementary research of their interests (family, hobbies, pets, favorite sports teams) that may be posted on social media or simple dictionary-based attacks (ordinary short words). Many users choose the word “password” or their own name as their password.¹²
2. If the system applies filters to passwords to impose content and structure requirements (e.g., minimum length, inclusion of numbers or special characters, exclusion of words in a dictionary) then too many users use the same password over and over and for every possible application requiring a password including their external email, offshore gambling sites, auction sites, book clubs, and pornography vendors. Compromise of any one of those sites can easily lead to compromise of all of the user’s information from multiple sites.¹³
3. Reasonable system administrators require periodic changes of passwords; however, untrained (paranoid?) system administrators may force changes of passwords so often that the users become desperate because they keep forgetting their passwords. One expert reported,

...[T]here is a lot of evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily. Unless there is reason to believe a password has been compromised or shared, requiring regular password changes may actually do more harm than good in some cases.¹⁴

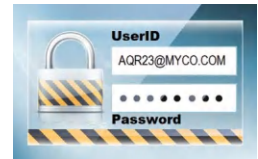


FIGURE 5.5
Password authentication.

4. Users faced with demands for overly frequent changes of passwords may adopt a policy of using the same password all the time, or possibly changing a single number in the password, e.g., *rAm#o8Blu2*, *rAm#o8Blu3*, *rAm#o8Blu4*, and so on.
5. Some administrators make the mistake of having a single day (e.g., once a month) on which all passwords expire; they thus create a flurry of interventions as support staff help users who have forgotten their new passwords.
6. Some users share their passwords with anyone who asks, e.g., technical support staff, the guy in the next cubicle, and even complete strangers on the street who offer them a chocolate¹⁵ or nothing at all. Shared passwords can open the original user to investigation or prosecution if the secured resources are misused.¹⁶
7. If the system applies password histories to prevent reuse of passwords on a particular system, some users unfortunately write their passwords down on scraps of paper and stick them to every available surface, often with helpful identifying notes such as, "Password for accounting system." Users are known to post such revealing sticky notes on their terminals, under their keyboards, under their chairs.... I was personally called in as a consultant in a case at a high school where a sysadmin actually posted the user ID and password for the *admin* account on the backs of terminals in a student computer lab; that information led to the dismissal of charges of academic dishonesty leveled against a particular student who had the misfortune to be a user of that lab when a misuse of the admin account was discovered.
8. Some system administrators still leave their password files accessible to any eight-year-old who wants to run a password cracker for fun and profit. A very few still use unencrypted password files.¹⁷
9. Many system administrators still receive no (or ignore any) real-time alert when attackers try online password guessing, especially if the attacker uses *slow scans* that attack many different user IDs, but only one at a time, over many hours or days.
10. Some system administrators still believe that inactivation of user IDs under password-guessing attack is a reasonable response; they thus hand their system over to attackers for a simple DoS: the attackers can simply try every account with a single dummy password that meets the minimum requirements of the authentication rules (e.g., *YoU*r%idJut5*). Admittedly, most system administrators understand that requiring manual intervention to reset a lost account is not the cleverest policy in the world; therefore, they configure their systems to have a reasonable timeout (e.g., a few minutes) that can double for each incorrect password submission. Such delays make exploring the password space effectively impossible for the attackers.
11. Sometimes organizations send users both their user ID and their password in the same unencrypted message, making it too easy for accidental or deliberate interception to break security.
12. In environments where time pressure is extreme, some users bypass the nuisance of constant logon/logoff cycles by having workstations logged on every morning by whoever gets there first and then simply using that session all day. Such abuse severely impedes investigation of errors because of the lack of an accurate audit trail. In multiple security audits of hospitals over several decades, I have repeatedly found workstations logged in for *days* by the same user ID that initiated the session. Doctors, nurses and technicians use those sessions without realizing how they may be interfering with proper analysis of potentially life-threatening errors.

HIDDEN COSTS OF PASSWORDS

In my practice, I have talked with many users who focus on their individual experience and needs rather than on corporate security management; they often think that passwords are free. Indeed, password functions come with our operating systems and much of our software; we don't have to pay anything extra to buy this form of authentication. Unfortunately, nothing seems to be entirely free! Both common sense and research findings support the view that authenticating identity using passwords is a significant expense for organizations.

The major issue is forgotten passwords. Users who lose track of their passwords may have access to an automated password-resetting process, in which case costs may be modest. A widely used approach simply sends an email to the authorized email address of the forgetful user and then has the user answer a number of these to authenticate to the system. Typically, the system sets up a one-way encrypted DB of personal information questions and answers input by the user and randomly pops up one or two questions for authentication.

Even this process has a modest cost that depends on the cost per minute of salary and extended costs (relating to costs of facilities, supplies, services and their financing) for the forgetful employee's time. Someone earning, say, \$120,000 a year (for 2,000 hours of work) might be costing the employer around \$1 per minute of delay just in salary; the costs of that employee's office space, share of utilities, and so on would be added to compute the overall cost.

The cost grows if the helpdesk gets involved – for instance, if the befuddled user can't remember their own answers to the authentication questions. If there's a lag in responding to the emergency call, in addition to the cost of the helpdesk personnel's time (which one can either include or discount as being paid anyway, depending on the point of view), the big cost begins to be the ticking clock as the locked-out user waits for a reply. For the \$1/minute employee mentioned above, a five-minute wait twiddling their fingers amounts to \$5 of wasted costs – but a half-hour delay is \$30 overall (employee salary and overhead plus helpdesk operations costs).

A 2019 report on helpdesk costs included this information:

While the output of service desks varies widely, here are a few average numbers:

- Across North America in 2016, the average ticket cost was \$15.56, with a low of \$2.93 and a high of \$46.69.
- Similarly, the cost per minute of service desk handle time averaged \$1.60, with a minimum of 76¢ and a max of \$2.50.
- In 2018, the cost per minute of service desk voice time was \$2.13 on average.¹⁸

Multiply the cost per incident by the average number of times people forget their passwords in the organization and the costs begin to rise significantly. At some point, tokens and biometrics begin to seem less expensive, comparatively, than they seemed at first glance.

CHANGING PASSWORDS

In my experience, most security administrators have figured out that having all the passwords on a system expire on a specific day of the calendar is a prescription for a swamped helpdesk. The day after the expiration deadline, the poor help technicians are flooded with demands from irate users who have forgotten their new passwords (perhaps they forgot to write the new sequence



FIGURE 5.6 Hidden costs.



FIGURE 5.7 Changing passwords.

on a sticky note attached to their screen or to “hide” the new password inside their unlocked desk drawer or under their keyboard) (sigh).

If you are still stuck using passwords, as most organizations are,¹⁹ a far better approach to password management is to force password expiration on an individual basis, user by user and system by system. The load on the helpdesk thus gets distributed over all the working days instead of piling up a few days a year.

I once encountered another system-management issue that could lead to a self-imposed DoS. A correspondent informed me of a situation in which the technical-services group needed a change of email servers, forcing a change in the email-client software of several thousand users. The staff allocated a week for the changeover, after which no one’s unchanged email configuration would work. The argument was that a fixed deadline would force users to act, whereas a longer period would simply lead to lower compliance as users forgot all about the change request.

Now, it’s important to understand that the email system actually allowed overlap of the old and new configuration for several weeks before the deadline. Given that overlap, I think that a better approach to handling this kind of network configuration change involving users would have been to partition the change among groups of users. For example, perhaps the *Engineering Department* could have been guided through the change over a couple of days, and then the *Finance Department* and later the *Manufacturing Department*, and so on. That way, difficulties arising from implementation glitches would not affect everyone in the company all at once and the helpdesk and other technical staff could avoid being overwhelmed.

In addition, a staggered implementation schedule would allow early adopters to help work the bugs out, if any. [Hah! Have you *ever* encountered a project without bugs?] That’s why I suggested beginning with a technically more sophisticated group (*Engineering*) who might better be able to cope with bugs and cooperate with the helpdesk members in sorting out unexpected problems. By the time the later, less sophisticated groups reached their turn, some of the early glitches could have been removed.

It’s not exactly a, ah, *staggering* insight, but I hope it’s a useful one.

TERMINATING ACCESS

Most systems of authentication are good for session initiation but not so great for automatic session termination. One can place one’s finger on a fingerprint reader, insert a magnetic card into a reader, look into an iris scanner, speak into a microphone, type on a keyboard, sign one’s name – all of these methods can allow an authorized user to log on to a system. The problem is that once the interaction is supposed to be complete, there is usually no mechanism for *automatically* detecting the departure of the authorized user.

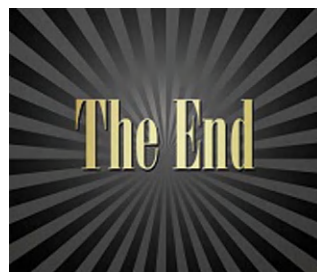


FIGURE 5.8
Terminating access.

- Asking the user to lock the system (e.g., *Windows-key/L*) or log off is helpful but not guaranteed to work; timeouts tend to be long enough that an unauthorized person can often use the established session as soon as the initiating person is gone.
- If one tries to use tokens such as magnetic cards or USB tokens to detect departure by forcing the user to leave the card or token in the reader while the session is in progress and to remove it before leaving, unpleasant consequences can result:
 - The user can leave the card in the reader and walk away or
 - The user will walk away with the card attached to their wrist and either be yanked backward or pull the equipment onto the floor with a clatter.

In the previous sections I have explained that I have long sought a system for using proximity devices as the basis for I&A, especially in the medical environment where most users are under too much pressure to tolerate logon/logoff procedures. Such applications benefit from a system that automatically allows session initiation when an authorized user approaches a workstation and then either suspends access or terminates the session when the user leaves – all without any particular human intervention.

We already have long-established access-control systems for physical security in facilities: *Wiegand cards*, which have metal particles embedded in plastic so they produce a unique signature in response to radio waves.²⁰ Proximity sensors can be placed in the wall to control door locks and allow people to go in and out without having to touch their cards.

Such technology is now available for access controls in computers and networks, and they have been implemented so as to allow recognition not only of the *arrival* of a person carrying the device but also the *departure*.

One example of a proximity system that conforms to these requirements is the *XyLoc Active RF Proximity Solution*:

XyLoc® protects workstations at a point when they are most vulnerable – after an authorized user logs on, and then steps away from the machine. XyLoc consists of a radio receiver “Lock” (reader) that plugs into the protected computer via USB, a wireless radio transmitter “Key” (badge/card) worn by the user, and client/server software components.

XyLoc provides full-time access control by assessing a user’s proximity and automatically locking the computer screen and keyboard when the user leaves the workstation. XyLoc knows when users are approaching and leaving a protected computer, and includes intelligence to handle busy multiuser environments.

XyLoc is highly configurable at user, workstation, and group levels. It can allow completely “hands-free” unlocking of a PC when a user returns within a configured grace period, and also supports a variety of two-factor authentication schemes. XyLoc simultaneously improves workstation security, compliance with security procedures, and end-user productivity.²¹

SPAM

Another issue of authentication is the false identities of criminals who send *unsolicited commercial email (spam)*, which is called that in abject worship of the beloved, superb, excellent, outstanding, brilliant *Monty Python Spam Skit*.²²

For those who care about copyright and trademarks, note that the Hormel Company owns the copyright to the name of its famous canned food and calls it *SPAM* in all capital letters. The company has very kindly allowed geeks to use *Spam* and *spam* without fear of legal pursuit.²³

I sometimes take the time to send a response to spammers who seem to be ignorant rather than criminal; these are usually people trying to sell consulting services. Here is the text of the macro I use in response (“CAN-SPAM” in all capital letters is the actual name of the law):

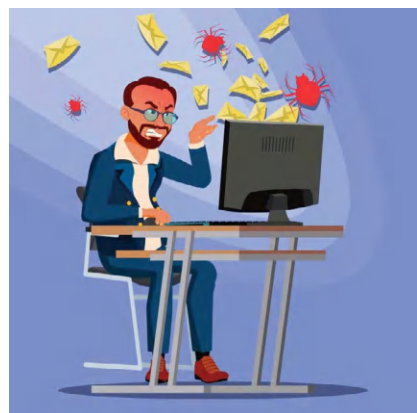


FIGURE 5.9 SPAM.

You are violating specific rules of the US CAN-SPAM Act of 2003 with the specific violations marked with asterisks (***) in the list below.

CAN-SPAM Act of 2003: Core Requirements

< <https://www.law.cornell.edu/node/37193> >

Section 5(a) of the CAN-SPAM Act of 2003 sets forth the basic legal principles that differentiate legal and illegal commercial email. See 15 U.S.C. § 7704(a). According to these principles, the senders of commercial email will be engaging in legal activity, so long as:

- 1) The header of the commercial email (indicating the sending source, destination and routing information) doesn't contain materially false or materially misleading information;
- 2) The subject line doesn't contain deceptive information;
- 3) The email provides "clear and conspicuous" identification that it is an advertisement or solicitation;
- 4) The email includes some type of return email address, which can be used to indicate that the recipient no longer wishes to receive spam email from the sender (i.e. to "opt-out");
- ***5) The email contains "clear and conspicuous" notice of the opportunity to opt-out of receiving future emails from the sender;
- 6) The email has not been sent after the sender received notice that the recipient no longer wishes to receive email from the sender (i.e. has "opted-out"); and
- ***7) The email contains a valid, physical postal address for the sender.

According to the Senate Commerce Committee Report, violations of these principles constitute "unfair or deceptive acts or practices" that are subject to enforcement action by the Federal Trade Commission ("FTC"), and certain other Federal agencies. See S. Rep. No. 108-102 (2003), at 17.

For another summary of the core legal principles distinguishing legal from illegal commercial email, see the FTC's CAN-SPAM Act Compliance Guide for Businesses (September 2009) < <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business> >.

[I am not a lawyer and this is not legal advice. For legal advice, consult an attorney licensed to practice in your jurisdiction and qualified in the specific area of the law concerned.]

Do not spam me again.

P.S. Openly breaking US federal law is not generally regarded as a good marketing technique for building a client base in the USA.

M. E. Kabay, PhD

I must admit that my response to criminals' spam is not polite at all, but let's not go there in this textbook!

THE FAKE LETTER STICKER

In December 2010, my wife and I received an official-looking letter with what appeared to be a sticker similar to those used by the USPS to certify or register mail:



FIGURE 5.10 Printed “sticker” on front and back of envelope.

The fake sticker was in fact printed directly on the envelope.

The upper left corner of the envelope included an intimidating warning forbidding tampering and referring to U.S. federal law. There was no organization named in the return address:

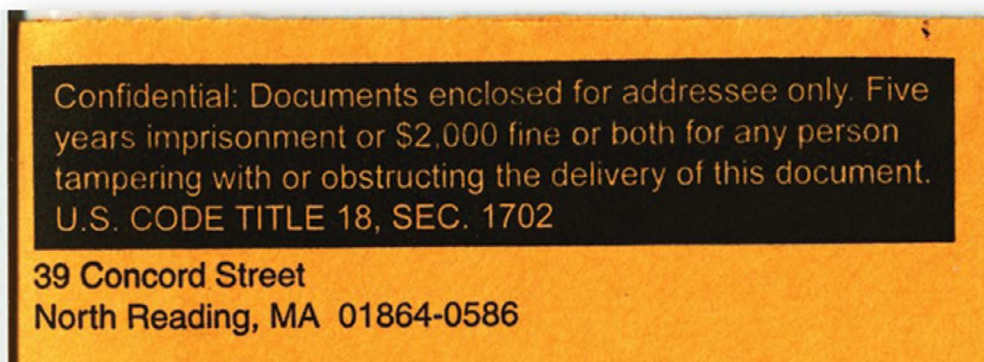


FIGURE 5.11 Fake warning.

The section of the *U.S. Code* named in the warning is indeed a warning against “Obstruction of correspondence” but there is no fine stipulated.²⁴

The envelope contained a flier from a car dealership advertising their next event. The misleading envelope was presumably designed to increase the probability that people would open it.

We had received an identical mailing in December 2009. I went to the dealership with the envelope in hand to complain about the effect of such fraudulent misrepresentation on elderly recipients. I myself had found my heartbeat increasing as I opened the original letter in 2009 – and then a sense of outrage that I had been tricked into opening junk mail. In 2010, I filed a complaint with the U.S. *Postal Inspection Service* (USPIS) about this practice.²⁵

Readers would do well to examine any letter that has official-looking, possibly intimidating material on the front or back but no identification of the sender. If what appears to be a sticker is actually printed on the envelope, be skeptical of anything in the envelope.

The designer of this scam has dubious moral standards and a delusional belief in the effectiveness of his marketing scheme. Intimidating people is not associated with warm, positive feelings about the dishonest sender; indeed, when my wife was in the service department of this dealership the day I phoned them with my complaint about the envelope, another customer agreed that the inauthentic envelope made him angry, too. If the car dealership is willing to lie on an envelope, would you trust them to give you a fair deal on a trade-in?

KITTY PORN

Back in 2012, my wife and I looked for a Russian Blue kitten we could adopt. We found an ad on the “kittensforadoption.us” site with a picture of a cute kitty available in Massachusetts, a few hours’ drive from our home in Vermont. We contacted the owner using the REPLY function.

We quickly got a nice email from “Susan Haper” cheerfully telling us [sic]

Greetings from this end and i’m glad to read back from you.As i said,we have three available 1 male and two female and they are purebred Russian blues.They are 13 weeks old respectively, The male is called Paige and the females are called Shannon and Jessy.i am glad that you want to take one of them.

[All the errors are in the original message.]

I received a phone call a day later by a man with a thick African accent who said he was the husband of “Mrs Susan.” I had to return his call, so I used the number I saw on my mobile phone, 385.200.1409. While I was speaking with him on a bad line, another African-sounding man interrupted the conversation, which was almost incomprehensible. The caller kept insisting that he wanted my wife’s email address, even though she had already received an email response as shown above.

Then we received the following astonishing news: the “Massachusetts” kitties were in Salt Lake City, Utah – more than 3000 km away (all errors in the original)!

hi after reading your mail, i was over whelm and wanted no body else to have this my baby except your loving family for they are perfect match to siamese. they are 4 months old and i am located in salt lake city Utah and i have both male and female of the baby. i will advice since you are a cat lover to take both the male and female to you. i can them ship to you there in vermont and it is not the first time i will be doing that so you dont have to worry. also attached to this email are the pics of the male and female. like i said they are for adoption and all you have to pay is for the shipping to you and before sending you this email i had to talk to the agency and they told me it will cost you 380\$ for both male and female to be home deliver to you from Utah to Vermont. they will be needing the following from you: full name, contact number and nearest airport to your location (that is if you will receive them at the airport) but if you will like for them to be deliver to your home address then you have to add: city and postal code, street name and home address. originally i had 4 babies as you will see and only the two single photos i am sending of the male and female are left

At this point, my alarm for “advance-fee fraud” went off and I looked into the situation in detail. Here are my key findings:

- The phone number (385.200.1409) had over 6,000 hits on Google for every imaginable kind of animal – including wild animals that cannot legally be raised or traded in the USA and animals covered under the *Convention on International Traffic in Endangered Species* (CITES).²⁶
- Analysis of the first thousand Google hits for ads using the 385.200.1409 phone number showed that almost all of them were on sites registered outside the USA.
- Exactly the same description of the kittens (“With pedigree. Vaccinated cat. Sterilized cat.”) generated 5,620,000 hits on the kittensforadoption.us website alone.
- The picture of the nice cat on a blue background was quick to find using *Google Images* using the search string < russian blue kitten > and turned out to be from a picture gallery; clicking on “Image Properties” showed that the specific image was from 2009 or earlier.



FIGURE 5.12 Fake kitten ad.

- More careful examination of the same page where the original “Massachusetts” kitty was posted showed dozens of cases of identical photographs used for different cats supposedly in widely separated areas of the United States.

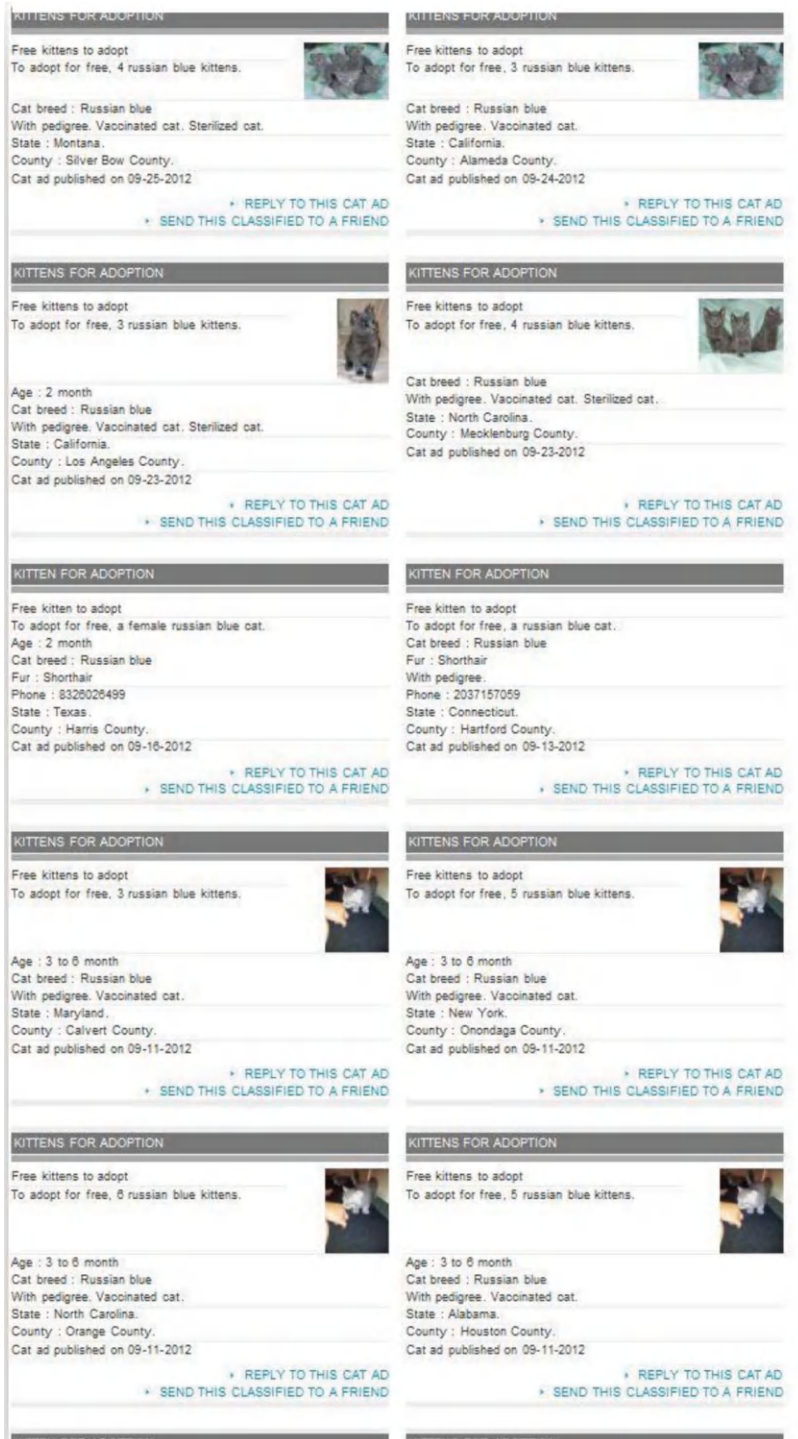


FIGURE 5.13 More fake kitten offers.

Using a domain-registration service, we found that the kittensforadoption.us website was registered by a German company supposedly by someone living in Beverly Hills, California. The phone number of the registrant, 213.631.1402, was not a working number.

Website	Domain registered in
www.adtob.com	Romania
www.animalssale.com	Ukraine
www.bedfordshire-central-bedfordshire.adtob.com	Romania
www.juneau.adtob.com	Romania
www.kittensforadoption.us	Germany
www.little-rock.adtob.com	Romania
www.usaphonestore.org	Australia
www.usmarketdb.com	USA

FIGURE 5.14 Domains for scammers' phone number.

The pattern fits that of the *advance-fee fraud*,²⁷ also known as the *4-1-9 Nigerian Fraud* (a reference to the Nigerian penal code section covering this kind of crime)²⁸ in which a sucker is cajoled into believing that (s)he will get something for nothing. The scammers then announce that a fee is required for completion. The request for “shipping” costs for nonexistent cats (unless someone has figured out how to clone the critters <g>) is a giveaway. Had we sent money, we would almost certainly have been told that another, even higher fee was required for completion of the transaction, which never actually completes in such frauds.

We should have been suspicious the moment we determined that the expensive Russian blue pure-bred kittens were *free* – and included three months of special food! The preliminary encouragement from the illiterate criminals was intended to entangle the gullible victims into a strong emotional connection with the virtual pets so that they would be more willing to send a payment to the scammers.

So in sum, here are some principles we should have applied from the start before getting any further involved in this scam:

1. Before looking into the purchase (or adoption) or anything, immediately use a search engine to scan for identical unusual words, misspellings, and phrases. Look for multiple ads that have identical wording and photographs of the product or animal.
2. If there are photos of the product or creature, check Google Images to see if you can locate identical photos that suggest that the user is simply faking a picture.
3. If there is a phone number available in the ad, see if the area code matches the claimed location in the ad. Then search for the entire number using a search engine; be skeptical if there are multiple, mutually exclusive hits. If someone claims to be in Utah and in Massachusetts at the same time, something's wrong.
4. Be skeptical of offers that are too good to be true. Why would someone be giving away expensive products or animals to complete strangers?
5. Never agree to send money in advance of the delivery. There are ways of safeguarding one's payments (e.g., through *PayPal*²⁹ or *eBay*³⁰) so that neither buyers nor sellers can be cheated.

We were still looking for a cat, but we went to the local animal shelter instead for our new member of the family.

SPANISH-BULL FIGHT

The email message announced breathlessly that I had won a lottery in Spain called *El Gordo* (The Fat One). “Mrs Esther Lodwig,” the “Promotions Director” of “*Global Stakes Lottery International*” wrote,

We are pleased to inform you of the release, of the long awaited results of the EL GORDO SPANISH GLOBALSTAKE LOTTERY/INTERNATIONAL PROMOTIONS PROGRAMES held on the 18th Jun 2003. You were entered as dependent clients with reference Number: IPL/096685769WP1, and batch number GL/678753-PCQ03. Your name attached to the ticket number: 6453 drew a lucky winning number, which consequently won the sweep take in the second category, in four parts.

You have therefore been approved for a payment of €2,500,000 (TWO MILLION, FIVE HUNDRED THOUSAND EUROS) in cash credited to file reference number: IPL/096685769/WP1. This is from a total cash prize of €10,756.820 (TEN MILLION SEVEN HUNDRED AND FIFTY SIX THOUSAND, EIGHT HUNDRED AND TWENTY EUROS) Shared among the international winners in all categories, congratulations!!!

The letter went on to explain that I should call a phone number in the Netherlands (odd, that, no?) to claim my prize.

Now it happens that I have never bought a lottery ticket in my life; I’ve contributed to charitable lotteries by contributing the price of the ticket but refusing to take it (just one of those weird habits of mine). All my friends know this about me, so it wouldn’t make sense for anyone to enter me into a lottery. In addition, it’s illegal for a U.S. resident to participate in a foreign lottery; 18 USC §1301 states in that annoyingly complete way that laws are written (take a deep breath),

Whoever brings into the U.S. for the purpose of disposing of the same, or knowingly deposits with any express company or other common carrier for carriage, or carries in interstate or foreign commerce any paper, certificate, or instrument purporting to be or to represent a ticket, chance, share, or interest in or dependent upon the event of a lottery, gift enterprise, or similar scheme, offering prizes dependent in whole or in part upon lot or chance, or any advertisement of, or list of the prizes drawn or awarded by means of, any such lottery, gift enterprise, or similar scheme; or, being engaged in the business of procuring for a person in 1 State such a ticket, chance, share, or interest in a lottery, gift, enterprise or similar scheme conducted by another State (unless that business is permitted under an agreement between the States in question or appropriate authorities of those States), knowingly transmits in interstate or foreign commerce information to be used for the purpose of procuring such a ticket, chance, share, or interest; or knowingly takes or receives any such paper, certificate, instrument, advertisement, or list so brought, deposited, or transported, shall be fined under this title or imprisoned not more than two years, or both.³¹

Whew! So, in the USA, even if you did win a foreign lottery, it would be illegal to collect on it.

A quick bit of investigation on GOOGLE revealed that this scam had been circulating for about a year. I’ve listed a number of good resources about it in the links section below, but the essentials are as follows:

- Criminals (most of them outside Spain) are circulating bogus claims all over the world that (presumably many) potential victims have won lots of money in the Spanish *El Gordo* (sometimes misspelled “El Godo”) state lottery.
- If the victim does call the phone numbers listed in the email or postal mail messages, they are invariably told that they have to supply a tiny fraction of their “winnings” as a tax (or for some other bogus fee).



FIGURE 5.15 Torturing bulls.

- Anyone who actually falls for the ploy and sends money is asked for yet more and then more and more until they wise up; some victims have sent many thousands of dollars.
- Some poor souls have supplied the criminals with details of their bank account and other private information, allowing their names to be used in identity-theft schemes.³²

So OLÉ! Let's fight this, ah, Spanish bull by posting a note in the corporate newsletter and on Facebook.

JUNK FAX NOT WHAT IT SEEMS

On Friday morning August 12, 2005 at 07:09 my fax machine³³ received a prospectus claiming to be from a marketing company (let's call it *Orfilian Corp* to avoid lawsuits by the criminals) on behalf of a high-tech startup (let's call it *Bazoonium Corp*)(and yes, I checked both of those fake names on GOOGLE and they didn't show up). The fax urged people to buy the stock, claiming it would be rising in value by orders of magnitude within months. It also included a toll-free number for getting out of the junk-fax list (I didn't dial it) and claimed that *Orfilian Corp* had received lots of shares in return for touting the stock.

I dialed *69 (my old landline phone service's "previous-call-number code") on my fax machine to determine the origin of this junk fax; it was reported by the automated system as 123-456-7890 (real details concealed to protect the guilty). Unfortunately, that number did not produce any identification of the owner using the reverse-lookup functions.

I looked up *Orfilian Corp* on the Web but had no luck finding phone or email (they used a Web form for email enquiries) so I used a DNS lookup for < orfilian.com > using the ICANN WHOIS tool,³⁴ found the phone number in the DNS entry and heard a phone message from the system administrator explicitly stating that their company does not send junk fax and they didn't know where the particular stock-touting fax came from.

Using the same WHOIS technique on bazoonium.com, I spoke with Dr Whatsis Whoever from Bazoonium Corp; he was very nice and thoroughly exasperated by the inclusion of his company's name in this junk fax. He and his colleagues had already received several phone calls from angry recipients of the same junk fax I got. The company is currently involved in a merger and there are 6M shares in public hands. Dr Whoever was concerned that the bad publicity from the fake fax might harm the company at this sensitive time. I suggested that he obtain affidavits from everyone in the company affirming their complete lack of involvement in this junk fax and that he keep a record of possible financial losses resulting from the fraud – all of this after the usual IANAL warning.

I think this junk fax was part of a *pump 'n' dump* stock manipulation scheme.³⁵ Someone was faking a press release, blaming the company and an innocent marketing firm, and trying to move stock prices up or down depending on how they were managing the fraud. For example, if they bought low, they wanted the stock to rise in price (at least until they could sell at a profit). If they sold futures, they may have wanted the price to fall so they could buy at a lower price than their guaranteed selling price.

In any case, this scam was also violating FCC rules on unsolicited faxes.³⁶ This fraudulent information was presumably being sent across state lines (potential interstate wire fraud – 18 USC 1343)³⁷ although I don't know what effect the origination in Canada might have had (if that information was true). The junk fax was sullyng the reputation of two innocent firms and possibly causing them significant loss of business by tarnishing their reputations; and it might have cost holders of Orfilian shares money if people were to buy shares at artificially inflated prices or sell at artificially depressed prices.



FIGURE 5.16
Landline fax machine.

Finally, this case teaches us that calling up the ostensible villains identified as the senders of a junk fax (and sometimes on junk emails) and shrieking abuse at them may not always reach the true villains in this time of negligible authentication of identity.

Even if we implement call-blockers for our fax machines, criminals will use caller-ID spoofing tools such as voice over IP³⁸ or the methods briefly offered by an unfortunate fellow called Jason Jepson to conceal their originating phone number. Mr Jepson gave up his proposal to offer false caller IDs after receiving threatening email and phone messages “and even a death threat taped to his front door.”³⁹

Gosh, and I thought *I* didn’t like junk communications!

THEFT OF IDENTITY AND THE BURDEN OF PROOF

In the recent decade, theft of identity using computer-based information has become a problem affecting a growing number of victims:

According to the *Aite Group*, 47% of Americans experienced financial identity theft in 2020. The group’s report, *U.S. Identity Theft: The Stark Reality*,⁴⁰ found that losses from identity theft cases cost \$502.5 billion in 2019 and increased 42% to \$712.4 billion in 2020. The group explains that the huge increase was fueled by the high rate of unemployment identity theft during the pandemic, as increased and extended unemployment benefits made the sector an attractive target for fraudsters.

Losses were forecast to increase again in 2021 to \$721.3 billion. The study narrowed the identity theft definition to include only application fraud, where criminals used a victim’s identity to open a new account of some type, and account takeover, where an account is taken so criminals can steal money or access rewards. Examples of accounts include rewards accounts for airlines, hotels, or merchants; insurance policies; and other accounts.

In 2019 and 2020, 37% of consumers have been victims of application fraud and 38% experienced account takeovers. The highest percentage of consumers who were victimized in 2020 were between 35 and 44 years of age and accounted for 30% of all identity theft victims. The findings are from an online survey conducted in December 2020 of 8,653 U.S. consumers aged 18 and older.⁴¹

Published stories in the news media tell dreadful tales of people whose identity has been appropriated by criminals.⁴² The perpetrators use detailed information about the victims to obtain new credit cards, new lines of credit, new bank accounts, new cars, and new criminal records. The victims often find out about the theft of their good name when a loan is turned down, a credit-card application is refused, a new employer becomes alarmed by a criminal record, or the police arrest the victim after a routine traffic check. Worst of all is the reversal in the burden of proof. Where normally the immense apparatus of the state has to establish a reasonable basis for arrest and a strong basis for conviction, in identity theft the victims may have to prove their innocence by proving their identity.

The psychological consequences for the victims may be severe:

Few people are emotionally prepared for the impact of identity theft. Victims of identity theft may feel overwhelmed at times by the psychological pain of loss, helplessness, anger, isolation, betrayal, rage, and even embarrassment. This crime triggers deep fears regarding financial security, the safety of family members, and the ability to trust again. You might also have to deal with the fact that someone they know personally was victimized by the theft.

Finally, victims may feel frustrated by the very people they turn to for help. Identity theft is a difficult crime to solve, and the wheels of justice are still squeaky. Everyone involved must be patient with themselves and with those who want to help.⁴³



FIGURE 5.17 Identity theft growing.

SYSTEM DEFENSE AGAINST IDENTITY THEFT

How can one defend oneself against identity theft? Basically, until it gets harder for imposters to appropriate someone else's identity, the only method is vigilance. One can ask credit bureaus to check on one's own record. If you have an existing relationship with your local bank, try asking your customer-service officer to check your record for you and let you know what (s)he finds. Use an identity-theft tracking service; choose one that is highly regarded and meets your needs.⁴⁴

It seems to me that much of the blame for identity theft lies in the financial and legal systems. We are just not demanding sufficiently rigorous I&A of people requesting financial instruments. There exist sufficiently precise biometric authentication methods today that one ought to be able to tie a name to a physical identity. In the UK, recent trials of iris recognition at automated banking machines have been successful in providing non-intrusive authentication of identity to reduce fraud.

But no local I&A will solve the problem if someone in California seizes the identity of a victim in Vermont. The California institutions will have no basis for rejecting the application of the imposter.

Why not have a service for those who are willing to participate so that all financial institutions could share biometric information about the real owners of an identity? Using one-way matching of the biometric data, someone's identity could be confirmed quickly during verification of the applicant's financial record. If it is so easy to use credit-bureau records to protect vendors, why not use the same system to help individuals protect their identity?

Finally, it is critically important to establish some legal changes so that the burden of proof returns to the state instead of being reversed so that the victims of impersonation have to prove their innocence.

Perhaps local law enforcement officials should be made aware of the signs of identity theft so that they can respond carefully in such cases. For example, do the officer's direct observations seem consistent with the criminal records and outstanding warrants attributed to the person they have stopped? Does the 75-year-old woman seem to be a likely candidate for the rap-sheet that includes arson, prostitution, drug-trafficking and extortion? Does the 23-year-old driving the old Toyota seem to be the 45-year-old man wanted for grand auto theft? Of course, there may be cases where the imposters have chosen carefully to steal the identities of people they actually resemble, but at least law enforcement should be aware of the possibility of identity theft before slapping the handcuffs on junior or on grandma.

PRACTICAL SAFETY TIPS TO REDUCE IDENTITY THEFT

In addition to using an identity-theft prevention system, apply some easy methods to reduce your risk:

- NEVER use a debit card for anything other than withdrawing money from an ATM. If crooks compromise your debit card number and PIN, they can withdraw money by wire from your bank account – and you may be responsible for the charges if you fail to report the fraud quickly).⁴⁵
- If you want to use your credit card on the Internet, establish a *PayPal* account.⁴⁶ You register your card there, but *PayPal* never reveals your card number to the merchants.



FIGURE 5.18 Identity thieves.



FIGURE 5.19 Resisting identity thieves.

- NEVER use the same password for more than one critical account. Thus, your passwords for your email, your online banking, your access to your credit card, and your various online memberships are all to be different. You can use password-safes of various kinds to store the passwords for all your needs and access them automatically once you give a single master password.
- NEVER obey an email message that warns you that one of your accounts has been compromised and you have to log in to “verify your credentials” using an uninterpretable URL or one that has peculiar characters in it. For example, if you have an account with, say, the *PersnicketyBank*, logging into “[P3r5n1cke7yBank.com](#)” is not a good idea. All such messages are “phishing” scams that will direct you to fake websites that look like the real thing – but the criminals will record everything you give them, including your account number, your password, your date of birth, etc. – and then rip you a new hole in your finances. Instead, contact your account support using an *established* method, e.g., a phone number on your credit-card or on a credible webpage for your service that you find yourself.
- ALWAYS sign up for immediate notification of all charges on your credit-card account. Find out if this service is available, and then have the notifications sent to your email if you use that a lot or to your phone via *Short Message Service* (SMS) if you prefer that method. Check every charge immediately and call the security office at your card provider if you do not recognize the charge – like for example if it is a \$700 invoice for escort services in Bangkok or the purchase of a trip to the ionosphere in a peculiarly shaped spaceship.⁴⁷
- If you use online banking and credit-card maintenance, see if there is *multifactor authentication* (MFA) available – an additional security feature such as requesting a security authorization code to be generated on your computer or phone or sent to your phone by SMS before you (or a thief) can log into your account.⁴⁸
- Check your credit-card and bank statements the day they arrive or are available online. Investigate anything you do not recognize.
- Look carefully at your ATM before putting your card into it. If there is a new piece of equipment that projects out of the surface of the device where you are supposed to put your card in, call the security office on the nearby phone – it may be a pirate card-reader (*card skimmer*) that records or broadcasts your card information to criminals.⁴⁹

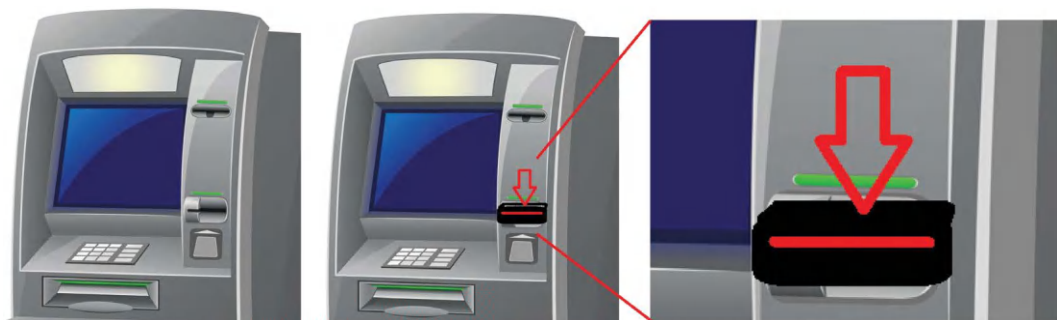


FIGURE 5.20 Card skimmer on ATM (right) compared with normal card slot (left).

- ALWAYS stand as close as you can to the keyboard of the ATM you are using; do not let anyone *shoulder-surf* your PIN from behind you. Most bank ATMs now have signs asking that only one customer enter the ATM room at once. If someone gets within a couple of feet of you when you are entering codes into such a keyboard, either stop or, if you can swing it safely, ask (tell) the person politely to back away (you can say that close contact makes you nervous). If that doesn't work, the person is either rude, a sociopath, or a criminal: cancel your transaction, leave at once, and inform the bank staff of the problem.

PRESCRIPTION FOR FAILURE: SIDE CHANNELS

One of the concepts I've always pointed out to my students is the importance of identifying and blocking *side channels*. For example, how can one signal a problem in a monitored system if that system stops working? Obviously, we must use another communication medium: a *side-channel*. Ideally, we use *synchronous* communication: real-time information transfer without delay. Synchronous communication could be simply walking over to tell someone who needs the information at once or phoning them for a live conversation (not a voicemail message).

Much less effective as part of a response to a problem is to use *asynchronous* information transfer such as leaving a voicemail message, sending text messages using *Short Message Service (SMS)*, *Facebook Messenger*, *Skype* and so on, putting information on electronic dashboards hoping that the right people will see it in time, posting a paper sticky-note on someone's desk as a warning, or dribbling pigment from a hole in the end of a stick onto compressed plant fibers to send the message via mule train. Asynchronous messaging is completely inappropriate for any communication about issues that require immediate response.

Side channels can play an important role in *breaking* security. For example, the *Acrobat* security feature can lock a file against copying or printing by using a password to allow such functions.⁵⁰ However, even without having to crack the password on the secured file, anyone can take a picture of the content of the file from a screen, perhaps page by page; the camera or the screen-shot software are uncontrolled side channels.

Some *data-loss-prevention (DLP)* systems use kernel-level modifications to prevent such functions as copying, modifying, printing, email, screen captures and so on. For example, the highly regarded *McAfee Data Loss Prevention Endpoint*® software⁵¹ provides many useful controls but again, none of these system-resident barriers can stop a disgruntled employee turned industrial spy from snapping a photo of a screen or printed page full of valuable, confidential information using a mobile-device camera as an uncontrolled side channel.

In addition to photographs, cell phones and tablets have microphones: it is trivial to initiate a recording and then slip the screen-darkened phone into one's carrying case, purse or pocket. Organizations with high security requirements use *sensitive compartmented information facilities (SCIFs)*.⁵² They complement their SCIFs with strict rules on exactly what electronic equipment is permitted past the security guards at the entrance to the secured portions of the facility. The whole point of a SCIF is to prevent unauthorized data leakage using side channels.

A classic side channel is *steganography*, which refers to hidden writing – information transfer in non-obvious forms such as integrated into music, photographs, videos, webpages and so on. Unlike cryptography, which alters cleartext into ciphertext that is accessible albeit uninterpretable, steganography conceals even the *existence* of the message. A microdot could be considered a steganographic technique, since unless one knows which dot on a printed page is actually a microphotograph readable through a microscope, one is unlikely to know that there's a secret message at all. Steganography using images typically modifies the last bit of each pixel's representation.⁵³

Decades ago, I discovered a failed form of DLP when I was given a prescription during an unfortunate visit to an emergency room (I had ripped my right leg's hamstring muscle with agonizing consequences). I scanned the prescription so I could send it to my wife (since I couldn't drive at that point) by email (because I forgot to give it to her when she left in the morning) to pick up a painkiller. [Figure 5.22](#) shows a blank section of the resulting scan.

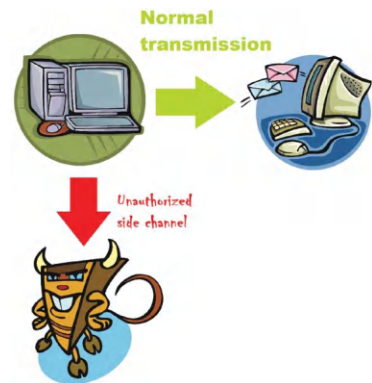


FIGURE 5.21 Unauthorized side channel.

The actinic light of the scanner brought out a marking invisible in ordinary light warning pharmacists that someone was presenting them with a *copy* of a prescription – a copy possibly modified for evil purposes.

Unfortunately, the method is limited. Figure 5.23 shows the same area of the paper photographed in ordinary fluorescent light on my desk using my cell-phone camera:

Oops. No VOID marks.

I reported the problem to the head of the pharmacy at the hospital, with a request that the alert be passed up the chain to the people who (a) created the paper and (b) ordered it to be used for prescriptions.

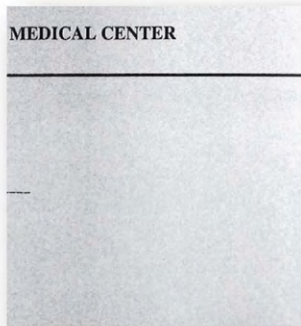


FIGURE 5.23 Copy missing VOID Marks.

There are many methods for making paper difficult to duplicate; for example, experts who manage the U.S. money supply⁵⁴ constantly invent and update⁵⁵ counterfeit-deterrence methods:

Security features maintained in the enhanced Federal Reserve notes include a portrait watermark visible when held up to a light, two numeric watermarks on the \$5s, an enhanced security thread that glows under an ultraviolet light, micro printing, improved color shifting ink that changes color when the note is tilted, and on the newly redesigned \$100 notes, a 3-D security ribbon and enhanced, raised printing.⁵⁶

The U.S. Treasury's *Bureau of Engraving and Printing* has vast resources compared with those of a prescription-pad maker, but at the very least, the people who created the non-copy paper for prescriptions should have checked for the possibility of defeating their counterfeit deterrence with a camera and an ordinary desk lamp before releasing their special product.

Failing to think outside our preconceptions is a prescription for failure. Reality overrides theory: we must test our assumptions!

CAPTCHA DA FLAG

Many readers have no doubt encountered funny-looking images of distorted letters that look as if they were created by someone in the grip of mind-altering substances or groups of annoying pictures with a demand to mark all those containing aquatic rotifers (OK, I made that up).⁵⁷ Sometimes these images are associated with sign-ups for webpages; occasionally one encounters email systems that demand that one decode the weird letters and numbers to be able to send email to a person being guarded against spam.

These puzzles are known as CAPTCHAs, standing for *Completely Automated Public Turing test to tell Computers and Humans Apart*. They were developed by The CAPTCHA Project at Carnegie Mellon University starting around 2000 as an approach to defeating bots (automated processes – from “robots”) that can be used to abuse online services. The examples cited on the CAPTCHA website include distortions of

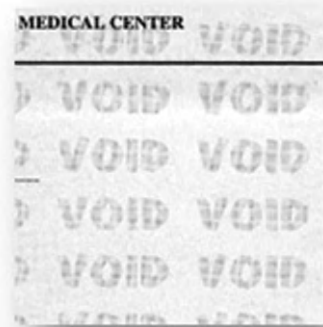


FIGURE 5.22 Copy of prescription showing VOID indicators.

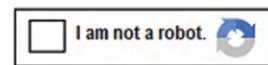
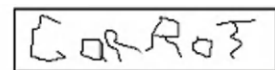


FIGURE 5.24 CAPTCHAs.

online polls, abuse of free email services, search-engine violations of privacy requests on websites, spam, and brute-force challenges to passwords on live systems.⁵⁸

The Labyrinth Society points out that applications of CAPTCHAs include:

- Preventing comment spam in blogs
- Protecting website registration
- Online polls
- Preventing dictionary attacks
- Search engine bots
- Worms and spam.⁵⁹

There are several types of CAPTCHAs in use today (Figure 5.24 shows three examples I made up). These visually based systems are evidently difficult or impossible for visually impaired users to master. Any attempt to use CAPTCHAs should offer alternatives for *bona fide* human beings with perceptual differences to authenticate themselves.

The CAPTCHAs that ask users to click on sections of photographs that match a particular criterion can be tricky if a human being doesn't check to see that there are no ambiguities or subtleties that may block users from succeeding in the test. For example, I created a deliberately difficult image-CAPTCHA at the bottom of Figure 5.24; it has two sections at the bottom left that show part of a goose's foot and four sections at the top right that show parts of a goose's neck and head. Not everyone is going to catch those subtleties. That's a *bad* CAPTCHA.

According to the CAPTCHA website, several artificial intelligence (AI) research groups are using CAPTCHAs as challenges and tools. For example, the *reCaptcha* project includes tools for harnessing the authentication of human beings as a mechanism for converting irregular text (e.g., material from centuries-old books) into electronic versions.⁶⁰

EASTER EGGS AND THE TRUSTED COMPUTING BASE

The confluence of several security threats threatens the *Trusted Computing Base* (TCB) on which security has depended for decades. The TCB was the constellation of trustworthy hardware, operating system, and application software that allowed for predictable results from predictable inputs.

Criminal hackers inserting malware into systems are a continuing threat to the TCB. Unfortunately, the TCB can also be corrupted by irresponsible programmers who introduce *unauthorized, undocumented code* into production systems: *Easter Eggs*. Such secret code, often intended for amusement of the programmers, is undocumented for the users and probably for managers. Access to the unauthorized functions is spread by word of mouth or through unofficial communications channels such as discussion groups or social media.

For example, back in 1998, security specialists were simultaneously horrified and amused by a primitive flight simulator concealed in *MS-Excel 97*.⁶¹ To access this game, users executed the following sequence of commands on a Windows system (stopped working as of 2002):

- Open Excel 97.
- Open a new worksheet and press the F5 key.
- Type X97:L97 and press the Enter key.
- Press the Tab key.
- Hold Ctrl-Shift and click the Chart Wizard button on the tool bar.
- Once the Easter egg is activated, use the mouse to fly around – right button for forward, left for reverse.

If users had *DirectX* drivers installed, a bizarre landscape appeared, and they could “fly” over (or under) the geometric forms by using the keyboard arrow keys. In the virtual distance, a stone

monitor planted in the ground was visible; flying over it, users could read the names of the development team scrolling by.

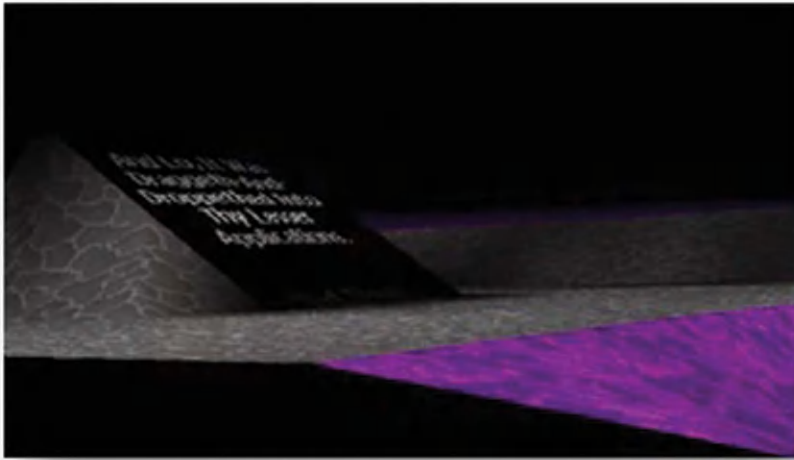


FIGURE 5.25 Excel easter-egg landscape.

How much space in the source and object code did this Easter Egg take? How much RAM and disk space were being wasted in total by all the people who installed and used this product? And much more seriously, what did this Easter Egg imply about quality assurance at the manufacturer's offices?

When testing executables, one of the necessary (but not sufficient) criteria is *test coverage*: how much of the executable code has actually been executed at least once during the QA process?⁶² Without running all the code at least once, one can state with certainty that the test process is incomplete. If the record of how many times each line of code has been executed during the best effort at exhaustive testing reveals sections or lines of code that were *never* executed, either the test scripts are inadequate or there is undocumented code that the software testers do not know how to force into execution. Failing to execute all the code means that there may be hidden functionality in the program: anything from an Easter Egg to something worse. What if the undiscovered code were to be invoked in unusual circumstances and cause damage to a user's spreadsheet or system? We would call such code a *logic bomb*.⁶³

There was at least one family of *Excel* macro viruses that altered the contents of cells randomly; the *Macro.Excel.Sugar* virus from 2001:

Upon activation it will create two files, "o6.reg" and "o6.bat", to the root directory of the C: drive. It will use these files to disable Excel's built-in macro virus protection by modifying the registry. Then it will check if there is a file named "Book1." in the Excel's startup directory. If the file does not exist, it will be created and infected. In that way the virus will be active every time when Excel is opened. To spread, the virus first copies itself to every workbook. It takes control when an infected workbook is deactivated. Next, it will go through all sheets within the workbook and will get control when an infected sheet is activated. The payload will be triggered in every month from September to December if the day equals the minute of the current system time. In this case it will replace the contents of up to 200 random cells with the following text: (*Dr. Diet Mountain Dew*). This text is written with random colors. It will also change contents of the top left ("A1") cell to *The -[Sugar.Poppy]- by VicodinES*.⁶⁴

This payload was immediately obvious, but more insidious *Excel*-macro viruses could cause more subtle and dangerous problems. For example, a virus could cause shifts in the low-order

significant digits of constants – something that might not be noticed in individual cells, but which might have significant effects on calculated results. A 2009 study by *Dartmouth College* scientists found errors in about 1–2% of the cells in a random sample of 50 real-world spreadsheets.⁶⁵ A 2013 review of spreadsheet errors and ways to prevent them⁶⁶ cites a 2008 meta-analysis (updated 2014) indicating that “...[N]line inspections audited 163 programs. They found errors in 84% using a weighted average.” The author (Prof Raymond Panko) argued in these concluding comments,

Future studies should spend much longer per spreadsheet. It seems best to examine whether ... code inspection rules should apply to spreadsheet inspection. This includes using multiple inspectors (five is a good number to use for data analysis on effectiveness), an initial meeting at which someone goes over a spreadsheet module in depth for the reviewers, the limitation of inspections to modules, and the placing of strict limitations on module size, inspection rates, and inspection time.⁶⁷

An information-warfare scenario involving unauthorized code could run as follows:

- Bad Guys infiltrate major software company and install undocumented code in widely distributed spreadsheet software. Faulty quality assurance allows the logic bomb to go into production releases.
- The logic bomb in the spreadsheet software receives payload instructions from an Internet connection.
- At a specified time, the spreadsheet program alters data in millions of spreadsheets in, say, the USA. Calculations go awry in subtle but dangerous ways. Since almost no one bothers to document their spreadsheets or provide test suites that can validate the calculations, few people notice the changes. Business, engineering, medical, and academic users make mistakes – they allocate the wrong amounts to investments and inventory, they predict the wrong stresses on bridge components, they calculate bad dosages for patient medication, and they assign good grades to bad students.
- This situation leads to decreased efficiency in the U.S. economy and is a contributing factor to a national and eventually international recession.

This scenario is an illustration of *asymmetric information warfare* – electronic sabotage on a grand scale with serious consequences for the target but for low cost to the attacker. Winn Schwartau used just this kind of scenario in his pioneering 1991 novel, *Terminal Compromise* (updated in 2002 and renamed *Pearl Harbor Dot Com* – still great fun).⁶⁸

So the next time you play with an Easter Egg in commercial software, stop to think: shouldn't you express your concerns to the manufacturer instead of just chuckling over a programmer's joke?

REDESI WORM DISGUISED AS SECURITY FIX ILLUSTRATES WARNING SIGNS OF PHISHING

The *Redesi* worm of 2001 used a particularly vicious form of disguise: it pretended to be a security patch or virus warning, thus playing on understandable nervousness about malicious software.⁶⁹

The subject line of the phishing email was randomly generated from a list that included the following:

- Emergency response from Microsoft Corp
- Important news from Microsoft
- IT departments on state of HIGH ALERT
- Microsoft security update
- Microsoft Update. Final Release Candidate
- New computer virus

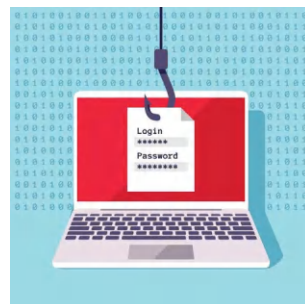


FIGURE 5.26 Phishing.

- Security Update by Microsoft
- Stop terrorists computer viruses reign
- Terrorist Emergency. Latest virus can wipe disk in minutes
- Terrorists release computer virus

The message itself read,

Just recieved [sic] this in my email I have contacted Microsoft and they say it's real! Due to the recent spate of email spread computer viruses Microsoft Corp. has released a security patch. Please apply the attached file to your Windows computer to stop any further spread or these malicious programs. Regards Microsoft Support.

A variant used a different strategy: it used misleading subject lines such as:

- A new type of Lager/Weed variant..... sorted!
- hell is coming for u, u will be sucked into a bottomless pit!!! – Gaz
- I don't want to write anything but Si is bullying me. – Jim
- I want to live in a wooden house – Arwel
- Kev Gives great orgasms to ladeez!! – Kev
- Michelle still owes me ú10 ... shit! – Si
- My dad not caring about my exam results – by Michelle
- Scientists have found traces of the HIV virus in cows milk...here is the proof – Will
- Why have I only got cheese and onion crisps? I hate them! ! – Si
- Yay. I caught a fish – Si

The latter variant used this body text: “heh. I tell ya this is nuts! You gotta check it out!” Attachments for both variants included the following:

- common.exe
- disk.exe
- rede.exe
- si.exe
- userconf.exe

Opening the attachment executed the payload, which included the following functions:

- Worm sent itself to contacts in the recipient's Microsoft Outlook Address Book
- Infects operating system
- Opened Windows dialog box showing that “the update was successful”
- Attempted to reformat hard drives on Windows 9X or Windows ME machines on November 11 because of code inserted into the AUTOEXEC.BAT file

Defensive actions to reduce vulnerability to phishing:

- Remind all users on your network NOT to open ANY executable email attachments or any unsolicited or unexpected attachments of any kind.
- Explain that no legitimate security tool is ever distributed by email, without a date, without a digital signature, and bypassing normal administrative controls.
- Don't open mail that appears to be arriving in your in-box by mistake (i.e., with someone else's name or a stranger's name on what seems to be personal correspondence).
- Delete unopened unwanted attachments from both the *Inbox* and the *Deleted Items* folders.
- Keep your antimalware software up to date automatically.

HIJACKING WEB PAGES

A student in one of my cyberlaw classes wrote to me about webpage hijacking:

Suppose a company wanted to obtain business from a rival company – let’s say < www.azbycxdw987.com >.⁷⁰ Is it possible for the competitor to create a similar site with the same name, < www.azbycxdw987.com >, that would be able to fool visitors to deal with the competitor rather than the original site? Is it possible for the attacker to configure their own server to use same IP address as the genuine site? Which measures can be taken to prevent such kind of fraud?



FIGURE 5.27 Hijacking.

No, it’s not going to be easy to use someone else’s URL directly. There are several strategies used to “hijack” URLs, but simply trying to duplicate someone’s IP address isn’t going to work. This section looks at several of the ways that URLs can be subverted and then finishes with some obvious countermeasures.

MISLEADING NAMES

Using domain names similar to those in URLs of existing, honest sites is a common method for diverting traffic from one site to a competing site. Pornographers often register the domain names of famous sites in different high-level domains, e.g., the U.S. government’s < whitehouse.gov > was mimicked by the URL < whitehouse.com >, which had pornographic pictures on it.⁷¹

Another technique is to register frequent misspellings of a famous site’s name; for example, around 2016, criminals were infecting victims’ computers with malware to send pop-up ads from < micosoft.com > with fraudulent information leading to further damage. Apparently, some users failed to note the missing “i” in “micosoft.”⁷²

Another commonly used method is the *homograph attack*: registering domain names using characters from different character sets; for example, using an “o” symbol that is actually from the Russian alphabet, thus making < microsoft.com > a domain different from < microsoft.com >. Such frauds are often used in phishing scams to trick victims into clicking on what look like legitimate URLs:

WWW.HONEST.COM/



WWW.HoNEST.COM/

FIGURE 5.28 Switching characters.

The Farsight Security report looked at more than 100 million domain names that use non-English character sets - introduced to make the net more familiar and usable for non-English speaking nations - and found about 27% that were unique, indicating the prevalent usage of internationalized domain names.

It also uncovered more than 8,000 international domain name homographs, or lookalike domain names, characters, representing or containing a top global brand name.

Farsight founder Paul Vixie, who wrote much of the software underpinning the net’s domain names told the BBC: “Any lower case letter can be represented by as many as 40 different variations.”

And many internationalised versions added just a tiny fleck or mark that was not easy to see.⁷³

Criminals can experiment using a WHOIS function⁷⁴ to try different misspellings of famous sites that haven’t yet been registered by using keys that are adjacent to letters in the real name on the keyboard. Perhaps using this strategy, various criminals registered “microsift.com,” “microsuft.com,” “microsoft.com” and so on, hoping to trick unobservant users into clicking on their fraudulent links.

MISLEADING LINKS

Another strategy fraudsters can use is to create *HTML* pages, including *HTML*-compliant email messages, that misrepresent the links to which the victim's browser will branch; if the *label* for a link claims it's, say, < [abc.def.com](#) > some inexperienced users may not notice that the link actually goes to < [ghi.jkl.com](#) > instead. Everyone should *hover their cursor over a link* before clicking on it; the actual URL will show up, usually in the lower left corner of the screen. Figure 5.29 shows how the real link can appear when the cursor is on the fake link labeled < [www.goodstuff.com](#) >.



FIGURE 5.29 Hovering over link shows real URL.

FRAMES VIOLATE COPYRIGHT

Some people bring in content from a site using *frames* that obscure the origin of the material; thus one could define the *HTML* on a webpage to give users the impression that they are successfully accessing a particular site, yet in fact everything around the frame is controlled by a different, perhaps competing, vendor. Such a case occurred in 1997, when several publishers launched a lawsuit against *TotalNews*, which was using frames to show visitors different news sources. However, the copyright owners claimed that this display of their materials in the context of *TotalNews* own webpage violated their ownership rights. The problem seemed to be exacerbated by the banner advertisements that *TotalNews* placed on its webpage, thus benefitting from revenue while using other people's property without recompense. The lawsuit was eventually settled out of court.⁷⁵



FIGURE 5.30 Frames violating copyright.

HIDDEN TEXT TRICKS USERS

Using hidden text such as *metatags* in *HTML* can confuse search engines into pointing at a site when users enter keywords even if in fact the fraudulent site has nothing to do with the keyword.

The practices at issue are labeled by the FTC as “*page jacking*” and “*mouse trapping*.” With page jacking, the perpetrator copies the legitimate Webpages of others, and adds a redirect script which includes the URL of another Website run by the perpetrator.

The page-jacked pages are then indexed by search engines, and Web users find and click through to the page-jacked pages via search-engine listings, thinking that they are going to a legitimate Webpage.



FIGURE 5.31 Trapped in an online hell.

With *mouse trapping*, scripts are added to the pages containing porn ads which cause more porn ads pages to be displayed when the user clicks the browser's back or close buttons. Pornographers in particular have been adept at lying about their sites; in some cases, they even put in words designed to attract children. In 1999, one villain who was shut down by the FTC even included Java applets that disabled the "back" arrow in browsers and deleted the ability to close the browsers. People trapped in this porno-hell had to reboot their computers to get out.⁷⁶

DNS CORRUPTION

There have been a few cases of *DNS corruption* that have led to Web hijacking. Corrupting the tables in the translation of URLs to IP addresses shifts sessions to the wrong servers. The most notorious case of DNS data-cache corruption occurred in July 1997, when Eugene Kashpureff filed fraudulent information with the *Internet Network Information Center* (InterNIC)⁷⁷ for its DNS updates, forcing domain-name servers around the globe to recognize temporary and unauthorized Internet addresses ending in .xxx, .mall, .nic and .per. A few weeks later, he inserted false information, possibly using a "helpful hints" field that could trick a server into associating a requested address with some other, unauthorized address on the Net. Kashpureff's interference forced people trying to access the website of *Network Solutions Inc.* (NSI) to end up at Kashpureff's *Alternic* site. At the time, *Alternic* was fighting NSI's monopoly over the .com, .net, .edu, .gov and .org domains.

Kashpureff faced civil suits from NSI for damages and possible criminal charges of computer trespass. Two weeks after contaminating the DNS, he claimed to be working with victim NSI to improve DNS server software to prevent future similar attacks. In 1998, the *Internet Engineering Task Force* (IETF)⁷⁸ continued its work on a new secure DNS which would include encrypted authentication for all DNS server updates, including controls over the "helpful hints" field.

In November 1998, Kashpureff was arrested by Canadian Immigration officials and handed over to the FBI on a warrant for violations of federal communications statutes. Also in 1998, the *U.S. Defense Advanced Research Projects Agency* (DARPA)⁷⁹ contracted with *Network Associates* (working with the *Internet Software Consortium*) to prevent further recurrence of Kashpureff's corruption of the DNS. The plan was to provide cryptographically strong authentication that would prevent imposters from modifying data in DNS data caches.

Kashpureff pleaded guilty to wire fraud in March 1998.⁸⁰ He was fined \$100 and sentenced to two years of probation. I was personally shocked and disappointed that he was not punished in accordance with the maxima for violating 18 USC 1030(a), which could have meant up to five years in federal prison and a maximum fine of \$250,000 for a first offense.⁸¹

WRITE-ACCESS IS DANGEROUS

Public websites such as those created with *WordPress*⁸² need careful definitions of file-access permissions. If unauthorized users have *write-access* to a website, all bets are off. Given such access, the attackers can subvert a website by branching automatically to an alternative site of their choosing – even a site that looks identical to the original but has nefarious features such



FIGURE 5.32 Corruption.



FIGURE 5.33 Write-access.

as password stealing or capturing credit-card numbers and other personal information. Depending on how actively the Webmaster checks the site, it is even conceivable that the owners of such a modified site might not notice immediately that what they were seeing was in fact a fraudulent version of their original material. However, if the Webmaster or network manager checked the volume of traffic, the sudden decline in activity would be an obvious clue to the problem. The standards for defining website access controls are well established.⁸³

SUMMARY OF COUNTERMEASURES

- Users should keep an eye on the actual URL that appears in their browser window; any discrepancy between the actual URL and the URL you expect to see should alert you to the possibility of fraud.
- Never click on any URLs in junk email, even if they claim that you can use them to get off the junk list; aside from not encouraging spammers, this policy also prevents you from confirming the validity of your email address to unscrupulous scumbags who then sell your confirmed address to other scumbags and fools [tell us how you really feel, Mich].
- In addition, consider running a personal firewall to block *ActiveX* controls and *Java* applets from unknown or untrustworthy sites.
- For those who control DNS servers, it is important to provide maximum security, including physical isolation, for these systems to prevent tampering.
- When establishing a new domain name, it may be worth the modest investment to buy rights to obvious variants, e.g., hyphenated forms, versions with underscores, and even obvious misspellings. On a personal note, I received a threatening email stating that Chinese criminals would register the domain name < mekabay.cn > unless I sent them money. You can imagine the level of foul language with which I responded to their “threat.”
- Check the Web using search engines to be sure you can identify sites that may be infringing on your trademarks using variant spellings.
- The same techniques that prevent website vandalism also preclude insertion of fraudulent URLs to hijack pages. Such techniques include setting all permissions on the *HTML* and active content to read-only for unauthorized users and using checksums to identify unauthorized modifications.



FIGURE 5.34

Checklist of countermeasures.

FORGED EMAIL HEADERS AND THE LAW

As many readers will know from personal experience, it is trivially easy for junk emailers and anyone else to forge headers of mail sent through the *Simple Mail Transfer Protocol* (SMTP). Almost all of the dozens of junk email messages I receive a week have forged headers.

Many of the forgers pretend that their mail comes from well-known sources such as *GMAIL*, *HOTMAIL*, *YAHOO*, and other free services. Others are more imaginative and use DNS entries and even country codes from such places as Italy, Japan, and Burma. It's important to realize that some of the sender addresses actually belong to innocent victims:



FIGURE 5.35 Forgeries.

Between 1 to 2% of all emails are flat-out scams, says email security company *Valimail*. They are unscrupulous people impersonating a company or organization or person you know, trying to get you to

do something like give up your banking details, send a payment, or divulge secret information. On the surface, an email might look just fine, saying it's from BankofAmerica.com, for instance. Actually, it's from some random domain controlled by a hacker who is looking to siphon funds illegally from you or your company's accounts.

At over 300 billion emails sent daily, that means 3-6 billion scam attempts daily. Over 90% of cybersecurity attacks start with email, says *Valimail*.⁸⁴

When I report spam to *abuse* addresses for GMAIL, HOTMAIL, OUTLOOK etc., my message includes this text:

< supposed-sender@mail-service.com >

If the address above really is the sender of this spam, please terminate that account. It is of course possible that the sending ID is false.

The criminals who send junk email have to include some kind of contact information if they expect to trick and cheat anyone into giving them money. Many such messages include URLs for websites or what appear to be real email addresses (different from the forged addresses in the headers). Some of them have postal addresses – often post-boxes to make it harder to track down the perpetrators.

Overpayment or *refund* scams always include a phone number, usually created using *voice-over-IP* (VoIP) to look like a valid number but actually connecting with numbers in other countries. These phone numbers may disappear quickly because the phone companies do respond to notification about such scams. These scams can involve email claiming that your account has been charged for software you don't use (e.g., *Norton Antivirus*®):

People tell us they're getting emails that look like they're from Norton, a company that sells antivirus and anti-malware software. (Tip: the emails are NOT from Norton.) The emails say you've been (or are about to be) charged for a Norton product — maybe an auto renewal or new order. If this is a mistake, the email says, you should call immediately. (Tip: don't.)

If you call, you'll be connected to a scammer. Some scammers might ask you to “verify” your credit card information, while others might say they need your password to remote into your computer so they can remove the Norton program. But if you let them, they could install malware, block you from getting to your own files, and sell you worthless services.⁸⁵

Sometimes I call these criminals just for fun to inflict loud, detailed, anatomically impossible instructions for exceedingly unsanitary processes. Others have reported using air-blast horns which cause considerable shock to the criminals.

A journalist originally from India has often tricked the criminals into revealing their origin:

Barring a few exceptions, the individuals calling me have had South Asian accents, leading me to suspect that they are calling from India. On several occasions, I've tested this theory by letting the voice on the other end go on for a few minutes before I suddenly interrupt with a torrent of Hindi curses that I retain full mastery of even after living in the United States for the past two decades. I haven't yet failed to elicit a retaliatory offensive in Hindi.⁸⁶

Speaking of innocent victims, some of the people who *seem* to be sending junk email are actually victims themselves. One year, I called an insurance agency that sent its toll-free number through junk email with forged headers; the lady on the answering-machine tape sounded shell-shocked.

Getting ready to call the scammers.



FIGURE 5.36 Annoying criminals.

Her message apologized repeatedly for sending unsolicited email and tried to refer complaints to the scoundrels who took her money after tricking her into believing they would do her sales some good through their despicable practice. One can just imagine the dismay caused by no-doubt virulent – and likely expensive – opinions sent through the hapless company’s voicemail.

Please, everyone: tell your marketing departments NEVER to agree to send out unsolicited email. It’s the kiss of death. And remind your staff not to reply to those “to-unsubscribe-send-a-reply-to” addresses; the general belief among anti-spam activists is that the reply messages feed the junk emailers’ lists of valid addresses and can actually increase the amount of junk you get.⁸⁷

NOTES

- 1 [United States Postal Inspection Service \(2023\)](#).
- 2 [Lal, Prasad, and Farik \(2016\)](#).
- 3 [Salveggio, Lovaas, Lease, and Guess \(2014\)](#).
- 4 [Veridium Trusted Digital Identity \(2020\)](#).
- 5 [Capterra Identity Management Software \(2021\)](#).
- 6 [Saiki, Obayashi, Li, Harao, and Miyake \(2019\)](#).
- 7 [Krim \(2004\)](#).
- 8 [American Civil Liberties Union \(2002\)](#).
- 9 [Najibi \(2020\)](#).
- 10 [Burt \(2021\)](#).
- 11 [Nash \(2020\)](#).
- 12 [Shein \(2020\)](#).
- 13 [Hashim \(2021\)](#).
- 14 [Cranor \(2016\)](#).
- 15 [ScienceDaily \(2016\)](#).
- 16 [Williams \(2019\)](#).
- 17 [Maddox \(2021\)](#).
- 18 [Kidd \(2019\)](#).
- 19 [Help Net Security \(2021\)](#).
- 20 [Kisi \(n/a\)](#).
- 21 [Ensure Technologies \(2021\)](#).
- 22 [Business Insider \(2017\)](#).
- 23 [Glasner \(2001\)](#).
- 24 [U.S. Code \(1994\)](#).
- 25 [U.S. Postal Service \(2019\)](#).
- 26 [CITES \(n/a\)](#).
- 27 [Advance Fee Fraud Coalition \(n/a\)](#).
- 28 [NYCriminal Defense – BUKH Law Firm \(2015\)](#).
- 29 [PayPal \(2023\)](#).
- 30 [eBay \(2023\)](#).
- 31 [U.S. Code \(1994\)](#).
- 32 [Government of Western Australia \(n/a\)](#).
- 33 For younger readers, a “facsimile” (fax) machine is an ancient substitute for email that allowed old people to send copies of documents to be printed on a printer connected to a wired phone system (a “landline”). This method was a significant improvement over sending messages written in Sumerian cuneiform on clay tablets transferred by mule train.
- 34 [ICANN \(n/a\)](#).
- 35 [U.S. Securities and Exchange Commission \(n/a\)](#).
- 36 [U.S. Federal Communications Commission \(2019\)](#).
- 37 [U.S. Code \(2008\)](#).
- 38 [Reuters \(2005\)](#).
- 39 [Belson \(2004\)](#).
- 40 [GIACT \(2021\)](#).
- 41 [Insurance Information Institute \(2021\)](#).

- 42 IdentityForce (2021).
- 43 U.S. State of Georgia (n/a).
- 44 Consumers Advocate (2021).
- 45 Clark.com Staff (2021).
- 46 PayPal (2020).
- 47 Dessem (2021).
- 48 Drake (2020).
- 49 Stephenson (2016).
- 50 Adobe (2021).
- 51 McAfee (2021).
- 52 SCIF SOLUTIONS (2021).
- 53 Kessler (2001).
- 54 U.S. Department of the Treasury (2021).
- 55 U.S. Department of the Treasury (2021).
- 56 U.S. Department of the Treasury (2021).
- 57 Cloudflare (2021).
- 58 Carnegie Mellon University (2010).
- 59 The Labyrinth Society (2023).
- 60 TechCrunch (2007).
- 61 Werring (1998).
- 62 Levine, Mason, and Hadley (2014).
- 63 Fitzgibbons (2019).
- 64 F-Secure (2001).
- 65 Powell, Baker, and Lawson, (2009).
- 66 Olshan (2013).
- 67 Panko (2014).
- 68 Schwartau, Pearl Harbor Dot Com (2002).
- 69 Loney (2001).
- 70 I actually had to search using GOOGLE to find a gibberish domain name that did not exist (yet?).
- 71 Peline (1997).
- 72 Kiguolis (2016).
- 73 BBC News (2018).
- 74 ICANN (n/a).
- 75 Richtel (1997).
- 76 TechLawJournal (1999).
- 77 U.S. Department of Commerce (n/a).
- 78 IETF (n/a).
- 79 U.S. Department of Defense (n/a).
- 80 U.S. Attorney – Eastern District of New York (1998).
- 81 U.S. Code (2020).
- 82 WordPress (n/a).
- 83 Bartley (2020).
- 84 Koetsier (2020).
- 85 Wu (2021).
- 86 Bhattacharjee, Y. (2021).
- 87 McAfee Labs (2016).

WORKS CITED

- Adobe. (2021, n/a n/a). *How to Password Protect PDF Files*. Retrieved August 10, 2021, from Adobe Acrobat: <https://www.adobe.com/acrobat/how-to/pdf-file-password-permissions.html>
- Advance Fee Fraud Coalition. (n/a, n/a n/a). *What is Advance Fee Fraud*. Retrieved August 3, 2021, from affcoalition: <http://affcoalition.org/>
- American Civil Liberties Union. (2002, May 14). *Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws, ACLU Says*. Retrieved November 30, 2021, from ACLU | Privacy & Technology | Government surveillance: <https://web.archive.org/web/20021105090055/http://www.aclu.org/Privacy/Privacy.cfm?ID=10340&c=130>

- Bartley, M. (2020, May 29). *WordPress File Permissions: Complete Beginner's Guide*. Retrieved August 12, 2021, from MalCare: <https://www.malcare.com/blog/wordpress-file-permissions/>
- BBC News. (2018, June 26). *Scammers Abuse Multilingual Domain Names*. Retrieved August 12, 2021, from BBC News | Tech: <https://www.bbc.com/news/technology-44612317>
- Belson, K. (2004, September 4). *Citing Threats, Entrepreneur Wants to Quit Caller ID Venture*. Retrieved August 3, 2021, from The New York Times: <https://www.nytimes.com/2004/09/04/technology/citing-threats-entrepreneur-wants-to-quit-caller-id-venture.html>
- Bhattacharjee, Y. (2021, January 27). Retrieved December 7, 2021, from New York Times Magazine: <https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html>
- Burt, C. (2021, September 24). *NEC Claims Win in NIST Iris Biometrics Accuracy Test*. Retrieved November 30, 2021, from BIOMETRIC UPDATE: <https://www.biometricupdate.com/202109/nec-claims-win-in-nist-iris-biometrics-accuracy-test>
- Business Insider. (2017, February 12). *Spam Stems from Monty Python Sketch*. Retrieved August 4, 2021, from Monty Python Channel: <https://www.youtube.com/watch?v=zLih-WQwBSs>
- Capterra Identity Management Software. (2021, June 14). *RSA SecurID*. Retrieved August 4, 2021, from Capterra: <https://www.capterra.com/p/172820/RSA-SecurID-Access/>
- Carnegie Mellon University. (2010, n/a n/a). *CAPTCHA: Telling Humans and Computers Apart Automatically*. Retrieved August 10, 2021, from Captcha.Net: <http://www.captcha.net/>
- CITES. (n/a, n/a n/a). *The CITES Species*. Retrieved August 3, 2021, from CITES: <https://cites.org/eng/disc/species.php>
- Clark.com Staff. (2021, May 3). *Why You Should Never Use a Debit Card To Pay for Anything*. Retrieved December 4, 2021, from Clark.com: <https://clark.com/personal-finance-credit/never-use-debit-card-pay/>
- Cloudflare. (2021, n/a n/a). *How CAPTCHAs Work | What Does CAPTCHA mean?* Retrieved August 10, 2021, from Cloudflare: <https://www.cloudflare.com/learning/bots/how-captchas-work/>
- Consumers Advocate. (2021, August 4). *10 Best Identity Theft Protection of 2021*. Retrieved August 6, 2021, from consumersadvocate.org: <https://www.consumersadvocate.org/id-theft-protection/a/best-id-theft-protection>
- Cranor, L. (2016, March 2). *Time to Rethink Mandatory Password Changes*. Retrieved August 3, 2021, from Tech@FTC: <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>
- Dessem, M. (2021, July 21). *Why Does Jeff Bezos' Rocket Look So Much Like a Penis? We Asked a Rocket Scientist*. Retrieved August 6, 2021, from SLATE: <https://slate.com/technology/2021/07/bezos-blue-origin-resembles-penis-rocket-scientist-explains-why.html>
- Drake, A. (2020, June 25). *Everything You Need to Know About Multi-Factor Authentication*. Retrieved August 6, 2021, from g2.com: <https://www.g2.com/articles/multi-factor-authentication>
- eBay. (2023). *eBay Money Back Guarantee*. Retrieved July 22, =2023, from eBay: <https://pages.ebay.com/ebay-money-back-guarantee/>
- Ensure Technologies. (2021, n/a n/a). *Leverage XyLoc's Patented Active RF Proximity Solutions for Maximum User Productivity and Walk-Away Security*. Retrieved August 4, 2021, from Ensure Technologies | Partners: <https://www.ensuretech.com/products/xyloc-active-rf-proximity-cards-and-readers/>
- Fitzgibbons, L. (2019, April n/a). *Definition: Logic Bomb*. Retrieved August 11, 2021, from TechTarget SearchSecurity: <https://searchsecurity.techtarget.com/definition/logic-bomb>
- F-Secure. (2001, January 27). *Sigar*. Retrieved August 11, 2021 from F-Secure Threat Descriptions: <https://www.f-secure.com/v-descs/sugar.shtml>
- GIACT. (2021, n/a n/a). *[New Report] U.S. Identity Theft: The Stark Reality*. Retrieved August 4, 2021, from GIACT: <https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/>
- Glasner, J. (2001, May 26). *A Brief History of SPAM, and Spam*. Retrieved July 22, 2023, from Wired: <https://www.wired.com/2001/05/a-brief-history-of-spam-and-spam/>
- Government of Western Australia. (n/a, n/a n/a). *Spanish Lottery (El Mundo or El Gordo)*. Retrieved August 3, 2021, from WA ScamNet: https://www.scamnet.wa.gov.au/scamnet/Contact_Us.htm
- Hashim, A. (2021, June 23). *Dangers of Reusing Passwords – Know why is it bad and how you can avoid it*. Retrieved December 4, 2021, from PrivacySavvy | Password | Guides: <https://privacysavvy.com/password/guides/reusing-passwords/>
- Help Net Security. (2021, February 15). *Rampant Password Reuse Puts Companies and Customers at Risk*. Retrieved August 4, 2021, from Help Net Security | Featured News: <https://www.helpnetsecurity.com/2021/02/15/password-reuse-risk/>
- ICANN. (n/a, n/a n/a). *Registration Data Lookup Tool*. Retrieved August 12, 2021, from ICANN | LOOKUP: <https://lookup.icann.org/>

- IdentityForce. (2021, n/a n/a). *Real Identity Theft Stories*. Retrieved August 6, 2021, from Real Identity Theft Stories Blog Series: <https://www.identityforce.com/blog/real-identity-theft-stories>
- IETF. (n/a, n/a n/a). *About the Internet Engineering Task Force*. Retrieved August 13, 2021, from IETF: <https://www.ietf.org/about/>
- Insurance Information Institute. (2021, n/a n/a). *Facts + Statistics: Identity Theft and Cybercrime*. Retrieved August 4, 2021, from Insurance Information Institute: <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
- Kessler, G. C. (2001, September n/a). *Steganography: Hiding Data Within Data*. Retrieved August 10, 2021, from Gary Kessler: <https://www.garykessler.net/library/steganography.html>
- Kidd, C. (2019, August 22). *Cost Per Ticket: The Ultimate Service Desk Metric*. Retrieved August 4, 2021, from BMC Service Management Blog: <https://www.bmc.com/blogs/cost-per-ticket/#>
- Kiguolis, U. (2016, August 25). *Micosoft.com-site.online ads (Tutorial)*. Retrieved August 12, 2021, from Spywar: <https://www.2-spyware.com/remove-micosoft-com-site-online-ads.html>
- Kisi. (n/a, n/a n/a). *Wiegand in Access Control: A Kisi Guide*. Retrieved August 4, 2021, from kisi: <https://www.getkisi.com/guides/wiegand>
- Koetsier, J. (2020, May 11). *Scammers Send 3.1 Billion Domain Spoofing Emails A Day. Here's How to Protect Yourself (And Your Company)*. Retrieved August 17, 2021, from Forbes: <https://www.forbes.com/sites/johnkoetsier/2020/05/11/scammers-send-31-billion-domain-spoofing-emails-a-day-heres-how-to-protect-yourself-and-your-company/#559a509f48cb>
- Krim, J. (2004, August 6). *Passport ID Technology Has High Error Rate*. Retrieved November 30, 2021, from Washington Post | Technology | Special Reports | Privacy: <https://www.washingtonpost.com/wp-dyn/articles/A43944-2004Aug5.html>
- Lal, N. A.; Prasad, S.; Farik, M. (2016, November n/a). *International Journal of Scientific & Technology Research*, 5(11), 246–249. Retrieved August 4, 2021, https://www.researchgate.net/publication/311514269_A_Review_Of_Authentication_Methods
- Levine, D. E., Mason, J., & Hadley, J. (2014). Software Development and Quality Assurance. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*, 6th Edition (6 ed., Vol. 1, pp. 2,224). Hoboken, NJ, USA: John Wiley & Sons. Retrieved September 13, 2022, <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Loney, M. (2001, October 18). *Redesi Worm Reformats C: Drives*. Retrieved August 13, 2021, from ZDNet: <https://www.zdnet.com/article/redesi-worm-reformats-c-drives/>
- Maddox, I. (2021, May 6). *13 Best Practices for User Account, Authentication, and Password Management, 2021 Edition*. Retrieved August 3, 2021, from Google Cloud: <https://cloud.google.com/blog/products/identity-security/account-authentication-and-password-management-best-practices>
- McAfee. (2021, April 4). *McAfee Data Loss Prevention 11.6.x Product Guide | Key features*. Retrieved August 10, 2021, from McAfee: <https://docs.mcafee.com/bundle/data-loss-prevention-11.6.x-product-guide/page/GUID-B5CEFD5F-4E28-4930-ACA8-63CB60F75B00.html>
- McAfee Labs. (2016, April 18). *Unsubscribing From Unwanted Email Carries Risks*. Retrieved August 17, 2021, from McAfee: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/unsubscribing-from-unwanted-email-carries-risks/>
- Najibi, A. (2020, October 24). *Racial Discrimination in Face Recognition Technology*. Retrieved November 30, 2021, from Harvard University | BLOG | SCIENCE POLICY AND SOCIAL JUSTICE: <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>
- Nash, J. (2020, November 3). *Can You See What I Hear? New Ear Biometrics Technique Has a High Accuracy Rate*. Retrieved November 30, 2021, from BIOMETRIC UPDATE: <https://www.biometricupdate.com/202011/can-you-see-what-i-hear-new-ear-biometrics-technique-has-a-high-accuracy-rate>
- NYCriminal Defense - BUKH Law Firm. (2015, n/a n/a). *419 Fraud Explained by a Criminal Defense Lawyer in NY*. Retrieved August 3, 2021, from NYCriminal Defense: <https://nycriminallawyer.com/fraud-charge/cross-border-fraud/419-fraud/>
- Olshan, J. (2013, April 20). *88% of Spreadsheets Have Errors*. Retrieved August 11, 2021, from MarketWatch: <https://www.marketwatch.com/story/88-of-spreadsheets-have-errors-2013-04-17>
- Panko, R. (2014, n/a n/a). *Audits of Operational Spreadsheets*. Retrieved August 11, 2021, from Panko.com: <http://panko.com/ssr/Audits.html>
- PayPal. (2020, n/a n/a). *PayPal Signup*. Retrieved August 6, 2021, from paypal.com: <https://www.paypal.com/us/webapps/mpp/sem/account-selection-signup>
- PayPal. (2023, n/a n/a). *Protection You Need, Peace of Mind You Deserve*. Retrieved July 22, 2023, from PayPal: <https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security>

- Pelline, J. (1997, September 5). *Whitehouse.com Goes to Porn*. Retrieved August 12, 2021, from cnet Tech: <https://www.cnet.com/tech/services-and-software/whitehouse-com-goes-to-porn/>
- Powell, S. G., Baker, K. R., & Lawson, B. (2009, July n/a). Errors in Operational Spreadsheets. *Journal of Organizational and End User Computing*, 21(3), 24–36. Retrieved August 11, 2021 from http://mba.tuck.dartmouth.edu/spreadsheet/product_pubs_files/errors.pdf
- Reuters. (2005, March 20). *Scammers Snag Money on Net Phones*. Retrieved August 3, 2021, from WIRED NEWS: <https://web.archive.org/web/20050322105611/http://www.wired.com/news/privacy/0,1848,66954,00.html>
- Richtel, M. (1997, June 6). *Big News Media Companies Settle With Web Site in Suit on Linking*. Retrieved August 12, 2021, from New York Times: <https://archive.nytimes.com/www.nytimes.com/library/cyber/week/060697totalnews.html>
- Saiki, M., Obayashi, N., Li, S., Harao, K., & Miyake, T. (2019, n/a n/a). Facial Recognition Solution for Offices — Improved Security, Increased Convenience. *NEC Technical Journal*, 14(1), n/a. Retrieved August 4, 2021, from NEC Technical Journal: <https://www.nec.com/en/global/techrep/journal/g19/n01/190110.html>
- Salveggio, E., Lovaas, S., Lease, D., & Guess, R. (2014). Biometric Authentication. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (Vol. 1, p. 2224). Hoboken, NJ, USA: John Wiley & Sons. Retrieved from <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Schwartau, W. (2002). *Pearl Harbor Dot Com*. Interpact Press. Retrieved August 11, 2021 from <https://www.amazon.com/Pearl-Harbor-Dot-Winn-Schwartau/dp/0962870064>
- ScienceDaily. (2016, May 12). *Social Engineering: Password in Exchange for Chocolate*. Retrieved December 4, 2021, from ScienceDaily | Science News: <https://www.sciencedaily.com/releases/2016/05/160512085123.htm>
- SCIF SOLUTIONS. (2021, n/a n/a). *The SCIF SOLUTIONS Difference*. Retrieved August 10, 2021, from SCIF SOLUTIONS: <https://scifsolutions.com/>
- Shein, E. (2020, May 5). *Bad Password Habits Continue with 53% Admitting to Using the Same Password*. Retrieved August 3, 2021, from TechRepublic: <https://www.techrepublic.com/article/bad-password-habits-continue-with-53-admitting-to-using-the-same-password/>
- Stephenson, Z. (2016, May 17). *Fraud Alert: Card Skimmers Discovered at 4 Greenville First Citizens Bank ATM Locations*. Retrieved August 6, 2021, from WNCT News: <https://www.wnct.com/news/fraud-alert-card-skimmers-discovered-at-4-greenville-first-citizens-bank-atm-locations/>
- TechCrunch. (2007, September 16). *reCAPTCHA: Using Captchas to Digitize Books*. Retrieved August 11, 2021, from TC Extra Crunch: <https://techcrunch.com/2007/09/16/recaptcha-using-captchas-to-digitize-books/>
- TechLawJournal. (1999, September 24). *How the “Page Jacking” and “Mouse Trapping” Web Scam Works*. Retrieved August 12, 2021, from TechLawJournal: <http://www.techlawjournal.com/internet/19990924b.htm>
- The Labyrinth Society. (2023, n/a n/a). *Help with the ReCAPTCHA Feature*. Retrieved July 22, 2023, from LabyrinthSociety: <https://labyrinthSociety.org/recaptcha-help>
- U.S. Attorney - Eastern District of New York. (1998, March 19). *Eugene E. Kashpureff Pleaded Guilty to Unleashing Software on the Internet That Interrupted Service for Tens of Thousands of Internet Users Worldwide*. Retrieved August 13, 2021, from U.S. Department of Justice: <https://web.archive.org/web/19990508144332/http://www.usdoj.gov/criminal/cybercrime/kashpurepr.htm>
- U.S. Code. (1994, September 13). *18 U.S. Code §1301 - Importing or Transporting Lottery Tickets*. Retrieved August 3, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/18/1301>
- U.S. Code. (1994, September 13). *18 U.S. Code §1702 - Obstruction of Correspondence*. Retrieved August 4, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/18/1702>
- U.S. Code. (2008, January 7). *18 U.S. Code §1343 - Fraud by Wire, Radio, or Television*. Retrieved August 3, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/18/1343>
- U.S. Code. (2020, October 20). *18 U.S. Code §1030 - Fraud and Related Activity in Connection with Computers*. Retrieved July 23, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/18/1030>
- U.S. Department of Commerce. (n/a, n/a n/a). *InterNIC – Public Information Regarding Domain Name Registration Services*. Retrieved August 13, 2021, from InterNIC: <https://www.internic.net/>
- U.S. Department of Defense. (n/a, n/a n/a). *Defense Advanced Research Projects Agency | About Us*. Retrieved August 13, 2021, from DARPA: <https://www.darpa.mil/about-us/about-darpa>
- U.S. Department of the Treasury. (2021, May 8). *Doing Business with the BEP - Counterfeit Deterrence*. Retrieved August 10, 2021, from U.S. Bureau of Engraving and Printing: <https://www.moneyfactory.gov/counterfeitdeterrence.html>

- U.S. Department of the Treasury. (2021, July 26). *FAQs – Currency Redesign*. Retrieved August 10, 2021, from U.S. Bureau of Engraving and Printing: <https://www.bep.gov/resources/faqs.html>
- U.S. Department of the Treasury. (2021, June 10). *U.S. Currency*. Retrieved August 10, 2021, from U.S. Bureau of Engraving and Printing: <https://www.moneyfactory.gov/uscurrency.html>
- U.S. Federal Communications Commission. (2019, May 8). *FAQs About Junk Faxes*. Retrieved August 3, 2021, from FCC Consumer Guides: <https://www.fcc.gov/consumers/guides/faqs-about-junk-faxes>
- U.S. Postal Service. (2019, July n/a). *How to Contact the U.S. Postal Inspection Service*. Retrieved August 4, 2021, from USPS: https://about.usps.com/publications/pub300a/pub300a_v04_revision_072019_tech_024.htm
- U.S. Securities and Exchange Commission. (n/a, n/a n/a). *Pump and Dump Schemes*. Retrieved August 3, 2021, from Investor.gov: <https://www.investor.gov/introduction-investing/investing-basics/glossary/pump-and-dump-schemes>
- U.S. State of Georgia. (n/a, n/a n/a). *Identity Theft: Emotional Impact*. Retrieved August 6, 2021, from Consumer Protection Division: <https://consumer.georgia.gov/consumer-topics/identity-theft-emotional-impact>
- United States Postal Inspection Service. (2023, February 21). *Counterfeit Stamps*. Retrieved July 11, 2023, from USPS | Scam Articles: <https://www.uspis.gov/news/scam-article/counterfeit-stamps>
- Veridium Trusted Digital Identity. (2020, January 30). *In Numbers: the Cost of Authentication*. Retrieved August 4, 2021, from Veridium: <https://www.veridiumid.com/passwords-cost-authentication-passwordless/>
- Werring, L. (1998, January 5). Easter Eggs in Commercial Software. (P. G. Neumann, Ed.) *The Risks Digest*, 19(53). Retrieved August 11, 2021, from RISKS Forum Digest: <https://catless.ncl.ac.uk/Risks/19/53#subj4>
- Williams, B. (2019, March 19). *The Dangers of Password Sharing at Work: Why You Should Think Twice Before Sharing Your Password with Anyone at the Office*. Retrieved August 3, 2021, from techradar.pro: <https://www.techradar.com/news/the-dangers-of-password-sharing-at-work>
- WordPress. (n/a, n/a n/a). *Welcome to the World's Most Popular Website Builder*. Retrieved August 12, 2021, from WordPress: <https://wordpress.com/>
- Wu, E. (2021, March 17). *Spotting Scammy Emails*. Retrieved August 17, 2021, from U.S. Federal Trade Commission | Consumer Information: <https://www.consumer.ftc.gov/blog/2021/03/spotting-scammy-emails>

6 Availability

FUNDAMENTALS OF AVAILABILITY

Availability refers to appropriate *speed of access* to information. Thus if the *service-level agreement* (SLA) for a DB system stipulates a *quality-of-service* (QoS) level of no more than a specified response time for any transaction, a delay beyond the limit in completing a transaction is a violation of the contractual definition of acceptable availability.

This chapter reviews

- Fundamentals of availability
- Longevity of digital information
- Secure data destruction
- Distributed denial-of-service attacks
- Operating-system crashes



FIGURE 6.1
Response time.

In my consulting work for software producers and users, a case of slow response involved a steep price.

...[A] software supplier in the mid-1980s had promised a response time of 10 seconds or less for all transactions, but one particular operation was taking 43 *minutes*. Because the SLA was violated, the client was threatening to sue the supplier for the entire development cost and the three years of maintenance payments—a total of \$3.8 million in 1986 dollars (about \$9 million in 2024 dollars).¹ Using an online performance tool, it quickly became obvious that the transaction in question was generating an enormous amount of disk I/O (read-and-write operations): 80,000 random-access reads in a particular data set to filter out a few target records using a nonindexed field. Installing and using an appropriate index and compacting the data set on that field as the primary key to provide rapid access to blocks of related records reduced response time to 6 seconds.²

Unacceptable delays in access to information can be serious, especially when the operations are mission critical.

Ransomware can be viewed as an attack on both availability and utility because the data are still present but cannot be decrypted without a key held by the attackers, so the victims can't get to the original data in a timely manner and what they can see is useless. In a serious ransomware attack on hospitals based in Vermont in 2020, staff were unable to use their medical-information systems and had to resort to keeping notes on paper. My wife, who was a neuropsychiatrist at the *Central Vermont Medical Center*, which is part of the *University of Vermont (UVM) Medical Center* said the attack was a complete disaster for everyone. No one could readily access up-to-date information about patients; the hospitals had to reduce patient treatments during the attack and while systems were being restored from backups:

The health system furloughed or reassigned about 300 employees who were unable to perform their jobs when the computer and phone systems were down.

When the IT systems were taken offline, *UVM Medical Center* and affiliated locations canceled or postponed some services, including elective procedures and cancer treatments. In some instances, patients with test results could not be contacted.

The attack cost *UVM Medical Center* around \$1.5 million per day in lost revenue and expenses to restore its computer systems. President and COO of *UVM Medical Center* Steve Leffler, MD, previously said the attack could cost about \$64 million before systems [were] fully restored.³

À LA RECHERCHE DU TEMPS PERDU: ETERNITY IN CYBERSPACE

Everyone makes backups and stores them, right? And everyone keeps archives of electronic data in accordance with legal requirements or organizational policy, right? So, there's never any problem getting older copies of information back in a readable format, right? And historians will have no problems accessing our 1983 *WordPerfect* files and email messages using *CompuServe* and *Prodigy*, right?

Well, no.

Some of us are storing records in ways that make it unlikely we will be able to read them in the long term required for archival use. And archivists are concerned with the loss of historically valuable data. Scholars in particular are concerned about the issue of long-term availability of data:

Key to our culture is that we can disseminate information, and then maintain and access it over time. While we are rapidly advancing from vulnerable physical solutions to superior, digital media, preserving and using data over the long term involves complicated research challenges and organization efforts.

Uwe Borghoff and his coauthors address the problem of storing, reading, and using digital data for periods longer than 50 years. They briefly describe several markup and document description languages like TIFF, PDF, HTML, and XML, explain the most important techniques such as migration and emulation, and present the *OAIS (Open Archival Information System) Reference Model*.⁴

Storing records is only half the task of records management; supporting availability and utility is the essential function. No one wants an unexpected WOM (*write-only memory*) for their records. For short-term storage, there is no problem ensuring that stored information will be usable. Even if a software upgrade changes file formats, the previous versions are usually readable and there are file-conversion utilities⁵ available for conversions.

The problems of obsolescence include hardware incompatibilities, software incompatibilities, and data degradation.

HARDWARE OBSOLESCENCE

Over recent decades, certain physical forms of storage have become essentially unusable. As an example, *AES*⁶ was a powerful force in the dedicated word-processor market in the 1970s; eight-inch disks held dozens or hundreds of pages of text and could be read in almost any office in North America. By the late 1980s, *AES* had succumbed to word-processing packages running on general-purpose computers; by 1990, the last company supporting *AES* equipment closed its doors. Today, it would be extremely difficult to recover data from *AES* diskettes because of the difficulty of finding the hardware to read them.

A long-running joke among computer nerds is that a child seeing a 3.5-inch floppy disk for the first time exclaims, "Wow! You have a 3D representation of the SAVE icon!" I lost any way of reading such disks decades ago. And when I think back to running the technical services at a major computer-service bureau in the 1980s, I wonder how anyone today could read the thousands of reels of magnetic tape that we stored as backups in a climate-controlled storage room that was 10×20 meters in size.

Another problem is that magnetic media degrade over time. Over a period of a few years, thermal disruption of magnetic domains gradually blurs the boundaries of the magnetized areas, making it harder for I/O devices to distinguish between the domains representing ones and those representing zeroes. These problems affect tapes, diskettes, and magnetic disks and cause increasing parity errors.⁷ Specialized equipment and software can compensate for these errors and recover most of the data on such old media provided they are physically readable.



FIGURE 6.2 Eternity.



FIGURE 6.3 Obsolete data storage.

Magnetic tape suffers from an additional source of degradation: The metal oxide becomes friable and begins to flake off the mylar backing.⁸ Such losses are unrecoverable. They occur within a few years in media stored under inadequate environmental controls and within five to ten years for properly maintained media. Regular regeneration by copying the data before the underlying medium disintegrates and writing it to new media prevents data loss.

Optical disks, which use laser beams to etch bubbles in the substrate, are much more stable than magnetic media. However, no one knows how long optical disks such as CD-ROMs and DVDs will last; nonetheless, technologists predict that the information will remain readable for decades and more. They will remain readable if and only if future optical systems include *backward compatibility*.⁹

Finally, even hardware eventually becomes impossible to maintain. It would be extremely difficult to retrieve and interpret data from word-processing equipment from even 20 years ago. And no one outside museums or hobbyists can read an 800 bpi 9-track ¾-inch magnetic tape from a 1980 HP3000 Series III minicomputer. Over time, even such parameters as electrical-power attributes may change, making obsolete equipment difficult to run even if they can be located.

SOFTWARE OBSOLESCENCE

Software incompatibilities include *application software* and *operating systems*.

The data may be readable, but will they be usable? Manufacturers provide backward compatibility, but there are limits. For example, WordPerfect 6.1 could convert files from earlier versions of *WordPerfect* – but only back to version 4.2. Over time, application programs evolve and drop support of the earlier data formats. Database programs, email, spreadsheets – all of today’s and tomorrow’s versions may have trouble interpreting data files correctly.

In any case, all conversion raises the possibility of data loss since new formats are not necessarily supersets of old formats. For example, in 1972, *RUNOFF*¹⁰ text files on IBM mainframe systems (and later on *Digital Equipment Corporation* – DEC – machines) added instructions to pause a daisy-wheel impact printer so the operator could change daisy wheels – but there was no requirement to document the desired daisy wheel. The operator made the choice. What would document conversion do with *that* instruction?

Operating systems evolve. Programs intended for the *Microsoft Disk Operating System* (MS-DOS) of decades ago do not necessarily function on today’s Windows systems. And the operating systems of yesteryear do not necessarily run on today’s hardware. Even emulators that run versions of one operating system on a machine running a different operating system can cause problems because, again, there is no guarantee of compatibility between the emulated system and the emulator.¹¹

Finally, even hardware eventually becomes impossible to maintain. As mentioned above, it would be extremely difficult to retrieve and interpret data from word-processing equipment from decades ago. No one outside museums or hobbyists can read an 800 bpi 9-track ¾-inch magnetic tape from a 1980 *HP3000 Series III* minicomputer. Over time, even such parameters as electrical power attributes may change, making obsolete equipment difficult to run even if they can be located.

The most robust method developed to date for long-term storage of data is COM (*Computer Output to Microfilm*).¹² Documents are printed to microfilm, appearing exactly as if they had been printed to paper and then microphotographed. Storage densities are high, storage costs are low, and in the worst case, the images can be read with a source of light and a simple lens. I sometimes imagine an earnest scholar in a non-industrialized post-apocalyptic world of the 26th century struggling to read ancient documents using a candle and an old magnifying glass.¹³

Information security demands us to be able to read old data: It is time for us to pay serious attention to long-term storage technologies.



FIGURE 6.4
Obsolete code.

STABLE URLs AND SCHOLARLY REFERENCES

The Web is not merely a marketing medium – it is an important part of the shared information space of humanity. Unfortunately, scholars are having trouble with the fluid nature of the Web because many people continue to treat their own documents with little regard to how others use them.

For all scholarly work, documents used in preparing a report must normally be referenced so that readers can pursue a point or check a statement for correctness. However, documents placed on websites appear, change, and disappear with breathtaking rapidity compared with the glacial stability of academic journals filed in library stacks.

This issue was addressed by Jerry Leichter in the *RISKS DIGEST* 20.14 on 1999-01-13 in his contribution “Now you see it, now you don’t.” He noted that a *Stanford University* research group formed a new company and removed all its reports from the Web:

I am concerned about the removal of previously-public research material. We hear repeated complaints that traditional journals don’t accept URL’s as bibliographic citations. If *even a university research department* approves the removal of on-line versions of its own research papers, how can we take the Web seriously as a resource for scholarship?¹⁴

At the beginning of March 2000, I attended the *9th Annual EICAR Conference* in Brussels. At the meeting of the *Task Force on Outreach and Education*, I raised the issue of unstable URLs for documents and was surprised and delighted by the thoughtful measures already in place to prevent “Document not found” messages – often known as “404s.”

EICAR uses URLs with a unique and permanent document ID to avoid getting a 404 when the URL of document changes. References to EICAR documents are actually calls to the search engine and the parameter serves as the key to retrieval. Even if all the documents were to be reorganized, the reference would remain stable as long as the URL of the search engine were the same.

Even if the location of the site were to shift (e.g., from a .dk address to a .de address), the document numbers would still be able to identify the right documents on the new site.

On the other hand, when document content changes but not the name, as in new versions, the default procedure at EICAR is to replace the content but keep the ID. I think this is a mistake, since scholarly articles may refer to parts of an earlier version that could be changed or disappear in a later version. I think that new versions should at minimum have a reference to the previous version’s (new) ID.

Wikipedia poses a particular problem for scholars: The *content* of articles may change at any time. A notorious case concerns the *Wikipedia* article about Paul Revere. In May 2011, Sarah Palin, an extreme right-wing U.S. politician, mistakenly claimed that Paul Revere rode to warn the *British* on his famous midnight ride. She stuck to her view in interviews.¹⁵ Her acolytes then began trying to change the *Wikipedia* entry about Paul Revere to conform to their cult leader’s assertions and caused a ruckus in the *Wikipedia* community.¹⁶ As a result of this kind of potential instability, my instructions to students include the warning, “*Wikipedia* may be used to locate resources but may *not* be used as a primary reference.”¹⁷

If an organization closes its website (e.g., if the organization goes out of existence), it would be good if the website documents were transferred to another site and a stub left in place to redirect references to the new site. The use of unique IDs would be very useful in such redirection. The new custodian of the documents could even prefix the old ID with a data segment referring to the original location so that documents would not get lost. For example, if the MEGA.ORG website had a document 1234, perhaps a request for that document could be translated to document ID MEGA-1234 on the custodian’s site.

In recent years, the *Internet Archive* (“*Wayback Machine*”) discussed in the next section has provided a valuable service by providing access to copies of webpages that have disappeared.



FIGURE 6.5
Unstable URLs.

THE WAYBACK MACHINE™

“Rocky and His Friends” was a cartoon series for children, later renamed *Rocky & Bullwinkle & Friends*© and *The Bullwinkle Show*© that ran from 1959 to 1963.¹⁸ Two of the regular characters were a professorial beagle, Mr Peabody, and his human child Sherman; they would regularly go back into the past using the “WABAC Machine.”¹⁹

The *Internet Archive* provides access to “millions of free books, movies, software, music, websites, and more”²⁰ and runs the *WayBack Machine*™:

One of the more infuriating things about the Internet is when a website closes down.

You might follow a favorite writer’s blog, save links to helpful articles, and share interesting posts on social media. But then one day, you return to the website to discover that it is gone.

The site does not exist anymore. All of the useful stories and information are now missing. It is like they never existed.

The good news is that you may be able to find those sites again, even after they are offline. You can find help from a website called the WayBack Machine.

....

The WayBack Machine site shows a kind of history of the Internet. It shows websites that are no longer online and older versions of current sites.

....

The WayBack Machine provides archived records of publicly available websites. Not all websites or versions of sites are available, but many are.²¹



FIGURE 6.6 The Internet Archive.

In this textbook, there are many cases where I found that the only source available for old but useful documents from websites was the *WayBack Machine*. To locate a missing page, one puts the URL into the search field and a graph of archival entries appears. Clicking on a dot brings up the archived page.

The concern remains that if our planet loses the Internet, (or for that matter, if there are no computers at all in a post-apocalyptic wasteland), we will be in trouble with respect to continuity of knowledge.

APPROPRIATE GUIDELINES FOR DATA DESTRUCTION

In December 2001, *Enron*, a major energy company, declared bankruptcy after corrupt practices that cheated its investors and concealed gross negligence in part through data destruction:

Arthur Andersen was one of the first casualties of *Enron*’s notorious demise. In June 2002, the firm was found guilty of obstructing justice for shredding *Enron*’s financial documents to conceal them from the SEC [*Securities and Exchange Commission*]. The conviction was overturned later, on appeal; however, the firm was deeply disgraced by the scandal and dwindled into a holding company.²²

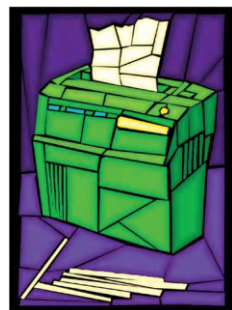


FIGURE 6.7 Paper shredder.

The case was described by authorities as

...[T]he most complex white-collar crime investigation in the FBI's history.

The sheer magnitude of the case prompted creation of the multi-agency *Enron Task Force*, a unique blend of investigators and analysts from the FBI, the *Internal Revenue Service-Criminal Investigation Division*, the *Securities and Exchange Commission*, and prosecutors from the *Department of Justice*.

Agents conducted more than 1,800 interviews and collected more than 3,000 boxes of evidence and more than four terabytes of digitized data. More than \$164 million was seized; ... about \$90 million [was] forfeited to help compensate victims. Twenty-two people [were] convicted for their actions related to the fraud, including *Enron's* chief executive officer, the president/chief operating officer, the chief financial officer, the chief accounting officer, and others.²³

With the popular and technical press reporting extensively on the *Enron* scandal, where data destruction played a role in the interpretation of how *Enron's* accountants behaved, many organizations reconsidered their own data-retention and data-destruction policies. A colleague submitted the following (edited) question received from a client in 2002:

We are seeking your advice on the issue of how we destroy records. We're currently working with various vendors on proposals and if shredding is determined to be a corporate policy, then a company-wide policy would be needed to achieve the best price. It would also determine the vendors we could deal with, since we might want a single vendor to support all regions. The paper-recycling companies won't take responsibility for confidentiality of our data, since information security is not part of their business. In contrast, shredding companies will pick up discarded materials from locked cabinets and even transport materials in a locked truck if necessary; they accept responsibility for our information from beginning to end. Can we legitimately shift the liability and responsibility to a third party through the contract? Can you provide us with any industry standards on handling destruction and what companies are doing in light of the *Enron* issue or because of the growing emphasis on privacy? If the expectation is that shredding will become a preferred method for destroying customer information then we should push to clean things up in 2002 and budget for costs expected in 2003, when we would start shredding lots of materials.

I explained that before engaging in any new data destruction, the client would do well to consult corporate counsel to establish the legal requirements that contribute to determining appropriate data-retention policies. Different classes of data will have different retention periods mandated by law, regulations, or business requirements such as due diligence investigations preceding mergers and acquisitions.

The idea of using a single contract for all sites is appealing: It ties into the principle that policies should be applied as uniformly as possible (with due allowance for special cases). For example, in a court of law, it would be tedious and even embarrassing to have to detail the precise data-retention and data-destruction policies for a dozen locations, each of which had significant but largely unwarranted variations in their practices.

There are many secure-shredding firms; a service that helps organizations in the United States find reputable and suitable companies is *Shred Nations*.²⁴ It includes listings for shredders that come to a site for data destruction or those that let customers ship their materials to a local facility. The services can handle not only paper, but also "hard drives, x-rays and cell phones."

Specialized shredding companies do indeed accept responsibility for documents *once they have control* over the paper or other media; however, they cannot take responsibility for what is done to data *before* they are discarded. Since employees have by far the largest opportunity for data destruction, mis-filing, or theft, each organization will naturally keep the largest responsibility for data confidentiality and face the greatest liability for compromise of confidential data – not to speak of losses incurred through data scavenging by industrial spies or criminal hackers.

It will take time to train employees to use special lock boxes to discard confidential documents; many will, at first, continue unconsciously to throw sensitive documents in ordinary trash or to place them in ordinary unprotected recycling bins.

Any change in policies on data destruction should be closely coordinated with the IT group to be sure that backups and archives are included in the analysis. Electronic or optical archives of documents, including email – and including backups – are a rich source of data mining during the legal discovery process. In addition, the client should examine the distribution of documents it wishes to destroy but which reside on employees' desktops, laptops, or even personal home computers. Unfortunately, many users have no idea that copying company information onto their home computers poses a security risk; in addition, many novices store documents higgledy-piggledy in a single folder (e.g., "My Documents") with no subfolders, with useless generic filenames such as "Document.docx" and with empty property sheets that convey nothing about the subject matter or provenance of the documents. Finding and extirpating all copies of documents that ought to be destroyed may be much harder than it seems at first glance.

As for starting to shred paper documents on a large scale, there are some public-relations issues as well as legal issues to consider. Before engaging in any new data destruction, I would ensure that the IT and documents staff consult the corporate counsel to be sure that there are no legal proceedings anticipated. For example, it would be embarrassing to have public disclosure of widespread data destruction, even though perfectly legal, just before a court-ordered discovery was due to start. That was precisely what happened in the *Enron* case before the court orders were served.

It will be critically important to ensure that nothing is destroyed that is in fact clearly useful or needed. In their enthusiasm for getting rid of superfluous materials, it is quite likely that some employees will go overboard and destroy documents that the organization actually wants to keep available. This risk is especially serious when people start the perhaps unfamiliar process of destroying magnetic or optical media. Many users have a lamentable habit of not labeling their storage media, or worse, reusing materials with an old and incorrect label. If employees start throwing out these storage media without accurately evaluating the importance of the information carried on these devices, the organization may suffer irretrievable losses and possibly serious legal consequences.

If system documentation is inadequate, it is also possible that untrained personnel may *forget* or be *unaware* of cloud backups.²⁵ Some employees may not know that their data in, say, *Dropbox* is being stored online; the advantage is that cloud-backup services may keep dated backups that are useful if the original files are lost; the disadvantage is that cloud-backup services may keep dated backups that violate policies on data retention or that contain confidential information that can be misused.

Organizations should lay out clearly understandable, unambiguous standards for electronic-data destruction. It should be possible to go through a checklist that leads a user to a firm conviction that destroying a particular dataset is completely appropriate, completely inappropriate, or questionable. The questionable cases should be discussed with a supervisor. The unambiguous decisions should be documented so that the organization has a permanent record of what was destroyed in the cleanup. Now, excessive detail might defeat the purpose of the data destruction, so the data-management guidelines should include examples of suitable notations for tracking the data destruction. The subject of dealing with criminal behavior is outside the scope of this section, but at the very least, management should make it clear in its policies that destroying data indicating criminal activity is *not* a legitimate process and that the organization's policies explicitly forbid cover-ups of any such criminality. In a well-run organization, any employee who has reason to suspect criminal behavior by colleagues and who is nervous about reporting such evidence within the chain of responsibility should be *encouraged* to contact law-enforcement organizations for help.

LESSONS FROM DDoS

As most readers know, DDoS attacks can involve the unauthorized installation of special client software on hundreds or perhaps thousands of poorly secured computer systems linked to the Internet.²⁶ These so-called *slave* or *zombie* programs sit passively on the damaged systems waiting for encrypted commands from the appropriate “*master*” program. The slaves are ready to bombard a selected target of a particular time with a flood of unwanted traffic. The volume is high enough to cause serious slowdowns in server response to user requests, in some cases the servers crash.



FIGURE 6.8
Zombie programs.

Security experts have been warning for years that the Net is vulnerable to *denial-of-service* (DoS) attacks. Donn Parker warned of automated computer crime in his 1998 book, *Fighting Computer Crime: A New Framework for Protecting Information*.²⁷ By mid-2021, a major study revealed

...a staggering 50% increase in peak attack traffic compared to 2019, with a jump to 1.18 Terabytes per Second (TBps) or 887 Mega Packets Per Second (Mpps).

In 2020, a staggering 57 Petabits or 14 tera packets of malicious data have been cleaned. During the same period, the average size of a DDoS attack was 19 Gbps (23 Mpps), with an average duration of 10 minutes.²⁸

Is there anything we can do about these attacks? Security expert Paul Rubens published an excellent summary in 2013 and updated his article in 2016 and 2018. He wrote that “We can defend target systems to make it harder for the attackers to overwhelm them.”²⁹ Here are his suggestions (with my own explanations).

1. *Identify the DDoS attack early*: Automatically track the patterns of access and alert staff as soon as an overload begins.
2. *Overprovision bandwidth*: Design or contract for more capacity than you normally expect.
3. *Defend the network perimeter*: Define maximum transfer rates for routers, drop malformed or spoofed packets and terminate connections that stay incomplete too long.
4. *Call your ISP or hosting provider*: Let them know as soon as possible that you are under attack.
5. *Call a DDoS-mitigation provider*: These companies can switch traffic from the target website to a system with far larger bandwidth to allow legitimate users to continue having access, even if slower than usual.
6. *Create a DDoS playbook*: Define precisely how to identify and respond to a DDoS attack to minimize damage and to keep users (or customers) informed of the situation.

Similar recommendations are widely reported by other security specialists.^{30,31,32}

A more general message is that everybody using the Net has a social responsibility as well as a professional obligation to patch all known vulnerabilities in *both business and personal systems* so criminals cannot exploit weakly secured systems to attack strongly secured systems.

At least some of the attacks may involve headers with spoofed originator addresses; no site should *ever* allow packets with forged headers to get *out* of their perimeter through their firewalls.³³

In the medium run, we need to impose more demanding volume testing on all systems as a normal part of quality assurance. Another improvement in current network systems would be to integrate some of the artificial-intelligence routines that have been applied in modern IDSs to recognize bogus traffic and block it before the spurious requests and data can bog down critical servers.

In the longer run, we may have to agree on methods for strong authentication of Internet traffic. I hope to see a day when all packets on the Internet will be digitally identified to include the real IP addresses of the originators; those systems refusing to use digital signatures will have their

packets classified as low-priority traffic. Using a system of cryptographically sound packet checksums including packet sequence numbers will make it possible to establish a trustworthy session with trustworthy partners. Anyone not playing by the rules would be relegated to low-priority transfer and would have much more trouble trying to deliver a DoS attack.

In some ways, such a system would resemble what we already do with paper mail. We recognize and often discard unsolicited commercial mail without even having to open it. Our tolerance for junk mail declines when we become busier. These easy measures institute an informal triage based on our natural evaluation of our own processing power. Similarly, with adequate I&A of Internet packets, routers could decide which packets deserved immediate attention and which ones would have to wait for attention.

Another possible tool in the fight against DDoS will be a universally accessible service where DDoS traffic would automatically be reported in real time; any system could check for reports of suspect traffic immediately to speed the response to the initiation of a DDoS.

AN EARLY DDoS CASE: “MAFIABOY”

More than two decades ago, one of the first widespread DDoS attacks caused a flurry of concern in February 2000. News reports exploded as police authorities in Canada, the United States, and other countries scrambled to find out who brought down *Amazon*, [Buy.com](#), *CNN*, *Dell*, *eBay*, *Excite*, *U. Mass.*, *U. Cal. Santa Barbara*, *Yahoo*, and other prominent websites. Investigators tracked the attacks to Michael Calce, Montreal-area youth who called himself *Mafiaboy* in the hacker underground.³⁴



FIGURE 6.9
Criminal hacker.

A 15-year-old boy [was] charged with two counts of computer mischief for crippling the CNN website and 1,200 related sites in a cyber attack....

Cyber attacks against *CNN*, *Yahoo!*, *eBay*, *Amazon*, *ETrade* and other major web sites in February inconvenienced millions of users and raised questions about Internet security.

The apparently coordinated attacks overloaded the sites with a barrage of messages generated by hackers.³⁵

The youth, was caught when *Royal Canadian Mounted Police* wiretaps captured him bragging about his exploits:

Mafiaboy had bragged in online chats and to friends that he had taken down [CNN.com](#), [Amazon.com](#), [Buy.com](#), *eBay*, and *E-Trade*, but they didn't believe him. Federal law-enforcement officials in Canada and the United States took note, however, following up on tips and tracing the electronic path that led to Mafiaboy's neighborhood in the West Island section of Montreal, sources familiar with the probe said.³⁶

The boy eventually pled guilty to 58 counts of mischief for launching the DDoS attacks against sites in the United States, Canada, Denmark, and Korea. He was sentenced to eight months in juvenile detention and a year of probation after that. In addition,

Mafiaboy [was] forbidden from profiting in any way from the incident until he has served his probation.

Mafiaboy [was] also prohibited from possessing any software that's not commercially available; he [could not] use the Internet to talk with any other hacker; and he [was] banned from hacking into any other sites....

...[T]he youth [was] required to donate \$250 to a Montreal charity for violating the terms of his bail, which said he had to attend school and be on his best behavior. The prosecutor said Mafiaboy had been suspended from school, which violated his bail provisions.³⁷

What strikes me about this case is the self-reported attitude of the young hacker when he was arrested. According to his own book, he was defiant in his interviews with police authorities. He stood by silently while one of his school friends publicly lied by identifying an innocent child as Mafiaboy:

I watched Vito walk out of the school and swagger up to the gaggle of cameras and reporters. He told the assembled press that he knew Mafiaboy's real name and then proceeded to reveal it. Except Vito didn't offer me up – he picked another student at the school, somebody we thought was kind of a loser. He told the press that that student was their man.... There was such mayhem that the boy was sent home from school early. I heard that the press followed him to his house.

As much as the situation was freaking me out, Vito managed to give me a laugh and help me feel a little bit better. I was so concerned about my own circumstances that I didn't feel any remorse over what we had done to that student. I regret the trouble I must have caused him. I can only imagine how frightened and confused he and his family must have been.³⁸

The guilty boy was surrounded by adults who knew nothing about computers (his dad had no idea what a modem was when he bought one for his son) and did not themselves grasp or admit the gravity of the crimes he carried out. Stock prices of some of the affected sites dropped noticeably during and immediately after the attacks and estimates of lost business reached into the millions of dollars.

At the time, I wrote that the public did not understand the consequences of criminal hacking. Network specialists should help to change this lack of knowledge by contributing to education of students, teachers, and parents. I urged adults to talk to youngsters about computer crimes so that these assaults on increasingly essential societal infrastructure can be rejected by normal children.³⁹

TRANSGRESSING THE UNWRITTEN LAW

Most people who have spent more than five minutes with me know that I am afflicted with a severe case of *Monty Python*⁴⁰ addiction. Indeed, I was the founder of the *Norwich University Monty Python Society* which met every week for a couple of years to watch episodes of the group's complete shows and sections of their movies. At the 2006 graduation of students of the *Norwich University School of Graduate Studies* (SGS), my arrival at the podium was greeted by a chorus of high-pitched cries of "Ni! Ni!"⁴¹ from dozens of graduating *Master of Science in Information Assurance* (MSIA) students, much to the dismay of the assembled dignitaries. At the SGS, I corrupted many of my colleagues into greeting each other with, "G'day Bruce! G'day Sheila!" in various approximations of an Australian accent.⁴²

The disease began when I was a graduate student at *Dartmouth College* from 1972 to 1976 and foolishly played recordings of *Monty Python* skits over and over while I was doing laboratory work; the skits were permanently burned into my brain. Even my saintly wife, who doesn't even *like the old TV show*, has come to utter occasional phrases such as "Yes, well, that's the sort of blinkered Philistine pig ignorance I've come to expect from you non-creative garbage."⁴³

I mention all this mostly for fun but also because of an incident I experienced in the mid-2000s while using the now-extinct *Yahoo Groups*⁴⁴ to organize collaboration among contributors to the Fifth Edition of the *Computer Security Handbook*. I was just setting up the group message board by loading one message per chapter so that collaborators could begin adding their discussions as threaded messages appended to each discussion head when I was suddenly barred from my own group. A cryptic message from *Yahoo* informed me that my account had been removed from the group because it was "tagged as an auto-responder." There was no further explanation.

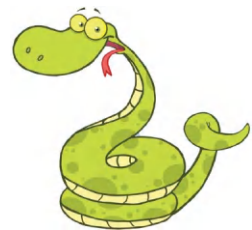


FIGURE 6.10 Python but not Monty.

A bit of exploration revealed the following explanation in the *Group Managers Forum* on Yahoo:

Did your address get tagged as an auto-responder? That occurs when you send too many messages to Yahoogroups.com in too short a time span.

1 - This can happen when you compose replies and posts offline and then email the bunch of messages all at once when you're online.

2 - Of course, it can happen when you set you mail service to send an auto-response like, "Hi! I'm on vacation and will return next weekend."

3 - It can also happen if a virus or spammer just happens to "spoof" your email address as the "From:" and send a bunch of spew to addresses "yahoogroups.com". (And, Yes, this can and does happen and there's nothing you can do about it!) ⁴⁵

Well, #1 was it! I had loaded 76 messages in a few minutes using cut/paste operations to so quickly that the automated system blocked me.

Now for the *Monty Python* reference. I searched to no avail for any warning about this problem in the *Yahoo Groups* documentation. The situation thus reminded me of the classic lines from *The Piranha Brothers*:

Interviewer: Stig, I've been told Dinsdale Piranha nailed your head to the floor.

Stig: No, no. Never, never. He was a smashing bloke. He used to give his mother flowers and that. He was like a brother to me.

Interviewer: But the police have film of Dinsdale actually nailing your head to the floor.

Stig: Oh yeah, well – he did that, yeah.

Interviewer: Why?

Stig: Well he had to, didn't he? I mean, be fair, there was nothing else he could do. I mean, I had transgressed the unwritten law.

Interviewer: What had you done?

Stig: Er... Well, he never told me that. But he gave me his word that it was the case, and that's good enough for me with old Dinsy. I mean, he didn't want to nail my head to the floor. I had to insist. He wanted to let me off. There's nothing Dinsdale wouldn't do for you. ⁴⁶

Moral: If you are setting up automated rules with drastic consequences for availability and utility on your networks, you might want to let people know about them in advance.

FEEDBACK FROM BAD OPERATING SYSTEMS

At a security conference in the 1990s, I asked a quality-assurance expert from *Microsoft* how often, on average, computers running *Windows 9x* operating systems⁴⁷ crashed per day. Colleagues around the lunch table chimed in with a wide range of estimates from twice a day to once every two days. Everyone laughed when I pointed out that a rollover problem with a counter in the operating system meant that no *Windows 9x* system could run longer than 49.7 days⁴⁸ – the very idea that a *Windows 9x* system could possibly run without crashing long before that limit struck everyone as ludicrous.

I suspect that no one knew in any detail back then just how often and why *Windows 9x* systems were crashing. The brutal fact was that *Windows 9x* systems crashed so often that an entire generation of computer users thought it was normal for an operating system to crash at least a few times a week. Part of the problem was that there was no security kernel, so that all programs ran as root and could make changes all over memory, even in other processes' stacks and pointers:



FIGURE 6.11
The Blue Screen of Death.

The root cause for all this instability is the fact that the Windows 9x operating system kernel was basically a cobbled-together version of the cold *Disk Operating System* (DOS) kernel. While DOS was a whiz kid in its heyday, it really wasn't designed to support a graphical user interface (GUI) or the type of multitasking that Windows 9x aspires to achieve. Basically, this means that Windows 9x was so busy with its juggling act that a tiny failure at any point could bring the whole operating system tumbling down.⁴⁹

In contrast, when I ran a data center in the 1980s, the *HP3000*⁵⁰ systems running the *Multi-Programming Executive* (MPE) we used as we serviced 1,000 users in 28 companies for 24/7 availability crashed so rarely – perhaps once in several weeks or months – that every event was logged and reported to HP. We took *core dumps* (copies of main memory) and I analyzed them to determine exactly which process had caused the system failure.⁵¹ HP recorded the problems and published a biweekly (paper) report called the *Software Status Bulletin* to warn users of known problems and propose patches or workarounds if possible.

This system also allowed HP customers to judge when it was safe to install new revisions of the operating system. I waited until the number of new problem reports per month had dropped to the baseline with which we were comfortable.

Now granted, there are many operating-system and application-program bugs that were and are indeed reported in the *Microsoft Knowledge Base*⁵², and I do congratulate the company on its commitment to customer service. Nonetheless, I guess that a lot of people, like me, simply rebooted our systems with a snarl and didn't even bother telling the vendor that there was a problem.

Back in 2000, I published an article in *Network World* suggesting that operating-system manufacturers and the creators of other kinds of software too offer users the option to enable automatic logging and communication of failures to the parent companies. Many users would be glad to enable such a function as long as the load were not too onerous on the connection (an unlikely problem) and if they were convinced that the company were genuinely protecting their privacy. Such protection could be achieved by using the unique processor ID available in new-generation processors and refraining from linking processor IDs to real-world data.

There are now dozens of bug-tracking tools available that can be integrated into software products.⁵³ With these tools, organizations can concentrate their efforts on the bugs causing the most frequent problems in the real world instead of depending only on the biased sample of people who bother to send in problem reports. In an ideal world, such statistics would actually be published openly so that users could monitor the state of new operating system and other software revisions and make informed choices about when to upgrade their systems.

As I wrote two decades ago, I hope that all software developers will adopt bug-tracking for all their products.

NOTES

- 1 [CoinNews Media Group LLC \(2021\)](#).
- 2 Kabay, Holden, and Walsh, *Operations Security and Production Controls* (2014).
- 3 [Dyrda \(2020\)](#).
- 4 [Borghoff, Rödigg, Scheffczyk, and Schmitz \(2007\)](#).
- 5 NCH Software.
- 6 Centre for Computing History.
- 7 [Morgan \(2018\)](#).
- 8 [Council on Library and Information Resources \(2018\)](#).
- 9 [Byers \(2003\)](#).
- 10 [Saltzer \(1964\)](#).
- 11 [Johnson and Antonelli \(2020\)](#).
- 12 [Reference* \(2020\)](#).
- 13 [Miller \(1959\)](#).
- 14 [Leichter \(1999\)](#).
- 15 [Palin \(2011\)](#).

- 16 Gaudin (2011).
- 17 Kabay, Term-Project Guidelines (2020).
- 18 Internet Movie Database (2021).
- 19 Rocky and Bullwinkle Fandom.
- 20 Internet Archive (2021).
- 21 Mohr (2017).
- 22 Segal (2021).
- 23 U.S. Federal Bureau of Investigation (2016).
- 24 Perlmutter (2019).
- 25 Muchmore and Moore (2021).
- 26 Cloudflare (2021).
- 27 Parker (1998).
- 28 HelpNetSecurity (2021).
- 29 Rubens (2018).
- 30 Giese (2020).
- 31 Geerts (2021).
- 32 Hewitt (2021).
- 33 Gezelter (2000).
- 34 Hersher (2015).
- 35 AP in Montreal (2000).
- 36 Pearlstein and Vise (2000).
- 37 Rosencrance (2001).
- 38 Calce and Silverman (2008).
- 39 Kabay, Ethics: Papers discussing ethical principles applied to the use of computers and communications technology (2021).
- 40 Monty Python (2021).
- 41 Monty Python (2009).
- 42 Monty Python (2007).
- 43 Monty Python (2020).
- 44 Yahoo! Groups (2006).
- 45 Yahoo! Groups (2007).
- 46 Monty Python (1970).
- 47 Microsoft (2015).
- 48 Microsoft (1999).
- 49 Schultz (2003).
- 50 BGImages Australia (2021).
- 51 I can't resist recounting one of my favorite conversations with a customer when I was on *Phone-In Consulting Service* for HP in the early 1980s. A major customer reported a system failure, so I asked, "Have you taken a dump?" There was a long pause and the customer said, "Uh, no, but why do you ask?" I said, "A *memory dump*" and he hurriedly said, "Oh, yeah, I took that."
- 52 Microsoft (2021).
- 53 Software Testing Help (2021).

WORKS CITED

- AP in Montreal. (2000, April 19). '*Mafiaboy*' charged with cyber-terrorism. Retrieved August 24, 2021, from Guardian: <https://www.theguardian.com/world/2000/apr/20/terrorism>
- BGImages Australia. (2021). *3000 Selections*. Retrieved August 31, 2021, from <http://www.hpmuseum.net/exhibit.php?class=3&cat=32>
- Borghoff, U. M., Rödiger, P., Scheffczyk, J., & Schmitz, L. (2007). *Long-Term Preservation of Digital Documents: Principles and Practices*. Springer Science & Business Media. Retrieved August 18, 2021, from https://play.google.com/store/books/details?pcampaignid=books_read_action&id=sZpm0dBV5MwC
- Byers, F. R. (2003, October). *Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists*. Retrieved August 18, 2021, from CLIR: <https://www.clir.org/wp-content/uploads/sites/6/pub121.pdf>
- Calce, M., & Silverman, C. (2008, January 1). *Mafiaboy: How I Cracked the Internet And Why It's Still Broken*. Retrieved August 24, 2021, from Silo.Pub: <https://silo.pub/mafiaboy-how-i-cracked-the-internet-and-why-its-still-broken.html>

- Centre for Computing History. *AES Office Automation*. Retrieved August 18, 2021, from Computinghistory: <http://www.computinghistory.org.uk/det/8195/AES-Office-Automation/>
- Cloudflare. (2021). *What is a DDoS Attack?* Retrieved August 23, 2021, from <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
- CoinNews Media Group LLC. (2021). Retrieved from US Inflation Calculator: <https://www.usinflationcalculator.com/>
- Council on Library and Information Resources. (2018, August 27). *What Can Go Wrong with Magnetic Media?* Retrieved August 18, 2021, from CLIR: https://www.clir.org/pubs/reports/pub54/2what_wrong/
- Dyrda, L. (2020, December 23). *Inside UVM Medical Center's Ransomware Attack: 11 Details*. Retrieved August 17, 2021, from Becker's Health IT: <https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html>
- Gaudin, S. (2011, June 6). *Sarah Palin Fans Try to Rewrite History on Wikipedia: Former Governor's Supporters Battle With Wikipedia Editors Over Paul Revere Page*. Retrieved August 19, 2021, from ComputerWorld: <https://www.computerworld.com/article/2509040/sarah-palin-fans-try-to-rewrite-history-on-wikipedia.html>
- Geerts, T. (2021, June 4). *7 Simple But Effective Tactics to Protect Your Website Against DDoS Attacks in 2021*. Retrieved August 24, 2021, from Cloud Security Alliance: <https://cloudsecurityalliance.org/blog/2021/06/04/7-simple-but-effective-tactics-to-protect-your-website-against-ddos-attacks-in-2021/>
- Gezelter, R. G. (2000). Personal communication. (M. E. Kabay, Interviewer).
- Giese, G. (2020, December 16). *10 WAYS TO PROTECT AGAINST DDOS ATTACKS*. Retrieved August 24, 2021, from The Akamai Blog: <https://blogs.akamai.com/2020/12/10-ways-to-protect-against-ddos-attacks.html>
- HelpNetSecurity. (2021, July 22). *DDoS attacks are up, with ever-greater network impact*. Retrieved August 23, 2021, from HelpNetSecurity | News: <https://www.helpnetsecurity.com/2021/07/22/ddos-attacks-up/>
- Hersher, R. (2015, February 7). *Meet Mafiaboy, The 'Bratty Kid' Who Took Down The Internet*. Retrieved August 24, 2021, from NPR | All Tech Considered: <https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet>
- Hewitt, K. (2021, August 16). *10 Best Practices to Prevent DDoS Attacks*. Retrieved August 24, 2021, from SecurityScorecard: <https://securityscorecard.com/blog/best-practices-to-prevent-ddos-attacks>
- Internet Archive. (2021, July 21). *Top Collections at the Archive*. Retrieved August 19, 2021, from Internet Archive: <https://archive.org/>
- Internet Movie Database. (2021). *The Bullwinkle Show*. Retrieved August 19, 2021, from IMDB: <https://www.imdb.com/title/tt0052507/>
- Johnson, D., & Antonelli, W. (2020, October 16). *Emulators can turn your PC into a Mac, let you play games from any era, and more — here's what you should know about the potential benefits and risks of using one*. Retrieved August 18, 2021, from INSIDER: <https://www.businessinsider.com/what-is-an-emulator>
- Kabay, M. E. (2020, November 20). *Term-Project Guidelines*. Retrieved August 19, 2021, from M. E. Kabay: http://www.mekabay.com/courses/academic/norwich/term-paper_guidelines.pdf
- Kabay, M. E. (2021, August 24). *Ethics: Papers Discussing Ethical Principles Applied to the Use of Computers and Communications Technology*. Retrieved August 24, 2021, from M. E. Kabay: <http://www.mekabay.com/ethics/index.htm>
- Kabay, M. E., Holden, D., & Walsh, M. (2014). Operations Security and Production Controls. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed., Vol. 1, p. 2240). Hoboken, NJ, USA: Wiley & Sons. Retrieved August 17, 2021, from <https://smile.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Leichter, J. (1999, January 3). *Now You See It, Now You Don't*. Retrieved August 19, 2021, from RISKS FORUM DIGEST: <https://catless.ncl.ac.uk/Risks/20/14#subj8>
- Microsoft. (1999, May 4). *Computer Hangs After 49.7 Days*. Retrieved August 31, 2021, from Microsoft Personal Support Center: <https://web.archive.org/web/19990508050925/http://support.microsoft.com/support/kb/articles/q216/6/41.asp>
- Microsoft. (2015, October). *A History of Windows*. Retrieved August 31, 2021, from Microsoft Windows: <https://web.archive.org/web/20160618205109/http://windows.microsoft.com/en-US/windows/history#T1=era4>
- Microsoft. (2021). *How to Query the Microsoft Knowledge Base by Using Keywords and Query Words*. Retrieved August 31, 2021, from Microsoft | Support: <https://support.microsoft.com/en-us/topic/how-to-query-the-microsoft-knowledge-base-by-using-keywords-and-query-words-1f39ec6a-edc7-e3dd-d265-77270160bfc6>
- Miller, W. M. (1959). *A Canticle for Leibowitz* (1984 reprint ed.). J. B. Lippincott & Co. Retrieved August 18, 2021, from <https://www.amazon.com/Canticle-Leibowitz-Walter-Miller-Jr/dp/0553273817>

- Mohr, C. N. (2017, February 8). *The Wayback Machine Shows History of the Internet*. Retrieved August 19, 2021, from VOA | Learning English: <https://learningenglish.voanews.com/a/wayback-machine/3710648.html>
- Monty Python. (1970, September 15). *I Had Transgressed the Unwritten Law*. Retrieved August 30, 2021, from Monty Python Ethel the Frog: <https://www.youtube.com/watch?v=GHIQzFuLAcU>
- Monty Python. (2007, April 10). *Bruce's Sketch*. Retrieved August 30, 2021, from Montry Python Channel: <https://www.youtube.com/watch?v=8gw1Ur62x0Q>
- Monty Python. (2009, January 14). *The Knights Who Say "Ni!"*. Retrieved August 30, 2021, from Monty Python Channel: <https://www.youtube.com/watch?v=zIV4poUZAQo>
- Monty Python. (2020, June 30). *The Architect Sketch*. Retrieved August 30, 2021, from Monty Python's Flying Circus: <https://www.youtube.com/watch?v=QfArEGCm7yM>
- Monty Python. (2021, July 14). *Monty Python Home*. Retrieved August 30, 2021, from Monty Python's Official Website: <http://www.montypython.com/>
- Morgan, C. (2018, August 28). *Data Storage Lifespans: How Long Will Media Really Last?* Retrieved August 18, 2021, from StorageCraft: <https://blog.storagecraft.com/data-storage-lifespan/>
- Muchmore, M., & Moore, B. (2021, March 31). *The Best Online Backup Services for 2021*. Retrieved August 23, 2021, from PC Matazine: <https://www.pcmag.com/picks/the-best-online-backup-services>
- NCH Software. *File Converter Software*. Retrieved August 18, 2021, from NCH Software | Converting Software: <https://www.nchsoftware.com/software/converters.html>
- Palin, S. (2011, June 5). Sarah Palin: Paul Revere Did Warn The British That The British Were Coming! (C. Wallace, Interviewer) FAUX NEWS. Retrieved August 19, 2021, from <https://www.youtube.com/watch?v=CLQTcZwbykw>
- Parker, D. B. (1998, September 10). *Fighting Computer Crime: A New Framework for Protecting Information*. Hoboken, NJ, USA: Wiley & Sons. Retrieved August 23, 2021, from AMAZON: <https://smile.amazon.com/Computer-Crime-Donn-B-Parker/dp/0471163783/>
- Pearlstein, S., & Vise, D. A. (2000, April 21). *In Hacker Mystery, A Plot Twist*. Retrieved August 24, 2021, from Washington Post: <https://www.washingtonpost.com/archive/politics/2000/04/21/in-hacker-mystery-a-plot-twist/111e4a2a-0863-40f3-b6c2-746020f3effb/>
- Perlmutter, C. (2019, July 19). *Shred Nations Paper Shredding Service Reviews*. Retrieved August 19, 2021, from ShredNations: <https://www.shrednations.com/2014/04/paper-shredding-service-reviews/?cn-reloaded=1>
- Reference*. (2020, April 10). *What Is Computer Output Microfilm?* Retrieved August 18, 2021, from reference*: <https://www.reference.com/world-view/computer-output-microfilm-a03d69b68b295bd0>
- Rocky and Bullwinkle Fandom. *WABAC Machine*. Retrieved August 19, 2021, from Rocky & Bullwinkle WIKI: https://rockyandbullwinkle.fandom.com/wiki/WABAC_machine
- Rosencrance, L. (2001, Seo 13). *Teen hacker 'Mafiaboy' sentenced*. Retrieved August 24, 2021, from ComputerWorld: <https://www.computerworld.com/article/2583318/teen-hacker-mafiaboy-sentenced.html>
- Rubens, P. (2018, June 26). *How to Stop DDoS Attacks: 6 Tips for Fighting DDoS Attacks*. Retrieved August 24, 2021, from eSecurity Planet: <https://www.esecurityplanet.com/networks/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/>
- Saltzer, J. H. (1964, November 6). *TYPSET and RUNOFF, Memorandum Editor and Type-out Commands*. Retrieved August 18, 2021, from MIT Project MAC: <http://web.mit.edu/Saltzer/www/publications/CC-244.html>
- Schultz, G. (2003, April 2). *Top Five Reasons to Leave Windows 9x Behind*. Retrieved August 31, 2021, from TechRepublic: <https://www.techrepublic.com/article/top-five-reasons-to-leave-windows-9x-behind/>
- Segal, T. (2021, June 1). *Enron Scandal: The Fall of a Wall Street Darling*. Retrieved August 19, 2021, from Investopedia | Laws & Regulations | Crime & Fraud: <https://www.investopedia.com/updates/enron-scandal-summary/>
- Software Testing Help. (2021, August 26). *17 Best Bug Tracking Tools: Defect Tracking Tools of 2021*. Retrieved August 31, 2021, from Software Testing Help: <https://www.softwaretestinghelp.com/popular-bug-tracking-software/>
- U.S. Federal Bureau of Investigation. (2016, December 13). *Enron*. Retrieved August 19, 2021, from FBI | History | Famous Cases & Criminals: <https://www.fbi.gov/history/famous-cases/enron>
- Yahoo! Groups. (2006, December 31). *YAHOO! GROUPS*. Retrieved August 30, 2021, from YAHOO! GROUPS: <https://web.archive.org/web/20061231210455/http://groups.yahoo.com/>
- Yahoo! Groups. (2007, February 25). *GroupManagers Forum*. Retrieved August 30, 2021, from YAHOO! GROUPS: <https://web.archive.org/web/20070225210949/http://tech.groups.yahoo.com/group/GroupManagersForum/>

7 Utility

Utility refers to *usefulness* of data. For example, if a U.S. bank were accidentally to convert U.S. customers' balances to Euros, that error would be a violation of utility. Placing 103 icons on the main screen of a computer in no particular order (yes, I've seen that in reality) is not as *useful* as organizing the information in well-named folders. Storing bibliographic details on a set of paper cards is not as *useful* as storing the information in a *MS-Word* bibliography file (source.xml).¹ Using paper cards to store notes on research is not as *useful* as using *Computer-Aided Thematic Analysis*.²

Topics in this chapter include the following:

- One of the irritating results of ignoring utility is having to help untutored users find files they have stored randomly on their computers. Instead of using hierarchical folders, they plop their files on their main screen in random order and then complain about having to search the hundreds of tiny icons looking for a particular file. This chapter includes specific guidelines on how to name and store files efficiently.
- Another problem that users face is having to hunt for programs. A section of this chapter discusses how to organize program access.
- When users have more than one computer, the devices can fall out of synchronization; there are straightforward methods for ensuring that whatever is stored on one unit can automatically be replicated on another.
- Finally, backups are essential for recovery from problems but also for forensic work or for compliance with legal requirements.



FIGURE 7.1 Utility.

ORGANIZING AND SAFEGUARDING INFORMATION ON DISK

I have occasionally been asked by students and colleagues how I manage information that I use in writing articles and books. One question from a reader was,

I am ... curious how you manage data you come across. I sense that when you are writing a paper or book and need to tap into some past work you or someone else has done, you have organized your hard drive in such a way that... you don't have to hunt to long to find it (maybe you use a DB of some sort rather than a directory structure).



FIGURE 7.2
Data on disk.

This section summarizes how I handle information on disk. I don't claim that my methods are ideal or based on any particular theory; I just don't like clutter, and I like to be able to find stuff when I need it. I also dislike having to redo my work, so I also summarize how I have chosen to back up my data.

The figures in this chapter include screenshots of my main system in 2023, which uses Windows 11. However, the guidelines can apply to any operating system with suitable adaptation. My main point is that you can benefit by figuring out a system that suits *your* needs – not that my system should be adopted by everyone.

DISKS AND PARTITIONS

First of all, it's useful to have multiple disk drives or to partition disk drives into virtual drives with different functions. For example, on my system, the drives are as shown in [Figure 7.3](#).

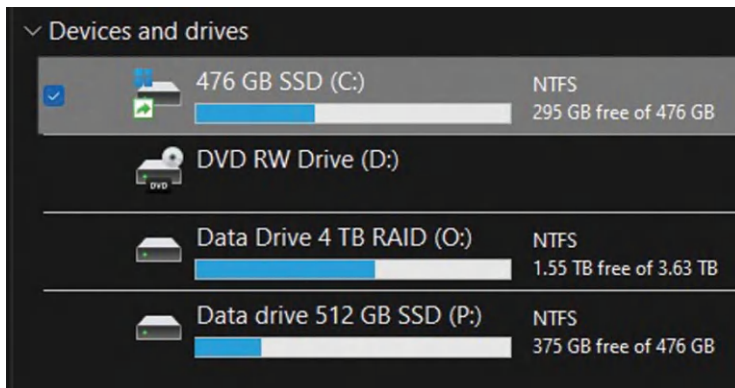


FIGURE 7.3 Storage units on MAIN.

Keeping as much user data off the OS disk makes it easier to handle backup/restore operations. For example, the P: drive shown in [Figure 7.4](#) is the most actively used data drive; it's where I put the most frequently used folders and files and can be synchronized in a single operation between the main system and an external disk drive or a backup computer.

The folders on the P: drive have the following contents:

- *bu*: Backup-utility files for different backup tools
- *consulting_current*: Various current projects
- *db*: Documentation such as personal information, outlook email archives, and databases of various problems that have been solved
- *djml_available*: Several thousand unused jokes for my *Daily Joke Mailing List* that goes out to a few dozen friends
- *Dropbox_BU*: Daily backups of the Dropbox files that I share with my wife
- *fin_&_legal*: All the accounting and legal records for our accountant to use in filing taxes
- *installation*: Licenses and installation files for every purchased (or free) program on my systems
- *mk*: Personal records such as my CV, correspondence, poems, and so on
- *publishing_current*: Articles and books I'm working on (e.g., this textbook was in that folder until I finished it)
- *teaching_current*: Courses currently being used
- *webmk*: All the files needed for my personal website (mekabay.com)
- *XFR*: Working files such as temporary downloads, frequently used icons (e.g., <facepalm.jpg> and <oy-gevalt.jpg>) and convenient links to other frequently used folders

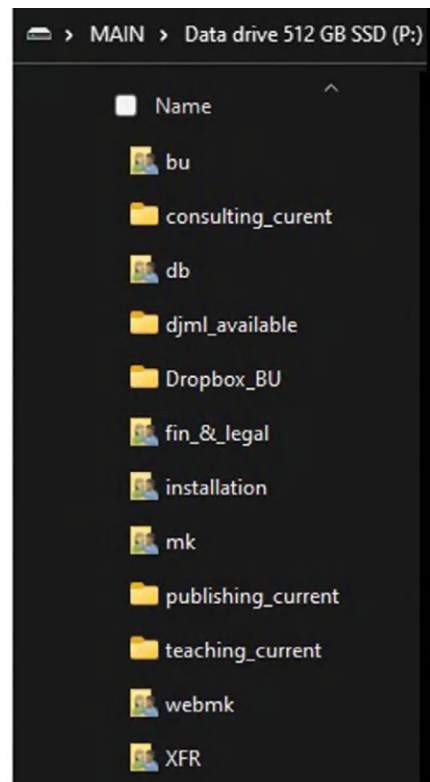


FIGURE 7.4 P drive contents.

Keeping frequently used data on a physical drive separate from the C: (system) drive reduces contention for the disk controllers; especially if a low-memory system has to use lots of virtual-memory swapping on the system drive, there is a performance gain in having separate read/write heads for the OS and user data.

The C: and P: drives are both *solid-state drives* (SSDs) with fast I/O rates. They are never defragmented because defragging is not recommended for such drives (there's a limit to how many times an SSD can write into any given location on disk).³

The O: drive, a two-disk RAID configured for mirroring (RAID 1)⁴ is for more static and less critical data that are convenient to keep around. Figure 7.5 shows how it's where I put daily and monthly backups as well as archival material.

An important option is *not* to check *Hide file extensions for known file types*. People who don't see the real file extensions can sometimes be fooled by malicious software files that misrepresent their actual file types; for example, a Trojan horse file might be called something like *useful.txt.exe* and have a text-file icon associated with it. With suppression of file extensions enabled, the victim would see *useful.txt* with a text icon and might not realize that *that* particular file should have a type-suffix visible when none of the other ones do. Opening the false text file would then run the harmful program.

USEFUL MATERIALS SHOULD BE ORGANIZED

I keep non-confidential, useful information in my *Reference* folder, shown in Figure 7.6.

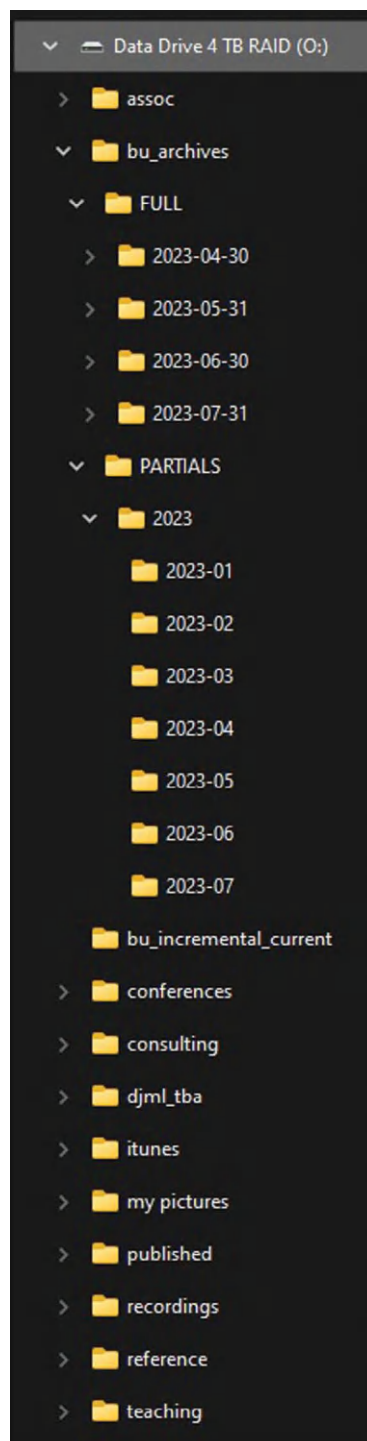


FIGURE 7.5 O: drive.

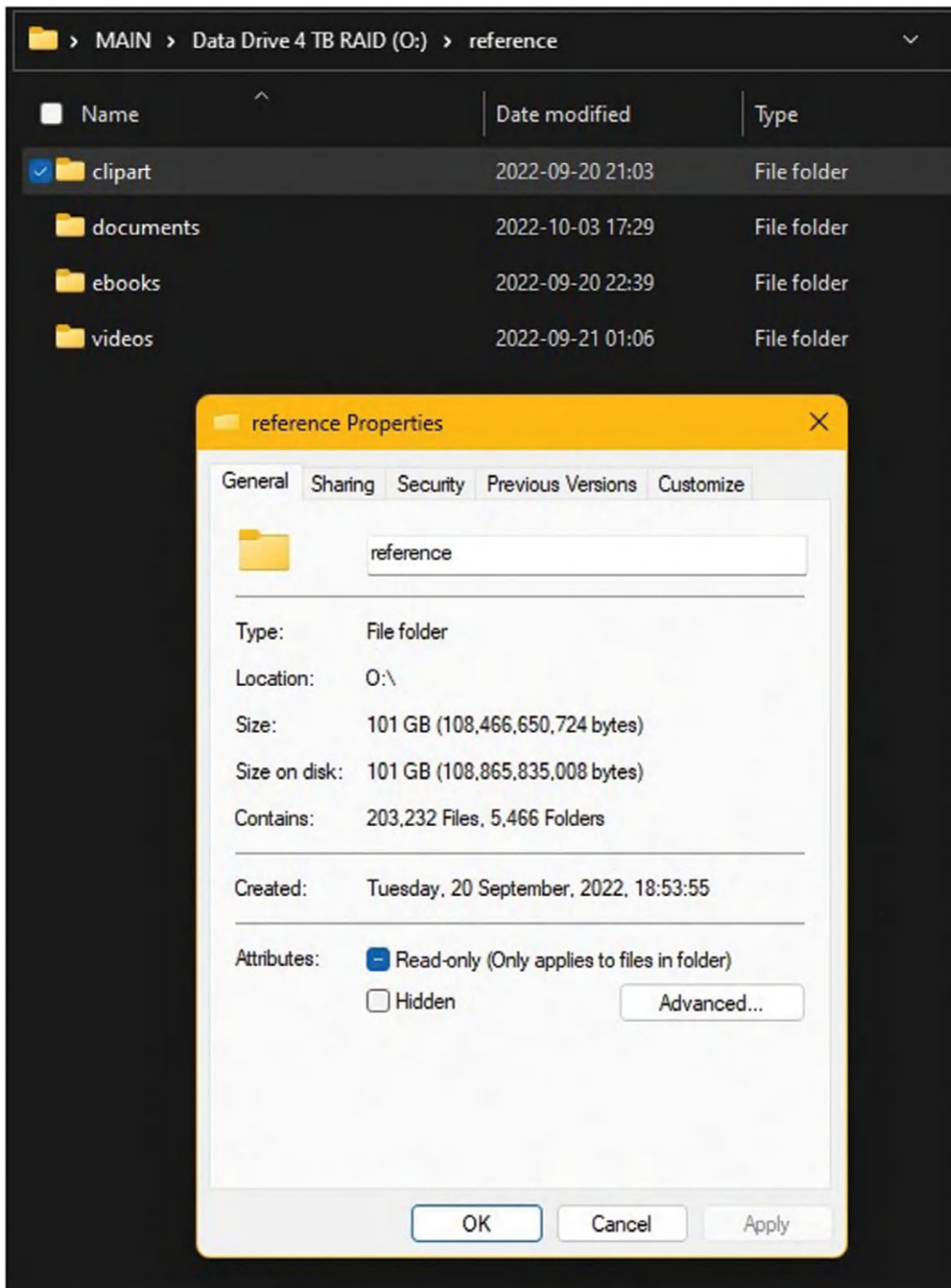


FIGURE 7.6 Reference folder.

The *clipart* folder contains about 132,000 licensed images that I bought years ago in the 10-CD *Serif MonsterCD* collection from the *SerifPagePlus* product of 1996.⁵ I did have to convert them years later from the outdated *.wmf* format to *.jpg* format using *Doxillion Plus* from *NCH Software*.⁶

Because the Web is not a stable place, one can't always count on finding neat stuff one has seen after a year has gone by. The *documents* folder is where I keep examples, case studies, and interesting materials potentially useful for thinking, writing, and lecturing.

The *ebooks* folder contains conference proceedings and electronic versions of textbooks. The *videos* folder has training materials collected over the last several decades.

FINDING FILES

If you are working on many projects at the same time, you may need multiple folders to keep your materials organized. Sometimes locating specific information can become a daunting task. For example, at the time of writing, I had 3.06 TB of data in 319,747 files and 27,740 folders on my O: drive and 101 GB of data in 31,759 files and 3,262 folders on my P: drive.

The most obvious way to find files is to have good file names. For example, my folder about our tractor has obvious names that include dates for convenience (so that the date modified doesn't control the sort sequence).

A quick note here about version numbers:

I strongly recommend that you get into the habit of saving changes to important files (e.g., the manuscript of this textbook as shown in Figure 7.8) using version numbers. That way, if you accidentally damage information in a critical file, you may be able to find it in a previous version that you have backed up. If you always back up to the same file name, it's harder to locate the undamaged information because you need to search backups.

The next feature is one that too few people use or are even aware of: The *advanced-document-properties sheet* for MS Office documents shown in Figure 7.8.



FIGURE 7.7 Searching.

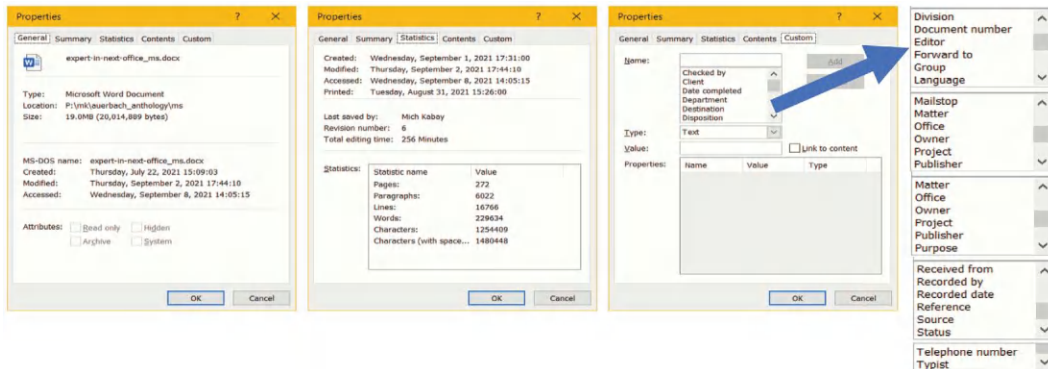


FIGURE 7.8 Advanced document properties.

The properties sheet is potentially useful, but, it can sometimes reveal more information that you intended if you forget that it's there. Many people in business have forgotten that the properties sheet may contain confidential information such as names of reviewers, specific keywords referring to internal project names, telephone numbers, and even comments they would have preferred to keep within the bounds of their organization. Check your properties sheet before sending any document to a stranger or to someone outside your workgroup or organization to be sure you approve of the information it is releasing to the world.

SEARCHING CONTENT

Windows can search on filenames and text in files provided you allow it to do so.⁷ Specialized search tools are available for Windows and for other operating systems that can locate files more quickly than the integrated search functions.⁸

TEMPLATES

Another way of storing work is to save *templates*. For example, choosing to create a new document in MS-Word brings up a page showing standard formats, as shown in [Figure 7.9](#). Users can define their own templates easily by saving them with file-type `<.dotx>`.

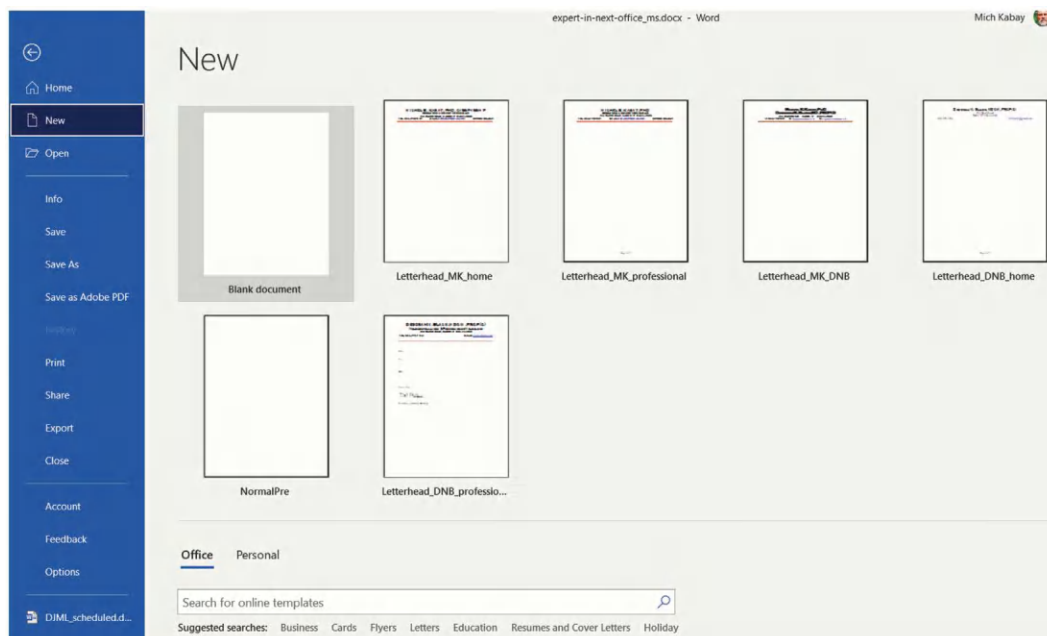


FIGURE 7.9 Word templates.

Templates for presentations using PowerPoint are particularly useful for maintaining consistent formats in multiple lectures. You don't have to set up the headings and footings and font preferences and so on; templates ensure consistency, which is helpful for students because they can get used to the meanings you attach to specific font sizes and enhancements.

Similarly, in documents for publication such as regular columns in magazines, I find it helpful to have all the boilerplate in place, so I don't have to worry about it. That can include copyright information, standard identification, permissions, and so on.

If you find that your list of templates includes rarely used files that you do not want cluttering up the display when you create a new file, you can simply store the files with a descriptive name in a different folder for future use. Remember to *SAVE AS* the new file immediately after opening the informal template so you don't accidentally overwrite your original file. [Figure 7.10](#) shows categories of such files on my system. Again, the point is NOT to tell you how to organize your materials but simply to suggest that you do so as best suits *your* needs and preferences.

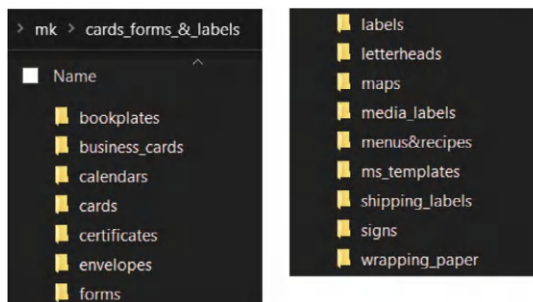


FIGURE 7.10 Useful files.

THE DESKTOP

I've seen colleagues who have dozens or even hundreds of icons on their screen in a helter-skelter arrangement; I have no idea why that would be acceptable. I have personally seen them struggling to locate the symbols for what they need to run or to see.

Figure 7.11 shows a screen shot of my three computer screens.



FIGURE 7.11 Screen layout.

As you can see, everything I use often is on the toolbars and the screen icons. I organize my icons in a logical way, but I think everybody has their own way of organizing their tools, so I don't think it's worth going into the details. As long as you know where things are, you can find them quickly. Personally, I generally put the icons in alphabetical order, but one gets used to any familiar pattern. The image shows the toolbar at the bottom of the middle screen, but I have the toolbar on all three screens; they normally hide unless I point to the bottom of the screen with the cursor.

On a personal note that has nothing to do with efficiency, the images on the screen are randomly chosen from a collection of several thousand images I like that I have gathered over years and that change every hour (completely controllable using the **< Personalization > Background >** settings).

Individual programs also have toolbars, and I've adjusted those to suit my work habits too. For example, Figure 7.13 shows how in *MS-Word*, my toolbars are customized in a way that makes sense to me – again, the point is not to suggest that you use that arrangement but rather that you customize to suit your habits. Apply the same principle in other frequently used programs to save time and reduce errors.

While we're on the topic of *MS-Word*, if you are writing, say, a textbook with over 700 footnotes to unique references, do keep backups of the *source.xml* files that contain the enormous amount of work you have put into your bibliography. Figure shows where the bibliography file is kept on my system.

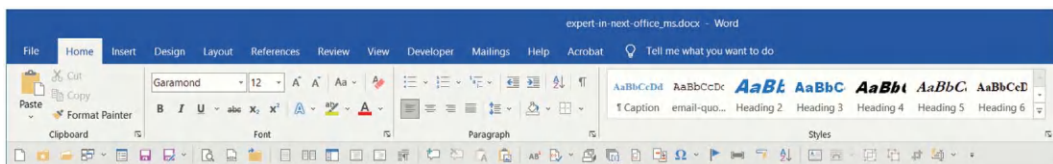


FIGURE 7.12 Personalized toolbar.

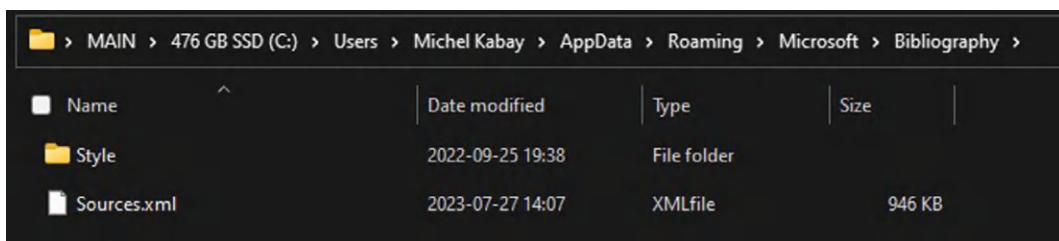


FIGURE 7.13 Bibliography file.

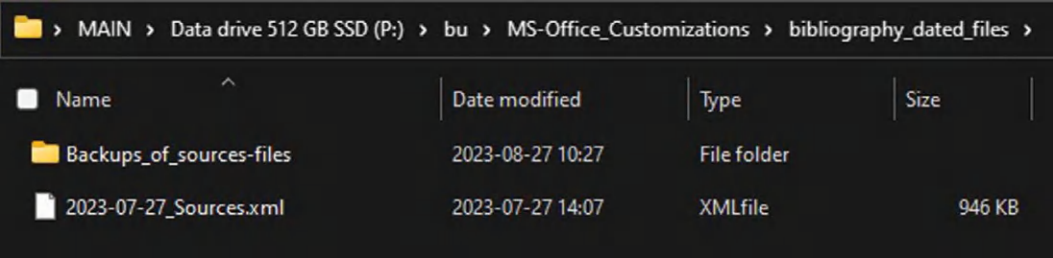


FIGURE 7.14 Backups for the source file.

Figure 7.14 shows where I stored backups of the manuscript of this textbook. The <Backups_of_source-files> folder contained all the dated backups in case I made a mistake and needed to use a previous version of the sources.

SYSTEM SYNCHRONIZATION

How does one manage to have the same information two or more systems? For many years, every evening when I returned from my university office, where I used my university-assigned portable computer to my home office, where I used a more powerful tower computer, I would immediately ensure that both systems had the same data using *Laplink*, as shown in Figure 7.15. For decades, I have used *LapLink*,⁹ but there are many options available for synchronization.

After the data cloning, the two computers had exactly the same data files, effectively providing a real-time backup.

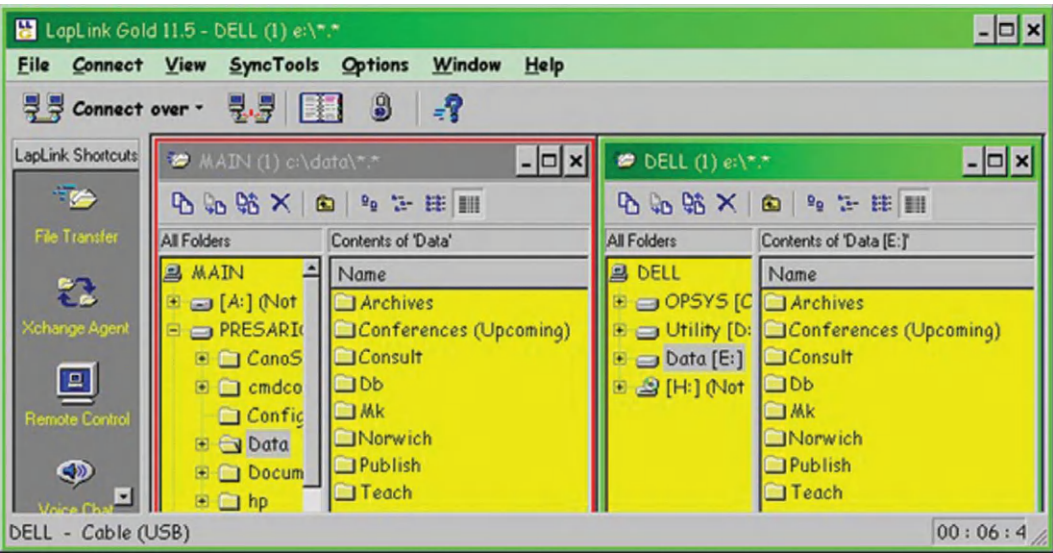


FIGURE 7.15 Laplink interface for synchronizing systems.

The other approach to live backups is to use *cloud-based software*, which stores copies, including older copies, on servers accessible via the Internet.¹¹ The advantage of such systems is that the backups are off-site and thus protected from local physical damage. The disadvantage is that the data are unavailable if the network connection fails. Cloud-based backups are particularly useful in the fight against ransomware as long as the time-stamped cloud-backup files don't get overwritten.¹²

SYSTEM BACKUPS

What if your computer fails completely? You may have to bring the system in to a repair shop to determine the cause. If the system disk has failed, the technicians will install a new disk – but where will the software and data come from? If you have dozens of programs installed, rebuilding your software configuration can take days of work. It makes sense to invest in a product that provides *disk cloning*¹³ or cross-computer software installation¹⁴ that allows you to create installation disks (*image backups*) that will duplicate your software configuration on a replacement computer in minutes. Taking this kind of backup should be a normal precaution for business travelers before setting out on a trip. Personally, I take full-system image backups every month in case my main system goes bad, and I need to update my spare system (with compatible hardware and software) with the current software configurations. Up-to-date daily backups on separate external disks provide the rest of the data transfer.

The daily data backups are kept on one of my system drives but also on five separate external hard drives (Figure 7.16) that I alternate day by day; for example, #1 can hold the backups on, say, Monday, #2 has the backups on Tuesday and #3 has the backup for Wednesday (and so on day by day).

Those backup drives must *not* be left connected to the system after backups complete. Having isolated backup drives ensures protection against ransomware that encrypts hard drives and system failures that can accidentally damage data.

I also update a secondary, older computer system that I call “SPARE” for rapid response should “MAIN” fail. The updates can be accomplished using synchronization software that duplicates the contents of the backup drives on the SPARE drives.



FIGURE 7.16 External backup drives.

BACKUPS AS AN ANTI-FRAUD TOOL

Over several decades in academia, any professor is likely to encounter at least a few cases of plagiarism from foolish students. One of the most pernicious types of plagiarism involves theft of papers from a roommate’s computer. The story usually goes something like this real case from 2011 where I worked as a professor:

- Incompetent, disorganized student fails to prepare an essay that account for a significant part of his or her grade in a course that is required for completion of their degree.
- Desperate, the dilatory student realizes that his or her roommate, who is taking the same course, has already completed the assignment.
- Dishonest student takes advantage of roommate’s absence to break into the poorly secured system – either simply by using the computer when it has not been locked or by learning or receiving the roommate’s password.
- Plagiarizing student copies the draft or final version of the term paper, puts own name on it and submits it in place of the missing essay.
- Honest student, not having any idea of the theft, also hands in own paper shortly thereafter – and gets accused of plagiarism.

In class after class, I try to drum into my students that one of the best classes of evidence of their authorship of any work is a trail of backups with a *version number* for each file.

Here is a simple process for establishing a trail of evidence of ownership:

- Each time they open the current version of the document for the first time on a particular day, they should immediately save a new version of the document within incremented version number. For example, if yesterday's file is called < is342_term-paper_1_v06.docx > then today's file is immediately saved as < is342_term-paper_1_v07.docx >.
- At the end or beginning of every day, a student should make an *encrypted* differential backup that includes all files changed during the last 24 hours.
- A copy of the backup should be stored on a separate, removable device such as a portable hard disk or a flash drive – and that backup should be kept securely away from the computer itself. Typically, students can simply carry these small devices in their pockets, briefcases, purses, or knapsacks.

If a thief takes control of the term paper and claims ownership, the victim immediately has an electronic trail that effectively proves that they, and not the thief, worked on the paper. Even if the thief steals the backups from the hard drive, their encryption should prevent exploitation. Having the document trail at hand makes it impossible for the thief to successfully claim ownership of the term paper.

In the case described above, the honest student did indeed have a series of dated backups; the thief had nothing but the last copy. The thief was expelled from the university.

Finally, students living in dormitories and sharing a dorm room with others should use the following simple precautions:

- Use whole-disk encryption on your personal computer.
- Lock your computer when you leave your room – no matter how soon you think you will return.
- Be sure that your password cannot easily be guessed: Don't use anything that is related to family, hobbies, courses; best is to generate an easily remembered password that isn't a real word.
- Don't use the same password for your encrypted backups that you do for login to your computer or for access to your academic network. Every password should be different.
- Set a timeout on your computer so that it locks automatically after a reasonable period of inactivity. You will have to decide what's reasonable as a function of your normal use patterns. For example, if you rarely go more than, say, 20 minutes without activity on your system while you are working, then use 20 minutes as your timeout. Adjust the timeout so that it does not irritate you – otherwise you'll end up deactivating it.

These principles also apply to professionals' systems. Proper security can protect against fraudulent accusations by criminals who access colleague's systems to insert incriminating data or to steal information for misrepresentation of the origins.

Figure 7.17 shows some of the backups for the manuscript of this textbook.

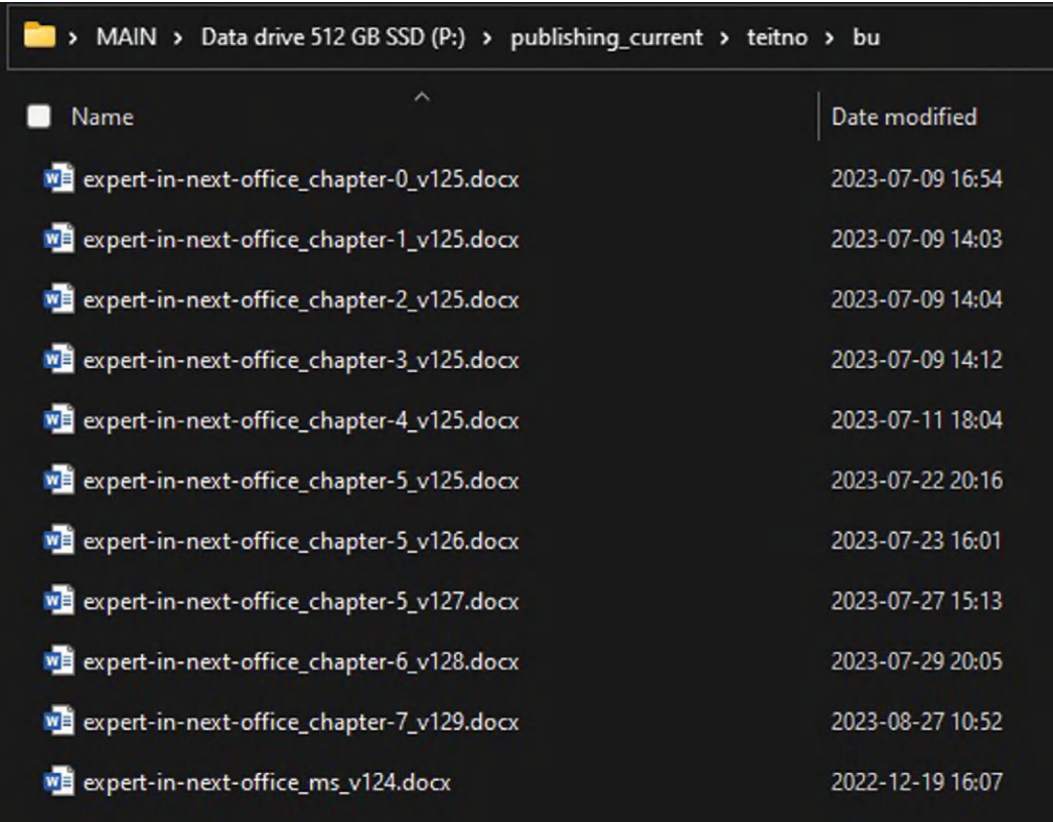


FIGURE 7.17 Backups of textbook MS.

NOTES

- 1 Microsoft (2019).
- 2 Kabay, CATA: Computer-Aided Thematic Analysis (2006).
- 3 Micron (2020).
- 4 Freedman (2021).
- 5 Serif (1996).
- 6 NCH Software (n/a).
- 7 Garrison (2017).
- 8 G2 (n/a).
- 9 Laplink (2021).
- 10 Capterra (2021).
- 11 Wagenseil (2021).
- 12 Burt (2018).
- 13 DeMuro and Turner (2021).
- 14 Sinclair (2021).

WORKS CITED

Burt, J. (2018, December 20). *Cloud Backup: How It Can Protect Against Ransomware*. Retrieved July 7, 2021, from DARKReading: <https://www.darkreading.com/cloud-security/cloud-backup-how-it-can-protect-against-ransomware/a/d-id/747921>

Capterra. (2021). *File Sync Software*. Retrieved September 10, 2021, from Capterra: <https://www.capterra.com/file-sync-software/>

- DeMuro, J. P., & Turner, B. (2021, July 12). *Best Disk Cloning Software of 2021*. Retrieved July 25, 2021, from techradar.pro: <https://www.techradar.com/best/best-disk-cloning-software>
- Freedman, A. (2021, July 1). *Definition: RAID 1*. Retrieved September 1, 2021, from Computer Language! Computer Desktop Encyclopedia: <https://www.computerlanguage.com/results.php?definition=RAID+1>
- G2. (n/a, n/a n/a). *Best Desktop Search Software*. Retrieved September 8, 2021, from G2 Product Reviews: <https://www.g2.com/categories/desktop-search>
- Garrison, J. (2017, August 14). *How to Search for Text Inside of Any File Using Windows Search*. Retrieved September 8, 2021, from How-To Geek: <https://www.howtogeek.com/99406/how-to-search-for-text-inside-of-any-file-using-windows-search/>
- Kabay, M. E. (2006, October 5). *CATA: Computer-Aided Thematic Analysis*. Retrieved Aug 31, 2021, from M. E. Kabay: <http://www.mekabay.com/methodology/CATA.pdf>
- Laplink. (2021). *Laplink SYnc*. Retrieved September 10, 2021, from Laplink: <https://web.laplink.com/product/laplink-sync/>
- Micron. (2020). *Should I defrag my SSD?* Retrieved September 1, 2021, from Micron | Crucial: <https://www.crucial.com/articles/about-ssd/should-you-defrag-an-ssd>
- Microsoft. (2019, June 8). *Working With Bibliographies*. Retrieved August 31, 2021, from Microsoft | Docs | Documentation: <https://docs.microsoft.com/en-us/office/vba/word/concepts/working-with-word/working-with-bibliographies>
- NCH Software. *File Converter Software*. Retrieved August 18, 2021, from NCH Software | Converting Software <https://www.nchsoftware.com/software/converters.html>
- Serif. (1996, October 1). *Welcome to Serif!* Retrieved September 2, 2021, from Serif: <https://web.archive.org/web/19961114210159/http://www.serif.com/>
- Sinclair, C. (2021, March 6). *6 Best Alternatives to PCMover [2021]*. Retrieved July 25, 2021, from the digital guide: <https://digitalguyde.com/the-best-alternatives-to-pcmover/>
- Wagenseil, P. (2021, August 16). *The best cloud backup services in 2021*. Retrieved September 10, 2021, from Tom's Guide: <https://www.tomsguide.com/best-picks/best-cloud-backup>

8 Threats

THREATS TO INFORMATION SECURITY

It is difficult to estimate precisely what causes damage to IS. Managers should be skeptical of any statistics about information security if they show unusually precise numbers.¹ The problem is twofold: People don't recognize crimes or damage, and when they do they usually don't report them anywhere that collects statistics.

Surveys that report on computer crime and other breaches of security are useful, but all of them suffer from the problems of *voluntary response* – the fundamental question of whether people who respond to questionnaires are representative of everyone in the field even though many people refuse to participate in the studies.²

Despite these problems, information-security experts generally agree on some rough guesses about how damage occurs. The basic classification looks at internal dangers, external threats, and attractive targets.

This chapter reviews

- Basic information protection methods
- The role of policy in supporting security
- Discussion of security problems within organizations
- Review of the types of external threats to security
- Factors influencing why criminals target different types of victims

BASIC PROTECTION: SAFE HEX

Many security specialists focus on significant improvement to commercial IS by encouraging basic protection mechanisms. Experts focus on the most important security processes so that clients spend their resources where there will be the greatest return on their investment. This approach is a simple application of optimization theory, from which we know that in any field, there is likely to be a small number of factors that predominate in determining results; some people refer to the *Pareto Principle*, claiming that 80% of everything is the result of 20% of the causal factors.³

The basic problems security specialists see in the field are

- Inadequate security policies,
- Poor training,
- Inadequate security awareness,
- Bad management,
- Improper use of security technology,
- Inadequate maintenance of security and operating system software, and
- Lack of computer-emergency preparedness.



FIGURE 8.1 Threats.

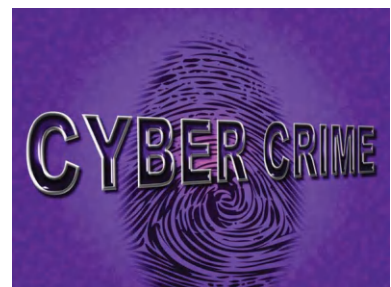


FIGURE 8.2 Protect against cybercrime.

POLICY, POWER, AND POSITION

Many firms have no security policy at all; others have policies that are so old that no one remembers their details (or sometimes even their location).⁴ Policies are an expression of an organization's values; if security is relegated to shelfware, employees will act accordingly. Too often, security is an after-thought; someone is assigned the task of managing security but lacks defined responsibilities, has no authority, and can serve solely as a figurehead.

One of the most innovative measures in the industry is the recognition of information-systems security as a responsibility equivalent to stewardship of financial resources or of operations. The *Chief Information Security Officer* (CISO) should report at the same institutional level as the CFO, and CIO. Making the information-security officer report to the CIO (or lower) is a conflict of interest; one would not want the Chief Auditor to report to the CFO; the same principle of separation of duties should apply to security.

Security policies naturally cover many different aspects of operations. Physical security requires adequate safeguards to prevent intrusion into restricted areas. Effective technology such as ICSA-certified biometric authentication involving fingerprints, irises, retinas, faces, and voice- or signature-pattern recognition can materially improve controls over access – and can equally well be applied to controlling logical access to systems. Smart cards and other tokens – especially cell-phones with SMS and authentication software⁵ are also useful tools for I & A.

However, continuing to rely solely on passwords for high-security applications is unwise. All of our experience in security indicates that people are bad at picking passwords and that too many people don't understand the importance of keeping passwords secret (hence the custom of checking for sticky notes attached to terminals, under keyboards, and so on when auditors evaluate the effectiveness of security awareness training).

Setting the parameters properly on operating systems, firewalls, IDSs, and system logging is essential for security. In my work, I found that many customers used default settings instead of choosing parameters that reflect their security policies. Firewalls help reduce the likelihood of penetration; IDSs reduce the lag between penetration and response. Logging enables forensics destination and possible prosecution. All of these elements are valuable in today's environment.

A critical element of security, especially for portable computers, is encryption. With the easy availability of strong, unobtrusive encryption software today, there is no excuse for having sensitive data stored in the clear – that is to say, without encryption. Laptop and other computer thefts are growing from year to year; frequently, the value of the stolen data exceeds that of the hardware.

An area that is often overlooked in security architectures is email.⁶ Users can often evade restrictions on inbound and outbound communications imposed by firewalls simply by using email. Email should always be the property of the organization, not of individual employees; this policy should be announced every time an employee initializes the email program. This precaution allows investigation of possible malfeasance and ensures that employees do not develop a false expectation of privacy for corporate email.

A similar approach should govern access to the Web. Using corporate resources for Web access must clearly allow monitoring or logging to prevent the too-frequent abuse of time and bandwidth.⁷ In addition, access to pornographic or hateful materials on the Web makes an employer liable for accusations of tolerating a hostile work environment for other employees.⁸ Corporate policy should also preclude multi-user games that can bring a network to its knees during peak network periods.⁹ A reasonable compromise is to allow such games after business hours.

For organizations creating their own software, software quality assurance is an important element in security. Not only should we avoid bugs that cause errors and down time; in addition,



FIGURE 8.3 Policies.

we should avoid, detect, and remove deliberately implanted malicious code. Programmers have been known to insert logic bombs which will work to divert resources; effective testing and documentation – especially test coverage monitors that ensure parts of executable code are tested during quality assurance work – can discourage malefactors and catch harmful instructions before they are executed in production.

Similarly, it is important to fight external malicious code:

- Every workstation and server should be running up-to-date antimalware software¹⁰ and allowing it to run constantly in background.
- Every copy of *MS-Word* and *MS-Excel* should disable auto-execution of macros.¹¹
- Users should know that unsolicited or unexpected DOCX or XLSX files, executables or WinZIP compressed files sent as attachments to email should be checked with the supposed senders to be sure they are not from criminals.
- Legitimate attachments must be scanned by antimalware before being opened or run.
- To prevent automatic execution of Trojans that look like some other type of file, users should ensure that all file types are visible, not hidden.

As ever, organizations must take adequate backups, safeguard them during storage, and destroy data before discarding backup media. Even non-backup electronic media warrant attention. Removable disks and flashdrives are notorious for containing erased information that is perfectly readable using simple tools.¹² Even formatting a disk may not suffice to obliterate all traces of previous data until the deleted data areas are overwritten¹³; however, military-grade erasure programs can write multiple passes of randomized data over the entire surface of a disk or in clusters of specific erased files.¹⁴

INTERNAL DANGERS

Perhaps half or more of all the damage caused to IS comes from authorized personnel who are either untrained or incompetent. Another quarter or so of the damage seems to come from physical factors such as fire, water, and bad power. Maybe a fifth of the damage comes from dishonest and disgruntled employees.¹⁵ Computer viruses cause another few percent, and maybe about 5% or 10% of the damage is caused by external attack.¹⁶

The chapters that follow on *Management Principles* and on *Employment Practices & Policies* include extensive discussions of preventing insider crime.



FIGURE 8.4 Insider crime.



FIGURE 8.5 Criminal hackers.

The growth of Internet connectivity is altering these statistics. Many systems were once restricted to internal access, with maybe a slow modem or two for remote access by employees. Today we see production systems (those on which organizations depend day by day for continued operations) nonetheless being opened to access via TCP/IP connections from the wider Internet. Many organizations are also linking their systems tightly with those of trading partners using VPNs that increase the number of people allowed to access the systems. Devices such as refrigerators, cars, and manufacturing

systems are increasingly including Internet connectivity, joining the *Internet of Things* (IoT) and increasing opportunities for exploitation and risks of new vulnerabilities.¹⁷

Who are the people attacking computer systems? There seem to be the two major classes: *amateurs* and *professionals*. Amateurs include poorly supervised children, rebellious and badly socialized adolescents, and psychologically disturbed or ideologically warped adults. Some amateurs cloak their destructive attacks on badly protected computer systems in the language of social responsibility; they claim to have the best interests of their victims of heart. Their actions belie their words; however, well-meaning people do not place obscenities and insults on other people's property as these cybervandals do on many a website.

Hobbyist attacks have recently become a major problem with the widespread availability of tools for DDoS. Using these tools, even children can locate vulnerable sites on the Internet, implant special "zombie" software, and then later activate the zombie programs to send streams of spurious requests to one or more selected victims. Under siege from dozens or even hundreds of zombie programs, many such victims are swamped by the volume of traffic and see their response time for real customers and visitors increasing unacceptably.

Criminal (black-hat) hackers are harder to characterize, since there are probably fewer of them and they may be harder to catch; however, some criminal hackers are earning a living with their skills. Some professionals use public and illegal sources of information to help unscrupulous private investigators. Some computer criminals steal credit card numbers and sell them to the criminal underground or participate in theft of services from telephone and mobile-phone companies. An unknown number may be involved in industrial espionage.¹⁸

The use of *MSOffice* products greatly increased the vulnerability of users because of *Microsoft's* decision to include a powerful scripting language at the heart of its word-processing, spreadsheet, presentation, DB, and email products. Email can therefore carry documents that include the equivalent of programs – macro viruses that can not only harm documents but also call system routines and therefore wreak havoc with the operating system, memory, and files. Other contributors to trouble include scripting languages used on websites (e.g., *ActiveX*, *Java*, *Javascript*) and even the fundamental formatting language of the Web, HTML.¹⁹ All of these tools have been misused to harm users.

Some criminal hackers have set up shop as security consultants and offer penetration analysis and consulting services for their clients. There is a serious question about the trustworthiness of people who used to break or skirt the law and now claim that they no longer do so; some security experts argue that leopards have indelible spots, whereas others are willing to believe that there is such a thing as an *ex-hacker*. I strongly urge managers considering hiring such people to conduct extensive, in-detail interviews to discuss the candidates' attitudes toward their *previous* (we hope) activities. Ensure that their contracts include severe penalty clauses if any of their employees are found to be breaching client confidentiality, damaging data, or breaking applicable laws in the course of their duties.

ATTRACTIVE TARGETS

Several factors influence the likelihood of attack. For example, a small, obscure tool-and-die company with eight employees is unlikely to be as attractive to any external attacker interested in stealing confidential data or launching a ransomware attack as a major corporation with thousands of employees and a significant share of its market. However, it is possible that having a public website makes any organization an attractive target for cybervandals. For example, even small but poorly secured websites may be useful to criminals as launching pads for phishing attacks.

Statistical analysis of data breach investigations in 2019 revealed that the top six target categories for cyberattacks were:

- Small businesses
- Healthcare institutions



FIGURE 8.6 Targets.

- Government agencies
- Financial institutions
- Educational institutions
- Energy and utility suppliers²⁰

Some hackers attack sites for political purposes; recent attacks on such victims as Indian nuclear power company websites are said to be examples of *hactivism*.²¹

Most attacks on Internet-connected systems today are completely automated. Port scanners are operating 24 hours a day from thousands of sites around the world looking for vulnerabilities. These automated attack tools pay no attention to the nature of the site under attack: they're simply looking for vulnerable computers that can be used as platforms for various types of attack on other computers. Thus, the widespread availability of automated attack tools has made everyone a possible target regardless of how attractive their systems might be to a human criminal.²²

NOTES

- 1 Wolff (2018).
- 2 VOXCO (n/a).
- 3 Tardi (2020).
- 4 Atkins (2014).
- 5 Microsoft (2023).
- 6 Dosal (2019).
- 7 Sevilla (2021).
- 8 The Armstrong Law Firm (n/a).
- 9 Shein, 80% of people have played games while working (2020).
- 10 Rubenking (2021).
- 11 Center for Internet Security (n/a).
- 12 Hoffman, Why Deleted Files Can Be Recovered, and How You Can Prevent It (2018).
- 13 Cole (2021).
- 14 Fisher (2021).
- 15 Zadelhoff (2016).
- 16 ERMProtect Cybersecurity Solutions (n/a).
- 17 Sembera and Urbanec (2021).
- 18 Poppy (2019).
- 19 Anupam and Mayer (1998).
- 20 Western Governors University (2021).
- 21 CyberPolicy (n/a).
- 22 WhatUp Gold Team (2019).

WORKS CITED

- Anupam, V., & Mayer, A. (1998, January 26). *Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies*. Retrieved September 13, 2021, from Proceedings of the 7th USENIX Security Symposium: https://www.usenix.org/publications/library/proceedings/sec98/full_papers/anupam/anupam.pdf
- Atkins, S. (2014, March 6). *Exhibit A: The Perils of Outdated Policies*. Retrieved September 13, 2021, from NAVEX Global | Risk & Compliance Matters: <https://www.navexglobal.com/blog/article/exhibit-perils-outdated-policies/>
- Center for Internet Security. (n/a, n/a n/a). *Intel Insight: How to Disable Macros*. Retrieved September 14, 2021, from CIS | Resources | White Papers: <https://www.cisecurity.org/white-papers/intel-insight-how-to-disable-macros/>
- Cole, A. (2021, April 13). *How to Recover Files from a Formatted Hard Drive*. Retrieved September 14, 2021, from Clever How-To's: <https://www.cleverfiles.com/howto/recover-formatted-hdd.html>
- CyberPolicy. (n/a, n/a n/a). *What Type of Organization Do Hackers Target the Most?* Retrieved September 13, 2021, from CyberPolicy | Cybersecurity Education: <https://www.cyberpolicy.com/cybersecurity-education/what-type-of-organizations-do-hackers-target-the-most>

- Dosal, E. (2019, December 12). *Why You Shouldn't Ignore Email Security*. Retrieved September 13, 2021, from COMPUQUIP Cybersecurity: <https://www.compuquip.com/blog/why-email-security-is-important>
- ERMProtect Cybersecurity Solutions. (n/a, n/a n/a). *External vs. Internal Cybersecurity Risks: Know the Difference*. Retrieved September 13, 2021, from ERMProtect: <https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference/>
- Fisher, T. (2021, September 4). *36 Best Free Data Destruction Software Programs*. Retrieved September 14, 2021, from Lifewire | Software & Apps: <https://www.lifewire.com/free-data-destruction-software-programs-2626174>
- Hoffman, C. (2018, June 8). *Why Deleted Files Can Be Recovered, and How You Can Prevent It*. Retrieved September 14, 2021, from How-To Geek: <https://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/>
- Microsoft. (2023, n/a n/a). *Download Microsoft Authenticator*. Retrieved August 27, 2023, from Microsoft | Security | Mobile-authenticator: <https://www.microsoft.com/en-us/security/mobile-authenticator-app>
- Poppy, J. (2019, January 3). *The Hacker's Economy*. Retrieved September 13, 2021, from BulletProof | Blog: <https://www.bulletproof.co.uk/blog/the-hackers-economy>
- Rubenking, N. J. (2021, May 4). *The Best Malware Removal and Protection Software for 2021*. Retrieved September 14, 2021, from PC Magazine: <https://www.pcmag.com/picks/the-best-malware-removal-and-protection-software>
- Semberra, V., & Urbanec, J. (2021, July 22). *IoT Security Issues, Threats, and Defenses*. Retrieved September 13, 2021, from TREND Micro | Security News | Internet of Things: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses>
- Sevilla, G. (2021, August 26). *The Best Employee Monitoring Software for 2021*. Retrieved September 13, 2021, from PC Magazine | Best Products | Human Resources | Employee Monitoring Software: <https://www.pcmag.com/picks/the-best-employee-monitoring-software>
- Shein, E. (2020, May 29). *80% of People Have Played Games While Working*. Retrieved September 13, 2021, from TechRepublic: <https://www.techrepublic.com/article/80-of-people-have-played-games-while-working/>
- Tardi, C. (2020, May 25). *80-20 Rule*. Retrieved September 13, 2021, from Investopedia: <https://www.investopedia.com/terms/1/80-20-rule.asp>
- The Armstrong Law Firm. (n/a, n/a n/a). *Sexual Harassment: Inappropriate Images on Screen*. Retrieved September 13, 2021, from Armstrong Law Firm | Sexual Harassment at Work: <https://www.thearmstronglawfirm.com/sexual-harassment/inappropriate-images-on-screen/>
- VOXCO. (n/a, n/a n/a). *Voluntary Response Sample: Definition, Examples & Uses*. Retrieved September 13, 2021, from VOXCO: <https://www.voxco.com/blog/voluntary-response-sample/>
- Western Governors University. (2021, n/a n/a). *6 Industries Most Vulnerable to Cyber Attacks*. Retrieved December 8, 2021, from WGU | Information Technology | Blog: <https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html#close>
- WhatUp Gold Team. (2019, April 10). *Port Scanning 101: What It Is, What It Does, Why Hackers Love It, and Why You Will Too*. Retrieved September 13, 2021, from Progress WhatsUpGold: <https://www.whatsupgold.com/blog/port-scanning-101-what-it-is-what-it-does>
- Wolff, J. (2018, February 20). *How unreliable data leads to the undercounting of cybercrime*. Retrieved September 13, 2021, from Pacific Standard Magazine: <https://psmag.com/news/the-problem-with-cybercrime-statistics>
- Zadelhoff, M. v. (2016, September 19). *The Biggest Cybersecurity Threats Are Inside Your Company*. Retrieved September 13, 2021, from Harvard Business Review: <https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company>

9 Management Principles

The basic reasons we care about information-systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity of documents we create, send, and receive. Finally, if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market-development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line.¹

Part of my job as an instructor in IA has been to collect and analyze above-ground intelligence: news items from newswire services, publications such as the *ACM Risks Forum*,² *Crypto-Gram*,³ *Cybersecurity & Information Systems Digest*,⁴ and so on; I have used these resources for public seminars⁵ and academic courses.^{6,7} My impression from all of this reading is that non-specialists believe that criminal hackers are the most important threat to information-systems security. However, everything I know about information security contradicts this belief. This section is an attempt to dispel some of the misinformation about security circulating among non-specialists and to provide practical guidelines to managers for significant improvements in securing information.

This chapter reviews

- Basic principles of effective management
- How to help staff resist social engineering
- System administration practices for strong security
- How to make the best use of consulting services
- Methods for organizing information from meetings and research efforts

SECURITY BY OBJECTIVES

Back in 2002, I was creating curriculum for the management module of *Norwich University's* new *MSIA* program. *Seminar Two* of the six in the 18-month program consisted of 11 weeks of study on foundation skills for IA managers, and *Week Six* in that seminar was about management skills.⁸ In the module, one of the topics I put in was *Management by Objectives* (MBO).

MBO centers on the need and value of defining *measurable objectives* for a group. The theory is that unless we can measure performance and



FIGURE 9.1
Management principles.



FIGURE 9.2 Objectives.

progress, our impressions of compliance with our goals will be too fuzzy and uncertain to motivate staff and to provide value to upper managers for strategic planning.

An important tool for MBO in the operations field is the Service-Level Agreement (SLA). This agreement serves as a contract that defines acceptable service. For example, one can define the maximum acceptable rate of downtime for a network or the maximum acceptable response time for an application program – or for the helpdesk. Knowing the limits is crucial for effective quality control; as staff see spikes or trends approaching the control limits, they can investigate the causes of irregular results or take action to correct appropriate factors before there's a serious problem. Without stated limits, people may wait until there's a disaster. When people rush around without a plan as they react to an emergency, everything is more expensive and more prone to error.

Applying MBO to IA, I'd say that it's not enough to use general terms like "be secure" or "protect information resources." I think that we should be using objectives such as "In the next three months, we will successfully prevent all unauthorized changes to our public Web server." We could use the concepts of SLAs to set a goal of ensuring a minimum available bandwidth for the network even in cases of DoS attacks. Perhaps a good measurable objective might be "Find no more than 10% of all workstations logged on to the network after 8 pm every night." How about, "Identify no more than 0.1% of all passwords by running crack programs on the password file?" Or "Limit porn-surfing on corporate machines to a maximum of 2% of total bandwidth during working hours?" If you do penetration tests, then it should be possible to define reasonable measurable objectives and then test those using the pen-tests.

Thinking in behavioral and measurable terms sharpens our ability to identify trouble spots and weak points in our security measures. Here's a jingle you can set to music like the *Burma Shave* ads⁹ of the early 20th century: "Sharpen up and apply MBO to IA today!"

SECURITY BY WALKING AROUND

When I worked for *HP* in the early 1980s, I was particularly impressed by the corporate norm of *management by walking around* (MBWA).¹⁰ Managers literally walked around the office, stopping off to chat with employees and with other managers. They picked up all sorts of valuable insights by watching what employees were doing – as opposed to what got reported through more formal channels. Managers could discover practical problems faster than by waiting for disaster; they could forestall problems by listening to the people most likely to know what was wrong (or right) with specific clients, tasks, projects, units, departments, or the whole company.

I remember the time when Steve, the systems engineering manager for all of *HP Canada*, came to the Montreal office to ask us "systems engineers" (SEs) (an incorrect and now-abandoned term for technical-support specialists, most of whom were *not* professional engineers) what we thought of a new programming tool we had been studying before its release. Steve sat on a desk with a bunch of us lounging on the floor, on chairs, and on other desks in the big open work area of the Montreal office. We told him flatly that the product was terrible; the syntax was inconsistent and illogical, the number of bugs was unacceptable, and we would have a disaster in customer confidence if we released it in that state. I think it speaks to the power of the *HP Way*,¹¹ the guiding principles of HP management, that Steve listened carefully and brought our comments back to headquarters for action. The remarkable thing is that we all felt absolutely confident that our gripes would be taken in the right spirit. Indeed, the release was delayed until the errors were corrected.

When we are working on security – such a complex mixture of technology and human psychology – I think that MBWA is a perfect approach to learning what's really happening in our organization. Instead of making management decisions based on what management would *like* to be true (*Management by Wishful Thinking*),¹² managers confront reality.



FIGURE 9.3 Managers walking around.

Walk around and listen carefully to uncensored comments from the people who are simultaneously trying to get their work done and to maintain information security. Then take action to fix the problems you find.

As a bonus, you get to tone up your legs, improve your blood pressure and use up the calories from that muffin you just ate.

POSITIVE REINFORCEMENT

Keeping employees committed to IA is tough. The fundamental problem is that the better our security, the less evidence we have to reinforce it. As weeks and months go by with no security incidents, employees unconsciously reduce compliance with security rules. This natural process is called *behavioral extinction* and is well known to behavioral psychologists.¹³ To overcome extinguishment in IA, we need *reinforcement*, and that's where security-awareness programs can use imagination and fun.

In an information-security class in 1993, a student told me about an interesting experiment she had carried out at a large company. Employees were not following company policy about logging off the mainframe systems, and the open sessions were interfering with operations by holding DBs open and preventing proper backups. In some cases, operators were able to terminate the sessions remotely, but in others they couldn't. Haranguing people didn't work. You could force employees to contact technical services for a new password, require them to discuss their errors with their managers, and otherwise try to punish them but the compliance rate hovered consistently around 40%.

My student did an experiment. She went around the night and found all the terminals in a specific department that were logged off properly. On the keyboards, she left a little chocolate wrapped in silver foil. There was no explanation for the chocolate. At the end of the month she found that compliance with logoff policy had climbed to around 80% in that department but remained at 40% everywhere else.

Praise and reward can be more powerful than punishment in changing behavior. Talk to any animal trainer for confirmation.¹⁴



FIGURE 9.4 Praise works.

CONFLICT OF INTEREST

The collapse of *Enron*, and revelations of widespread destruction of company documents by its auditors bring to mind the difficult position of auditors in any business. Auditors face a challenge because in some sense, they inevitably have a conflict of interest. In the financial world, auditors ostensibly serve the interests of stakeholders, including shareholders employees, suppliers, and clients of the organization they audit. Inevitably, financial auditors also serve at the discretion of decision makers within the very firms they are auditing.

The *Equity Funding* fraud was a widely publicized case in the early 1970s. The *Equity Funding Corporation of America* (EFCA) falsified its financial records to appear profitable to investors who were grossly cheated:



FIGURE 9.5 Greed.

...EFCA ... falsified financial records beginning at least as early as 1964 and continuing until the date the petition was filed. The falsification primarily consisted of inflating or creating assets and income, failing to record liabilities, and creating bogus insurance policies, which were then coinsured.... Following the completion of an audit by Touche Ross & Co., the Court-appointed auditors, more than \$143 million of fictitious or fraudulently inflated assets were eliminated from EFCA's books, and more than \$42 million of assets were written down to reflect more realistic values.¹⁵

The auditor who testified to the *probity* of EFCA derived some 80% of his revenues from that client; he was willing to accept unverified reports that were delivered late – late because they had been fabricated the night before by a management team. However, standards of the auditing profession explicitly state that

...[T]he auditor's unqualified opinion is an expression of reasonableness and fairness, but not of absolute assurance. This limitation arises because of the economic infeasibility of examining every transaction and every document relating to every transaction.... [F]raudulent activity which a detailed examination would not necessarily detect are: forgery, collusion, and unrecorded transactions.¹⁶

The auditor also had a very serious *conflict of interest*: (a) spend too much money examining records and he could be fired; (b) offend his client by issuing a negative report and a major portion of his income would disappear because nervous potential clients might decline to hire him in future.

In the *Enron* case, it appears that the company's auditors were also supplying extensive consulting services in addition to their auditing services:

Enron's auditor, Arthur Andersen, has been accused of applying lax standards in their audits because of a conflict of interest over the significant consulting fees generated by *Enron*. In 2000, Arthur Andersen earned \$25 million in audit fees and \$27 million in consulting fees. It is difficult to determine whether Andersen's audit problems at *Enron* arose from the financial incentives to retain the company as a consulting client, as an audit client or both. However, the size of the audit fee alone is likely to have had an important impact on local partners in their negotiations with *Enron's* management. *Enron's* audit fees accounted for roughly 27 percent of the audit fees of public clients for Arthur Andersen's Houston office.¹⁷

Attempts in recent years to pass legislation making it illegal to provide both financial auditing services and consulting services to the same clients by a single firm have been strongly resisted by a number of large firms; lobbyists have paid large sums to the re-election funds of many politicians who subsequently voted against such restrictions to reduce conflict of interest.¹⁸

Providing favorable treatment of special interests because of large “campaign” contributions (legitimately described as *bribes* in some cases¹⁹) sets up an inevitable conflict of interest between the protection and promotion of voter interests and protection and promotion of contributor interests. Legislators admitted as much in public hearings about the *Enron* failure and have stipulated that “Members, officers, and employees are generally prohibited from using their official position for personal gain.”²⁰

In a corporate environment, setting the information-security function as a subset of the IT function potentially establishes a conflict of interest. We know that it is unacceptable to have the head of quality assurance report directly to the head of programming; similarly, I argue that it is unacceptable to have the head of IA reporting directly to the head of IT. For example, the explicit or implicit goals of a CIO may center on a short time-horizon such as the quarterly bottom line in the profit-and-loss statement. Such a narrow focus may originate because that's the way the CIO was trained in business school that's what the *Board of Directors* demand, or because the CIO plans to leave the company soon; either way, spending money on IA will not suit the purposes of such an officer. In contrast, the goals of a CISO need to be long term and to encompass business requirements, not merely technology issues. Protecting corporate information assets may conflict with the cheapest method of accomplishing a specific task; the interests of the CIO and of the CISO will therefore conflict.

In my opinion, a CISO should report at the same level and have the same level of authority as the other chief officers – the CIO or the *Chief Technology Officer* (CTO), the *Chief Operating Officer* (COO), and the *Chief Financial Officer* (CFO) – and should report directly to the CEO or even to the *Board of Directors*.

BAD REPORTING STRUCTURE

A reader wrote to me in 2002:

I am a subscriber and regular reader of the *NetworkWorld* series of emailed articles. One that has caused me much reflection was the ‘Security and conflict of interest’ article (NWF on Security, 1/29/2002). So much so that I was inspired to write you and ask a (hypothetical, of course) question.

If one found oneself in such a position (i.e., where a CISO reported directly to a CIO and felt as you do about the potential for a conflict of interest, how should the CISO approach said CIO with this opinion? I’m sure you can imagine how potentially confrontational such a concept could become. It is arguable that, should the CIO refuse to contemplate the idea, the CISO would then be duty-bound to escalate the recommendation to the CEO. The supposed reason for the CIO’s refusal being that s/he is ‘hiding something.’

I believe that, in good conscience, the above scenario would be the *right* way to go about it, but if I were in that position I would be hesitant to pursue it, as it could also well become a ‘career-limiting move’. Any thoughts you have on the subject would be welcome.

I responded as follows (slightly edited):

Your point about approaching the CIO directly before bringing the possible realignment makes a lot of sense; it’s always best to talk one-on-one with someone when developing a new idea. I have always found, “I need your help” to be a good start to explaining one’s idea.

It also seems to me that the way to broach this subject most successfully involves a multi-pronged approach.

- First, you should ensure that your relationship with the CIO were founded on a genuine sense of collegiality and mutual respect at the least; if possible, I would hope for a sense of friendship and trust as well. Naturally, these conditions may be impossible to achieve due to personality conflicts, justified lack of trust, or actual criminality on the part of the CEO.
- Second, you should document everything leading to your recommendations and have the documents date-stamped, notarized, and stored in sealed envelopes in a corporate high-security safe with two signatures required for retrieval of the documents.
- Third, in my discussions with the CIO, I’d preface my comments with the assurance that nothing you say is to be interpreted as an attack on anyone’s integrity, least of all your colleague’s. You are proposing a structural change to reflect the needs of the entire organization; such careful definitions of independent responsibility can help to prevent the kind of disaster that seems to have occurred at the Enron corporation last year. And if you do get fired, I’d suggest you get an attorney who specializes in wrongful-dismissal suits. You are not supposed to be fired for suggesting improvements in corporate governance.

Speaking of Enron, that case may be a real gift to everyone concerned about independent oversight. Not only does it provide an object lesson in what can go wrong when people fail to maintain the highest standards of the accounting and auditing professions, but it also gives everyone with your concerns a straightforward example of the possible consequences of failing to act on principle.

If your CIO really is crooked, consider the alternatives:

1. Get fired for doing the right thing.
2. Lose your job when the company fails or you are accused of incompetence.
3. Even worse, you could be accused of collusion with the criminals and then face prosecution and possible time in jail.

Personally, I’ve rarely been in a situation where I thought I might be fired for riling an executive. In the mid-1980s, I was asked by a company president to prepare a brief showing how we could sue a



FIGURE 9.6 Angry boss.

relational-DB manufacturer for troubles our programmers had experienced in using their product. I began my research willingly, but the longer I studied the case and the more programmers I interviewed, the less I believed that the fault lay in the software. After a month of work, I submitted a brief that made a strong case against going to court. The president, somewhat ruffled, told me he was not expecting that result, but after reading the report, he didn't fire me.

In another situation, a general manager so enraged the staff that we banded together to demand changes in his micromanagement style so we could get our work done like adults. I was nominated as the spokesperson, so one afternoon I found myself telling the boss that if he didn't improve we'd all quit. Let me tell you, I didn't know what his response would be and I was seriously looking at the employment ads before I went into that meeting; however, to our relief, the boss, although really angry at first, did not in fact fire me or anyone else. He actually improved his style!

In conclusion, just think about the Enron executives who went along with the questionable actions of their hierarchical superiors – how do you think prospective employers regard their having stayed on quietly?

QUIS CUSTODIET IPSOS CUSTODIES?²¹

I received another interesting response to my original article about conflict of interest. I have altered some of the details to protect the authors, who understandably wanted to remain anonymous for their own safety:

We are a security and auditing software technology provider in a third-world country. Just recently we finished an assessment of the internal information security and auditing of the Justice Department....

However, one area of interest is the several thousand video tapes, sound tapes and related documents of the previous government, mainly the video tapes of the ex-head of the Federal Investigation Agency, of his many meetings, during which he paid bribes to control, manipulate and rob the country.

Currently the anti-corruption judges, staff and prosecutors are reviewing these tapes and transcripts, and almost daily they are uncovering the identity of other corrupted people in all areas of government and the private sector. In a part of the world where corruption has been a way of life for centuries, ... one can imagine the attempts made to gain access to these tapes ... and have them “permanently misplaced”....

The Justice Department is evaluating technology to digitalize all the tapes and documents, mainly for security reasons: controlling access, backup, etc.

What we have asked them, is who in fact will be in charge of the system? Who will be responsible for managing all users and administrators, access rights and permissions, etc.? Based on what we know of international security and auditing standards, rules and policies, it certainly cannot be any of the people who will use this system or anyone in the IT department, ALL OF WHOM HAVE A POTENTIAL CONFLICT OF INTEREST. Currently IT security is an IT department responsibility.

Talk about financial audit integrity, where the CFO can write a check and erase the transaction from his General Ledger; imagine what potential security issues the Justice Department will have if they implement this system with their current IT security and auditing structure. We have [been working on deciding] these basic issues and [to] define them, and [to] pass laws if necessary ... [on]... who will enforce what is decided, before they even begin to evaluate any specific software solutions and start the budgeting process.

I will update you as we learn if they have any common sense and reality in these basic premises and realities. The book *Secrets and Lies: Digital Security in a Networked World*, by Bruce Schneier, has appropriate words for your point: “If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”²²



FIGURE 9.7 Guarding the guards.

EMPLOYEE PREPARATION FOR RESISTING SOCIAL ENGINEERING

Some organizations make new employees go through training in their first weeks on the job. Unfortunately, fewer organizations bother to continue the process of training to adequate levels of employee integration. In general terms, such inadequacy results in higher rates of error, decreased employee satisfaction, and increased turnover.²³

Even if technology were not constantly changing, it would make sense to refresh the memory of employees on critical technical issues such as information security. In addition to formal courses, employees should be stimulated to consider security an intrinsic component of their work. As the respected security expert Bruce Schneier noted decades ago, security (like quality) is a process, not an end-point.²⁴

We know that many intrusions or abuses of secured systems are accomplished by social engineering: Employees are too often willing to give away valuable information to strangers in response to a personable voice and friendly tone. Phishing attacks depend on tricking employees into accepting dangerous files and links sent by criminals. Programmers who don't consider security in the design and implementation of code leave gaping vulnerabilities in their products; programming managers who don't insist on separate quality-assurance testing put insecure code into production with potentially disastrous consequences.

It is lack of awareness that allows criminals to take advantage of innocent, ignorant, and overly trusting people. Security-awareness programs must involve committed, repeated, germane examples of security vulnerabilities and violations in organizational newsletters or bulletins. Employees should participate in security drills that can be turned into enjoyable exercises in perspicacity and intelligent response.

The problem is that deceit can have profoundly disturbing effects on the deceived. If you hire someone to lie to your employees, don't be surprised if you generate a lot of anger and maybe even a few resignations. If the victim of social engineering makes a mistake and compromises security in this kind of test, you might find your organization facing a lawsuit for emotional suffering.²⁵ At the least you will find a drop in morale.

What kind of preparation can help to avoid these consequences?

I was speaking with the head of the lifeguards at the *Westmount Municipal Pool*²⁶ many decades ago and learned that the lifeguard team would arrange for occasional, unannounced drills in the pool. She explained that the pool management had approved a plan whereby a lifeguard or member of the swim team would simulate distress so that the lifeguard on duty could practice responding. This exercise was done with *thorough preparation*: everyone on the roster was aware of the possibility that there would be a simulation. The timing was unannounced, but the fact that there would be a simulation was understood by all.

One of the points the lifeguard told me is that during the planning phase, some members of the group raised concerns about lowering the thoroughness of response to an emergency if a lifeguard thought it might be merely a test. The group agreed explicitly that all apparent emergencies would be treated as real.

I think that we can apply the same principles in our own work.

First, as always when testing security, the attackers (whether internal or external) must obtain written authorization from the appropriate levels of management before any such analysis is carried out. Above all, employees should never attempt to test their organization's security without such written authorization. "Testing security" without permission is reasonably interpreted as violating the *Computer Fraud and Abuse Act* (CFAA), 18 US Code 1030(a).²⁷

At *Norwich University* we had a case in 2011 in which a freshman hacked the administrative systems of the University on his first day on campus. He claimed he was trying to be helpful, but he



FIGURE 9.8 Criminals in innocents' clothing.

never bothered to tell anyone what he was about to do, so he was expelled on his third day at school for violating the University's *Acceptable-Use Policy*.

PREPARING STAFF FOR SOCIAL-ENGINEERING TESTS

When preparing for a penetration test that involves social engineering, everyone in the organization should be thoroughly trained to understand the techniques of social engineering before beginning the tests. The key points are as follows:

The entire organization can prepare for social-engineering simulations as a team; no one is to be subjected to attempted deception without knowing that the experience was part of a training and awareness exercise. Even if someone falls for a trick, the emotional effect is far less than if the same error occurred without preparation. In an organization-wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering can be reduced.

Preparing staff for the onslaught of skilled social engineers has many benefits. We can frame the exercises as a form of game or contest: who will be the best at spotting the confidence tricksters? Who will be quickest to foil their nefarious plans? Role-playing games are an excellent way of changing beliefs, attitudes, and behavior: having staff members take up the roles of social engineer and defender – and then reversing roles – is not only amusing, it has a long-term effect on people's perceptions. It's much easier to remember a social interaction we've experienced personally than to pay attention to abstract words. We can even turn the event into an opportunity for a good deal of fun and laughter, making security and secure behavior a positive experience instead of the usual drudgery.

Moreover, in addition to risk avoidance (reducing the likelihood of hurt feelings, frustration and anger), solid preparation can result in increased vigilance at all times. Once staff members are sensitized to the social engineering tricks they've experienced in role-playing games, they are more likely to recognize them in strangers. Having practiced alerting the security team to apprehended breaches, they will find it easier to take the initiative later when they spot real breaches.

One particularly useful and widely used social-engineering training is helping employees recognize and avoid phishing attacks by providing examples of phishing.²⁸ System managers should randomly send plausible phishing messages via email to randomly selected employees and have the phishing links go to Web pages that say something like "YOU'VE BEEN PHISHED!" and explain (nicely) which features of the fake phishing emails should have warned the victims not to click on the links.

Sending the same fake phishing message to everyone in the group is not a good idea because word can spread too easily among the recipients and reduce the effectiveness of the program.

An additional technique to make the experience positive is to award points (and perhaps ultimately prizes) to the users who forward the fake phishing messages to the security group because they recognize the problem. This approach has the added advantage that members of the group may get into the habit of forwarding *all* suspicious messages to the security group, increasing the likelihood that warnings can be sent quickly to alert possible victims to avoid specific new phishing messages. Again, recognizing and praising (and perhaps rewarding) group members who collaborate in the security programs can increase participation.



FIGURE 9.9 Prepare!

BEWARE OF UNINTENDED CONSEQUENCES

Although I began programming in 1965 and began programming professionally for a 4GL compiler project in 1978, I have maintained a lifelong interest in science in general and biology in particular. Some readers may know that my original field of study (60 years ago) was biology. My doctorate was in invertebrate zoology and applied statistics. One of the journals I still read regularly is *Science*²⁹ from the *American Association for the Advancement of Science* (AAAS).³⁰ An article from 2006 brought to light some unexpected consequences of the Health Insurance Portability and Accountability Act (HIPAA).

Jocelyn Kaiser wrote a report in the March 17, 2006, issue entitled, “Rule to protect records may doom long-term heart study.”³¹ It seems that a major research study on heart attacks, the *Minnesota Heart Survey*, suffered some serious interference in its data gathering due to the strict requirements for patient confidentiality imposed by HIPAA and by state regulations. Specifically,

...[T]he Privacy Rule... gives patients access to their medical records and restricts how health care providers use them... One key change from existing practices requires researchers outside the provider organization to obtain written consent from each patient...or... to get a waiver from their institutional review board (IRB). Researchers can also receive a data set stripped of identifying information.

According to principal investigator Professor Russell V. Luepker, these rules made it extremely difficult to obtain medical information for their research. The article details a number of workarounds, but the essential point is that the *HIPAA Privacy Rule* and the state laws unexpectedly made some types of valuable contributions to the progress of medical science far more difficult than ever before.

Luepker and other scientists needed *some* identifier for the patient records because they were conducting longitudinal studies – time series that looked at patient histories. Stripping out *all* identifying data ruined the data set for their needs.

But as long as there was a *single* unique identifier that allowed records to be correlated, one could have provided stripped data (e.g., no name, no address) with lots of value for the researchers while preserving patient confidentiality.

Here’s where information-security technologies would have been helpful. It would have been simple to encrypt a unique or nearly unique identifier such as the *Social Security Number* (SSN)³² using the Public Key Cryptosystem (PKC) so that patient records would be correlated securely even across medical institutions with complete privacy protection. One would need to establish a single public key held by, say, the *National Institutes of Health* (NIH).³³ All researchers could receive patient data sets anonymized by converting the patients’ SSNs to a unique ciphertext using that NIH public key. The trick would be that the secret key generated at the same time as that public key would be destroyed; that is, no one would have a reasonable means of decrypting a particular ciphertext to deduce the original SSN. So patient confidentiality would be preserved but all the juicy clinical details would still be available for the scientists.

On a more general note, the wording of the *Privacy Rule* in *HIPAA* and of similar U.S. state laws illustrates the rule of unintended consequences. In our own work in IA, we ought to be careful to run pilot programs and studies to see if our brilliant ideas and stunningly precise policy formulations are actually having the effects we want – and only the effects we want.



FIGURE 9.10

Unwanted surprise.

SYSTEM ADMINISTRATION

Managers should fulfill their legal and professional obligations by supporting technical staff for basic system hygiene:

- Establishing a sound security architecture
- Staying up to date in the versions of security software and operating systems

- Monitoring intrusions using widely available auditing and IDS software
- Establishing computer emergency response teams so that the organization can intelligently respond to accidents and attacks; and
- Managers may also want to investigate the growing number of security assessment or evaluation services



FIGURE 9.11 System administration.

Managers should be aware that there are many resources available at no cost to keep their technical staff informed of new vulnerabilities and exploits. For example, the U.S.-based *Computer-Emergency Response-Team Coordination Center* (CERT/CC) of *Carnegie Mellon University* provides a wealth of data in its *Vulnerability Notes Database*.³⁴ The *National Vulnerability Database* (NVD) managed by NIST has thousands of useful entries:

The NVD is the U.S. government repository of standards-based vulnerability management data represented using the *Security Content Automation Protocol* (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes DBs of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.³⁵

Failure to assign responsibility to specific employees for keeping up to date with these and other vulnerability resources would be a serious error of judgment that could be construed as a failure to exercise duty of care and result in legal pursuits by those harmed by such incompetence.³⁶

ESTABLISH EFFECTIVE SECURITY CONFIGURATIONS

Security must adapt to constantly changing technical environments. For example, security managers in the 1950s had never heard of e-mail; those in the early 21st century are having to adapt to artificial intelligence.

An obvious concern because of the immense increase in connectivity is that every system with links to the Internet must have properly configured firewalls to implement security policies governing access to corporate data. Firewalls filter packets to and from the Internet, allowing control over what kinds of commands can be carried out on corporate systems by remote users.³⁷ Many firewalls are improperly configured.³⁸

Another frequent problem in network design is that there are no internal barriers to access; any employee can access any part of the corporate system, and anyone penetrating the external perimeter automatically has access to everything in the network. *Internal network firewalls* should be



FIGURE 9.12 Security tools.

placed strategically within an organization to reduce violations of security policies by employees and to limit the damage that can be caused if the external firewalls are breached.³⁹

MAINTAIN SOFTWARE

Most of the attacks on systems exploit known vulnerabilities, as stated by a group of government security agencies:

This Joint Cybersecurity Advisory was coauthored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI).

This advisory provides details on the top 30 vulnerabilities—primarily *Common Vulnerabilities and Exposures* (CVEs)—routinely exploited by malicious cyber actors in 2020 and those being widely exploited thus far in 2021.

Cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations worldwide. However, entities worldwide can mitigate the vulnerabilities listed in this report by applying the available patches to their systems and implementing a centralized patch management system.⁴⁰



FIGURE 9.13 Software maintenance.

Perhaps the single most important problem we face in managing security is that system personnel fail to keep their software up to date. Every system manager must ensure that their team includes at least one employee (preferably at least two) specifically tasked with subscribing to the alert services from all their hardware and software vendors and helping to decide which patches to install when. Operating-system patches are particularly important.^{41,42}

Knowing about patches is a good start, but the essential response is to implement security patches as soon as *reasonable*. In this context, judging when it is reasonable to install patches depends on how serious the vulnerability is, how trustworthy the patch is, and how much disruption installing the patch will cause to production at any given time. In production systems, patch installation must be planned carefully.

When I ran technical services at a large service bureau in the 1980s, I typically waited at least a week after a patch was published in the equipment-provider's software bulletin; I wanted to be reasonably sure that the patch worked correctly. Because we ran 365/24 operations, we installed operating-system patches only on weekends with warnings to the customers to be ready to participate in system testing. We would make two full backups, switch our disk drives to their spare disk packs, update the spare packs to match the data on the production disks, install the patch(es), and test the updated system all Saturday with the cooperation of assigned personnel from all our client companies. If there were no problems, I would give the go-ahead to install the patch(es) on the production packs on Sunday.

SECURE YOUR WEB TRANSACTIONS

Most organizations active on the Web understand the importance of security for their customers and trading partners. Even though the likelihood that any given packet will be intercepted while in transit on the Internet is very low, the business climate today practically demands encrypted traffic for any confidential information going over the Net. *Secure Sockets Layer* (SSL), for example, is a straightforward tool for satisfying the public demand for secure transactions.

Having an SSL ensures that the sensitive data of your website's visitors will be transferred over a secure network. Despite this important component of SSL, many end-users and organizations have delayed their adoption due to the price of the certificates and the complexity of implementation. Today, getting an SSL certificate is much easier because there are initiatives that provide them for free and have made their installation super simple.⁴³

Customer data captured during secure transactions should be safeguarded. Unauthorized release of such data could be a public relations and legal quagmire. In some cases, such as medical records, unauthorized disclosure may be a felony, depending on the jurisdiction. Customer data should be kept only if they will be used again; for example, keeping a customer's credit-card number on file without their explicit instructions or permission is a foolhardy error. Those data that must be kept should be encrypted so that unauthorized employees cannot access information they have no business seeing; key points (discussed in detail) from a PAYSIMPLE white paper include:

1. Understand your obligation
2. Use only approved equipment and software
3. Use only approved service providers
4. Never store electronic track data or the card security number in any form
5. Make sure all electronic storage of credit card account numbers is encrypted and all paper storage is secured
6. Make sure any phone recordings that contain credit card account numbers are encrypted.⁴⁴

Cached pages with secure information are vulnerable to examination by unauthorized personnel while they reside on disk; luckily, some browsers have changed over the decades to disable automatic caching (allowing caching using opt-in methods) but some have not. There are detailed instructions available for implementing and testing default deletion of SSL pages for a wide range of browsers and systems.⁴⁵

Another critical element of success in today's Internet is a strict privacy policy. Generally speaking, it is a bad idea to try to make money by selling customer data; the public repeatedly expresses its repugnance at having private information revealed to third parties, especially for gain.⁴⁶ Whatever you decide to do with customer data, your policy should be displayed clearly and correctly on your website.

DETECT SECURITY BREACHES

One of the changes in the security paradigm over the last few years has been a realization that we will not succeed in achieving perfect security. Our perimeters will be breached; authorized personnel will make mistakes; there will occasionally be problems stemming from dishonesty or from revenge. It is therefore appropriate for us to detect such breaches and be prepared to respond intelligently to them.

The least responsive approach to detecting problems is to examine log files or audit trails. The disadvantage of this approach is that one detects problems long after they have occurred. A better tool – one that complements



FIGURE 9.14 Commerce on the Web.



FIGURE 9.15 Breach detection.

a good audit trail – is a modern IDS.⁴⁷ These software tools identify unusual patterns of system use. Depending on their sensitivity, they can flag anomalous behavior by internal personnel (e.g., having an accountant login to the financial system at three in the morning) as well as spotting intruders by recognizing attack profiles. Such software can be programmed to alert system management to a potential problem using a variety of tools; for example, alarms, email, pagers, and even telephone calls.

Signature-based IDSs (SBIDS) use DBs of information about known attacks; *anomaly-based* IDSs (ABIDS) monitor each system's normal patterns of use and generates alerts when unusual activity occurs.⁴⁸ SBIDS can generate more false negatives (failing to detect an intrusion) and ABIDS can generate more false positives (labeling an unusual but acceptable event as an intrusion. On the other hand, ABIDS can better identify zero-day exploits. Ideally, both strategies can work together to enhance system security if system personnel respond appropriately to the generated alerts.

PENETRATION TESTING

Vulnerability analysis is a useful approach to measuring the success of INFOSEC policies; it's especially useful when there are known vulnerabilities introduced into a system and the percentage of identification of those known vulnerabilities is used as a measure of the quality of the penetration testing itself.

Penetration testing, often called *pen-testing*, is one tool that can support vulnerability analysis.⁴⁹ By itself, however, penetration testing – simply looking for a way to penetrate a security perimeter – is an inadequate measure of security. The important issue is not that a single breach was possible; that's almost inevitable if the attacker has enough time and determination to accomplish the breach. A wider perspective insists on identifying as many vulnerabilities as possible so they can be removed. The widest perspective analyzes the corporate culture of the target to understand why the vulnerabilities were present at all, then moves to fix the underlying processes so that new vulnerabilities can be prevented.

Some general principles:

- There is little point in penetration testing BEFORE we have provided.
 - Assurance that the pen-testers fully agree that their goal is to FIND PROBLEMS, not to show that there are none.
 - Awareness and training for all employees about the planned tests.
 - Role-playing exercises to prevent trauma if social-engineering techniques are part of the pen testing.
 - Assurance that individual mistakes will not be pinned to named individuals (mistakes do not include deliberate malfeasance).
 - Plans for positive (not negative) reinforcement such as prizes, honorable mentions and so on for low-vulnerability groups and systems.
 - Audit to locate obvious technical and procedural problems that are to be fixed *before* the pen-testers begin their work.
 - Post-test analysis plans similar to incident-response planning so that the best possible use can be made of the information.
- In addition, we should discuss the importance of legally valid contracts authorizing the pen-testers to perform their work without being charged with violations of the CFAA.
- Any information gathered by the pen-testers that includes personally identifiable data must be protected according to legal requirements; for example, U.S. HIPAA, U.S. *Family*

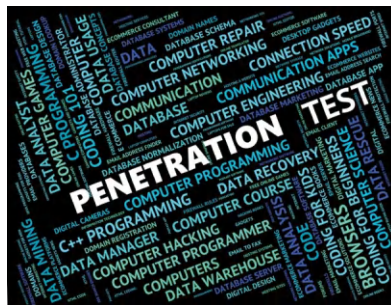


FIGURE 9.16 Pen-tests.

Educational Rights and Privacy Act (FERPA),⁵⁰ European Community General Data Protection Regulation (GDPR),⁵¹ and corporate policies.

- Pen-testers must be required to protect the confidentiality of all results of the exercises to protect the client-corporation's safety against illegal use of the discovered vulnerabilities and damage to their reputation.
- External pen-testers should be bonded to prevent bad actors from infiltrating the systems under test.

One question arises when planning such penetration analysis is whether social-engineering techniques should be used. My consistent answer is “No, not unless you are prepared to do an awful lot of work before trying it.” The same principles that were discussed in the section on *Employee Training & Social Engineering* apply to pen-tests.

PEN-TEST ANALYSIS

In an organization-wide debriefing, the results of the tests can be discussed so that everyone learns from the experience without feeling humiliated. The essential point is that by turning penetration analysis into a collective exercise, the disadvantages of social engineering and all the weakness-discovery methods can be reduced.

If most people *succeeded* in resisting social-engineering tricks or avoiding various errors, the atmosphere of the postmortem can be cheerful and low stress: that's the easy case.

One can capitalize on the success by analyzing the successful cases; ask the people involved how they spotted the fraud, how they responded, and if there's anything they would suggest improving the response. Ask the social engineers what they could have done to reduce suspicions or respond better to the successful resisters, thus increasing general awareness of threats. Role-playing is a powerful tool for such work – and then the group can brainstorm additional countermeasures.⁵² The whole exercise becomes a positive team opportunity for security improvement through encouragement, praise, and good will.

But how can one approach the postmortem analysis to minimize stress when most people *failed* to counter the social engineers? Those people will be entering the discussion with a natural sense of discomfort at the least – dread and shame at the worst. It's important to set the tone at once.

“We're here to learn from the exercise – that's what it's all about. I don't want anyone to feel that they have failed the group or are a Bad Person: the exercise is *succeeding* by bringing out areas we have to improve. Now let's get down to business.”

And by the way, that statement has to be *true*: group leaders should not pretend that they are positive about the exercise if they are internally contemptuous and hostile because of the successful trickery of the social engineers. Instead, the group leaders have to either resolve their feelings before the meeting or find someone else to lead the meeting.

During the postmortem, it can be helpful to use role-playing again. The people who were tricked can be encouraged to figure out what they missed, perhaps with the help of the social engineers or others. Group moderators can encourage members (including, *if they wish*, the victims of the trickery) to act out successful resistance to the tricks, reinforcing the sense that the session is a learning experience. Keeping the tone light, friendly and positive will help counter what could otherwise become a session of bitter and dispiriting self-flagellation or even abuse.

Most important in all cases is to keep a record of the suggested improvements and then to plan how to implement them in a phased sequence according to the criteria the group decides on. The

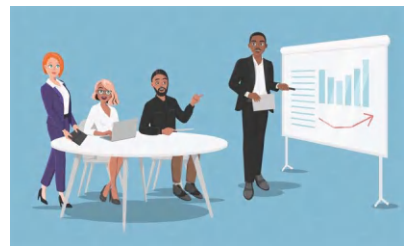


FIGURE 9.17 Pen-test analysis.

criteria for scheduling the improvements can include resource limitations and dependencies among the recommendations. Recording the sessions can provide information for members who were unable to attend as well as increasing the pressure on managers to ensure collaborative, friendly behavior.

Finally, allowing such postmortems to turn into abusive confrontations can be the basis of lawsuits for hostile working environments:

Technically, a hostile work environment is a workplace in which the conduct of supervisors or coworkers has created a discriminatory environment that a reasonable person would find so abusive or intimidating that it impacts the ability to work.⁵³

HANDLING BAD NEWS

Here's a scenario to consider.

You've installed a new system – say (using fake terms), a new ectopic frizzilator for the gandromorphic exilitory network⁵⁴. You've configured it according to specifications and have opened it for full access by your users.

Two days after the system opens for business, a couple of authorized security personnel show up at your office with some bad news: they have discovered that anyone can launch a DoS attack on the frizzilators simply by pinging them. Turns out they were curious to know if the frizzilators responded to a ping, and sure enough, they did. Then, just to be thorough, they tried bombarding the frizzilators with pings and established that the devices went completely dead, preventing any exilitory activity at all during the ping-storm.

So how do you respond?

Do you:

- a) Thank your experts warmly for letting you know about the vulnerability, promise to keep them in the loop with news, and then get to work fixing it? Or
- b) Accuse them of hacking your systems and threaten to have them fired and even arrested?

Believe me, I have received email from users in the (b) situation and know students who have suffered the same treatment for pointing out security flaws.

Why would anyone react to helpful employees or students who go to the trouble of pointing out a security vulnerability by attacking them? Remember, I'm not talking about any kind of intrusive or damaging testing here: a ping is a normal function on any network, not a hacking tool.

I think that the (b) response is an entirely irrational, emotional reaction of fear. The people reacting this way are afraid that they will be blamed for having a security hole; instead of being grateful for having the vulnerability pointed out, they convert their fear of punishment into anger at those who have put them in the uncomfortable position of having to admit and then correct what they think of as their mistake.

But everyone makes mistakes, especially when configuring gandromorphic exilitory networks. These are complex systems, and no one should expect instant perfection. What one *should* expect is rapid response to newly identified problems; that's part of a sound continuous-process-improvement strategy.

In the MSIA⁵⁵ program at *Norwich University* that I created in 2002 and directed until 2009, I established a rule from the very first that sometimes surprised students and some faculty: any student criticizing any aspect of the program and providing a constructive solution we could use got extra points. One of our students wrote to me saying that when she told her co-workers about getting an extra point on an exam for challenging a question and answer, they looked at her in disbelief; one said that challenging an exam question in *his* graduate program would generate permanent dirty looks from the instructor for the rest of the course.



FIGURE 9.18 Bad news.

The other aspect of response (b) above may be a bad management environment. If people are punished for routine, fixable errors, it's natural that they may pass on their mistreatment to others. If you have that kind of management environment, take a look at my narrated lectures on management style,⁵⁶ leadership,⁵⁷ and organizational psychology.⁵⁸ You may be able to spread the ideas around your office and change the climate of fear over the long run.

Let's hope we can stop shooting the messengers.

USE INDEPENDENT SECURITY EVALUATIONS

Many organizations recognize the benefits of using formal guidelines and methodologies from neutral third parties in establishing their security policies. Some groups have never developed policies; others have been unable to devote enough time to maintaining those policies. Sometimes the IT staff lack expertise in information security; other times upper management have refused to support the measures known by the staff to be important for protecting corporate information assets. In all these cases, external organizations such as consultants, professional associations, and certifying authorities can serve a useful purpose to alter the corporate culture and make the best use of security expertise.⁵⁹

It is a truism in quality assurance that no one can effectively test their own creation. For example, in software development, there is a long-standing view that *both* the development team *and* a separate quality-assurance team should test software before it goes into production.⁶⁰ We tend to miss unexpected errors because of our natural bias – not something evil, just how we see the world by focusing on our world-model.

Editors have long known that authors have trouble catching errors because we know what we intended to convey: we often don't even see our own typos and grammatical flaws because we focus on the meaning of what we wrote.⁶¹

The same principles apply to security. It is more difficult to see the vulnerability in our own defensive plans because we tend to see what we *wanted* to be effective. External testing of security can be a cost-effective measure that complements internal and external audits.

The difference between an *audit*⁶² and a *test* is that the former focuses on policy whereas the latter looks at results. An *audit* looks for compliance with written security policies; a *test* challenges the system regardless of policies. Audits often use standards developed by individual professionals,⁶³ professional organizations,⁶⁴ and governmental agencies.⁶⁵

When choosing external vulnerability analysts, companies should look carefully at the backgrounds of the employees who will be checking security. I do not recommend employing firms having active or recently active *criminal* hackers on staff: these external contractors may be accessing highly sensitive information including even passwords while they evaluate system security. Before signing a contract with an external agency for a security audit, clients should require detailed background information about each member of the proposed team, including criminal records if any. There should be a legally binding section of the contract requiring protection of all confidential data that may be divulged during the security evaluation.

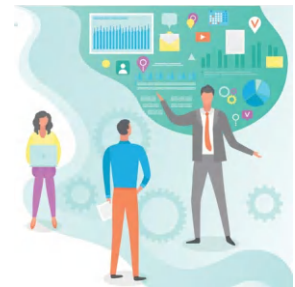


FIGURE 9.19 Independent evaluators.

WORKING WITH CONSULTANTS

One of the great developments of evolution and of civilization was specialization or the division of labor: allowing individuals to become really good at specific tasks without having to worry about all the other kinds of activity required to support life. Multicellular organisms show specialization of cell types in evolution as early as the sponges of the Cambrian period of 600 million years ago,⁶⁶ so this is hardly a new concept <smile>.

All human societies that have been studied seem to show some division of labor, even if it sometimes consists solely of different roles assigned to children, women and men, and elders. Archaeologists have long debated “whether the specialized activities that women undertake are those that lend themselves to being structured as ‘multi-task’ work, conducted intermittently to accommodate childcare.”⁶⁷ Another author proposes that the agricultural revolution of c. 10,000 BCE may have led to increased fertility, relegation to reproduction, and consequent widespread historical oppression of women in early post-Paleolithic cultures.⁶⁸

Sometimes it makes sense to get help from experts outside one’s own organization. The specialized knowledge and skills of experts may make their services too expensive to keep on hand permanently by employing them full time – and often consultants’ skills serve to initiate self-sustaining processes that don’t require constant input from outsiders.

ATTITUDES ABOUT CONSULTANTS

Some people are hostile to consultants, seeing them as threats to their own position or perceiving their use as an implicit devaluing of the employees’ competence. There are many jokes at consultants’ expense; for example, one I remember right away is “A consultant is a person who borrows your watch to tell you the time and then charges you for it.” Another favorite is this classic version of a consultant’s explanation of why the chicken crossed the road (name of the firm changed to avoid lawsuits):

Deregulation of the chicken’s side of the road was threatening its dominant market position. The chicken was faced with significant challenges to create and develop the competencies required for the newly competitive market. HyperExpensive Consulting, in a partnering relationship with the client, helped the chicken by rethinking its physical distribution strategy and implementation processes. Using the *Poultry Integration Model* (PIM), HyperExpensive helped the chicken use its skills, methodologies, knowledge capital and experiences to align the chicken’s people, processes and technology in support of its overall strategy within a Program Management framework. HyperExpensive Consulting convened a diverse cross-spectrum of road analysts and best chickens along with HyperExpensive consultants with deep skills in the transportation industry to engage in a two-day itinerary of meetings in order to leverage their personal knowledge capital, both tacit and explicit, and to enable them to synergize with each other in order to achieve the implicit goals of delivering and successfully architecting and implementing an enterprise-wide value framework across the continuum of poultry cross-median processes. The meeting was held in a park like setting enabling and creating an impactful environment which was strategically based, industry-focused, and built upon a consistent, clear, and unified market message and aligned with the chicken’s mission, vision, and core values. This was conducive towards the creation of a total business integration solution. HyperExpensive Consulting helped the chicken crossing to become more successful.⁶⁹

Sometimes the hostility shades over into abuse. I was once told by a staff member at a large corporation that he and his buddies used to string consultants along for weeks to encourage them to believe that they had a chance of winning a contract based on a *Request for Proposal* (RFP) even though the creeps had already chosen the winner. Apparently, these people had the same attitude toward consultants that sociopaths⁷⁰ have toward insects and other small animals they torture.



FIGURE 9.20 Consultants.



FIGURE 9.21
Skepticism.

GOALS FOR CONSULTING CONTRACTS

When the client and consultant are discussing problems and how the consultant could help, both parties must be conscious that a consultant always has three allegiances: to her employer (assuming she's not independent), to the manager hiring her and to the firm employing that manager. You must define the scope of the consulting assignment so that the consultant can in fact legitimately tackle the task. For example, it would be pointless for a local manager to request assistance in implementing a security solution requiring corporatewide changes. Such a project would be beyond the manager's scope.

The converse problem is consultants, especially those from large firms, which use templates to prepare consulting reports where string variables are modified to include details from the client firm, but which have little research and less analysis of the specifics of the client's situation and needs. It is an excellent practice to ask for a couple of sample anonymized reports from consultants before accepting their proposals; finding identical language in substantive sections of the two reports should give you pause.



FIGURE 9.22 Goals for consulting contracts.

EVALUATING POTENTIAL CONSULTANTS

As you evaluate potential consultants, look for those who can state their understanding of your goals clearly. I am fond of the phrase, “Let me see if I have understood” because it's a chance to test my perceptions against those of the client. Ask your candidates to tell you how they see your situation and to define the problems they perceive.

Be especially attentive to consultants who challenge your initial views of your problem: You *want* consultants who are able to think independently and bring their expertise to bear on your problems, not sycophants who are willing to hide their knowledge and their disagreement to get the contract. Just as important, you want consultants who can articulate their views clearly and non-aggressively. You need a reasoned exchange of views from which to learn, not a boxing match where winning is the object.

Sometimes consultants are (foolishly and improperly) asked by managers to produce support for a predefined set of conclusions as part of an internal political battle; consultants must be clear that their report may very well disagree with preconceptions. Indeed, consultants should be chary of accepting such assignments: they can be the kiss of death, since providing a professional result that conflicts with the client's predetermined outcome can result in slanderous comments in the community, yet unprofessionally kowtowing to unreasonable demands can justifiably lead to a tarnished reputation, litigation for malfeasance, and perhaps expulsion from professional societies.

One test you can apply to judge the professionalism of prospective consultants is to ask them to identify the limits of their professional competence. Professional consultants will clearly identify the limits of their knowledge. Faced with requests for help in areas beyond their competence, the consultant will point out that alternative sources of information would be more cost effective.

Keep track of consultants who refer you to a better resource for a specific project – their professionalism makes them good candidates for future assignments for their professional profiles.



FIGURE 9.23 Potential consultants.

CONSULTANTS' CODE OF ETHICS

The now-defunct *Consulting Alliance* had a useful *Consultants' Code of Ethics*⁷¹ that included these Responsibilities to the Client:

- A member shall always act in the best interest of the client, providing professional services with integrity, objectivity, and independence.
- A member shall accept only those assignments for which the member has the qualifications, knowledge and skill to serve the client effectively.
- A member shall, before accepting an assignment, reach a mutual understanding with the client as to the objectives, scope, work plan, and costs. A member shall establish fee arrangements with a client in advance of any substantive work.
- A member shall avoid conflicts of interest or the appearance of such. Members shall not accept simultaneous assignments from two or more clients who have potentially conflicting interests without informing all parties in advance and securing all parties' prior agreement.
- The member shall treat clients' information as confidential and take all reasonable steps to prevent it from access by unauthorized people. A member shall not take advantage of such privileged information for use by the member, the member's firm or another client, without appropriate permission.
- A member shall not engage in any malfeasance, dangerous behavior, or illegal activities in any matter related to an assignment and shall report to appropriate authorities within or external to a client organization any such activities discovered within the scope of an assignment.



FIGURE 9.24 Ethics.

Another useful tool is a list of unacceptable behaviors defined by the *International Association of Professional Security Consultants* (IAPSC)⁷²:

Unacceptable behaviors include, but are not limited to:

- Intimidating, harassing, abusive, violent, discriminatory, derogatory, or demeaning communication in any form, which includes, but is not limited to spoken, written, somatic, digital or actions by any participant in an IAPSC-supported event.
- Harmful or prejudicial communication in any form or information related to gender, race, color, ethnicity, sexual orientation, religion, disability, political orientation, genetic information, age, familial status, military status, domestic violence victim status, or other personal characteristics.
- Inappropriate use of nudity and/or sexually suggestive images.
- Deliberate intimidation, stalking/cyber stalking.
- Unwanted photography or video recording.
- Sustained disruption of talks or other events.
- Assault/battery.
- Unwelcome and uninvited attention or contact.
- Real or implied threat of physical harm.
- Real or implied threat of professional or financial damage or harm.
- Harassment committed in a joking manner still constitutes unacceptable behavior.⁷³

Clients can usefully discuss these terms with candidates for consulting contracts. Clearing the air before hiring a consultant can avoid conflicts, disappointment, anger, and litigation.

PLANNING FOR EFFECTIVE CONSULTATIONS

When you have chosen your consultant, prepare an action plan that defines what you both plan to do, by when and how you will know when to stop using their services.

One of my standard questions in any consulting assignment is, “What would you like to be able to do better than what you are doing now?”

All consulting should be aimed at *operational change*:

- Fixing what doesn’t work
- Improving what already does work
- Inventing new solutions for problems before they happen

By defining appropriate *metrics* (observable, preferably measurable aspects of the events of interest) and writing down the *levels* (specific observable goals) of the metrics that define desired results, you ensure that your external consultant focuses on *your* objectives, not a preconceived generalized concept divorced from your reality.

Finally, a consultant is not supposed to be a permanent employee of your corporate family. A reasonable expectation is that with time, the frequency of consultant visits will decline for any specific project. Require estimates of time and effort from the start of the negotiations, understanding that revisions will be appropriate as more information is collected and analyzed. Demand and expect regular reports on progress in the consulting work, including revised estimates of time and costs until completion.

CONSULTING AND TEACHING

As part of the assignment, consultants should expect to work closely with members of the client organization to impart their knowledge and methods to the client organization. Consulting should always involve teaching – long-term contributions to the client’s corporate culture.

At an airport one day in the mid-1980s, I met a consultant who did HP3000 minicomputer performance analysis, as I did. I asked him what tools he taught his clients to use in analyzing system performance; he answered, “Tools? I don’t teach any tools. Listen, if a client is going to spend thousands of dollars on a performance monitor, I’d rather he spend it on me.” I felt like throwing up.

After I wrote about that experience in my first *Office Automation* column in 1987 for the *INTEREX Magazine* of the now defunct *INTEREX* association of HP computer users,⁷⁴ the consultant phoned me after recognizing himself in the anonymized description. He asked, “Was that me??” and then proceeded to scream obscenities at me for five minutes (I put down the handset and kept working until I heard the rising inflection of a question), ending with a threat to kill me if I ever revealed his name.

That was not a consultant I would recommend to anyone.

So clients should ask possible consultants exactly how their organization will become *less* dependent on external help by paying for consulting time. When I created my old consulting company, *JINBU Corporation*⁷⁵ (the name means “progress” in Chinese), I gave it the motto *Progress Towards Autonomy*TM to summarize the fundamental notion that consultants must help their clients grow enough to dispense with the consultant’s services. I still have that motto on my current business cards.

I made it a point in my written consulting contracts to require that at least one employee of the client accompany me on all my audit activities so those persons could learn from me and share the



FIGURE 9.25 Planning.

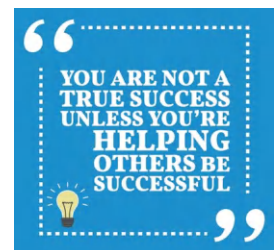


FIGURE 9.26 Consulting includes teaching.

knowledge with colleagues. The close interaction with employees also saved time (and money for the client) because I often got answers to important questions immediately or through the efforts of the client personnel.

TOOLS AND TECHNIQUES FOR EFFECTIVE ANALYSIS

In my more than 40 years of consulting work, I developed some useful methods that can be applied in many areas of management.

REAL-TIME NOTES

A technique that I developed to support effective problem-solving – and which you can discuss with potential or current consultants – is *Real-Time Notes*.

Whenever I'm interviewing staff members for an organizational or security analysis, I connect my laptop to their terminal so that the interviewee can see exactly what I am typing in my notes in real time. Back in the 1980s, the connection was from an HP 110⁷⁶ laptop using a cable; in recent years, we've been using sharing software such as ZOOM⁷⁷ for real-time access. The person can easily spot errors and make corrections or decide to suppress certain off-the-cuff comments. At the end of each interview, I transfer the notes to the interviewee right away with instructions to let me know if they think of anything else they want to add or change.

In my experience, this technique increases the cooperation of interviewees because they know they will not be embarrassed by misstatements or errors of judgment.



FIGURE 9.27 Real-Time notes.

COMPUTER-AIDED CONSENSUS

Another valuable tool I invented is *Computer-Aided Consensus* (CAC) for focus groups. Most people in business are familiar with the principles of *brainstorming*:

- The goal is to generate ideas in a group to solve specific problems.
- The group separates ideation from analysis, thus increasing creativity.
- The group leader sets a numerical goal for the discussion; for example, "Let's come up with 100 ideas on how to..."
- There is to be absolutely no positive or negative responses to any idea while they are being proposed; that limitation reduces inhibitions in the participants.
- A *scribe* typically writes the ideas (including jokes) on large sheets of paper on the walls of the room.
- When an idea from a participant prompts a new idea in another participant, there's a hand signal (e.g., thumbs up) to signal priority in contributing the new idea (thus helping to avoid forgetting).⁷⁸

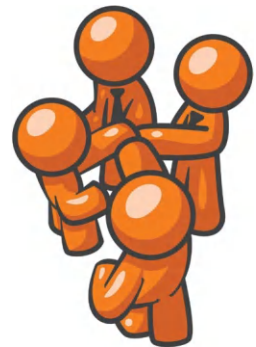


FIGURE 9.28 Consensus.

CAC extends ordinary brainstorming to include the *Delphi Technique*⁷⁹ developed by the RAND Corporation in the 1950s.⁸⁰

Participants:

- Develop quantitative estimates using expert opinions about a specific issues
- Rank the estimates

- Ask the people who provided the bottom and top quartiles of the estimates distribution for their reasons for their estimates
- Discuss the reasons
- Ask participants to revise their estimates
- Iterate to stability (e.g., when the estimates don't change from the previous cycle by more than a set limit).

In CAC, one uses a shared spreadsheet for a group to see simultaneously (e.g., projected in a meeting room or shared via electronic-meeting software).

The first step is for the group to agree on a shared *operational* scale for evaluating proposals that have been generated by brainstorming, whether synchronously (e.g., in person or in e-meetings) or asynchronously (e.g., through email or shared correspondence). Scales can be chosen for whatever metric makes sense with values that are agreed upon; for example,

- When should we start the project? (e.g., 4=this week, 3=this month, 2=this quarter, 1=this year, 0=never)
- How much time should we reserve? (e.g., 0=none, 1=a day, 2=a week, 3=a month, 4=a quarter, 5=a year)
- How many people should be on the project? (0=none, 1=one, 2=two, 3=five, 4=10, 5=25); and
- How much money should be allocated to the project? (5=\$1M, 4=\$100K, 3=\$10K, 2=\$1K, 1=\$100, 0=none)

Lay out the results of the prior brainstorming or other research method in a spreadsheet with one idea or proposal per row. Define one column per participant and have the participants enter their score for importance (priority, value...) in their column for each row of proposals or ideas.

Calculate the average of the numerical scores *and the variance* for each row of scores.

Sort the scores by descending importance or priority.

Group the ideas roughly by the priorities; for example, if there are, say, 40 ideas being evaluated and the sorted listing has a larger gap between the averages of the scores in, say, the eighth and the ninth ideas than between most of the other rows, arbitrarily define the first eight rows as a group, then *sort downward by variance* within that group. You now have a group of generally important ideas with the top item having the most *disagreement* among the scores in that group.

Now discuss the *reasons* for the most variable scores in that group and allow members to change their initial scores for the ideas as they discuss why they have such different scores. Reasons for the divergences may include:

- Different assumptions
- Divergent priorities
- Unshared and possibly contradictory information
- Different reasoning
- Mistakes

Sharing such information among the members of the team and having frank, constructive discussions about differences can speed the development of consensus. During this process, it is critically important for the group leader(s) to ensure a positive, collaborative environment, and avoid the development of hostility. Frequent recalculations and re-sorting help the participants see when they have come to stability – the sorted order within the group of proposals being discussed eventually stabilizes, so the team can move on to the next group of ideas in the sorted list.

There are notes and a narrated PowerPoint file about CAC based on my teaching materials available from my website.⁸¹

COMPUTER-AIDED THEMATIC ANALYSIS

Another tool I invented for analyzing the results of interviews and focus groups is *Computer-Aided Thematic Analysis* (CATA).⁸²

All writers face the problem of organizing written material, whether scientific papers, reports on competing products or business strategies, literary criticism, or their own insights.

It was to solve the problem of ordering information without a pre-existing analytical framework that I created CATA. CATA is usable by anyone with a computer and any software that can sort lines of text; for example, spreadsheet programs, DBs, and many word-processing programs.

In preparing this brief summary, I found reports of similar ideas and methods in the field of ethnography. Although using techniques very similar to CATA, the ethnographic software is highly specialized and the methods poorly known outside the field. CATA is a technique that is easily applied and accessible across disciplines. The use of techniques similar to CATA by ethnographers suggests its potential value in organizational analysis and in general, for the organization of research findings of any kind. It is particularly helpful to anyone involved in a literature review, such as researchers and also students writing term papers.



FIGURE 9.29 Looking for themes.

WHY I DEVELOPED CATA

In 1987, I was asked by two dear friends to evaluate the status of a research project in a discipline about which I was ignorant, community development. I was selected because my *lack* of experience would supposedly help me avoid bias and preconceptions. In retrospect, choosing a consultant because of their lack of experience with the client's business does seem strange, but that's what happened.

I interviewed 55 people for that analysis. During the interviews, I took notes on a portable computer. At the end of the data collection process, I had 450 pages of single-spaced transcript.

How was I to make sense of this daunting mass of qualitative information? Following the interview series, I extracted brief themes from each interview. For example, the following three paragraphs are from the original notes for part of an interview:

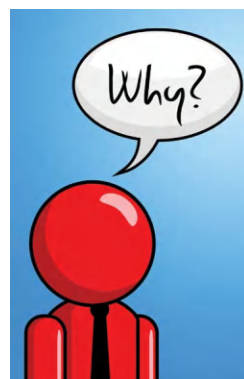


FIGURE 9.30
Origin story.

There are two areas I find weak: economic development and political development. I sometimes wonder if these are ignored on purpose. In practice, we find they're indispensable. Political and economic development return self-esteem and independence to the people. In our experience here, these are the most important aspects right now, while cultural and social development are taking place.

The other programs: Elders' Program. I have talked about this with. I still have many doubts there from the medical end. There's something missing there. From the nutritional end, also, I have to discuss things with him (he's the nutritionist, not me). And also there's the cultural thing again. But focusing on the elders is a wonderful idea, beyond doubt.

Respect for Traditions: excellent. No doubt about them. On personal note, however, whenever I've seen them, they seem overtired. Their lives don't seem balanced for their age. Their responsibilities seem huge, and I'm afraid they would wear themselves out. And they're outstanding, they're excellent.

I extracted the following themes from this section of the interview and typed them into a spreadsheet program with one line per theme. In a column assigned to represent the

particular interview, I marked the page number where the theme occurred so I could find the reference quickly.

THEME – Interview

weak: economic & political dev't – 43

wonder if economics & politics left out on purpose – 43

political & economic dev't important here now – 43

elders' program: doubts from medical end – 44

but elder focus wonderful – 44

respect for traditions: excellent. no doubt about them – 44

r.f.t. staff seem overtired – 44

r.f.t. responsibilities huge; could wear themselves out – 44

Thematic extraction from the entire 450 pages of transcript resulted in 923 themes and 15 pages of printout.

Next, I identified a few general areas into which the themes seem to fall. These categories, in no particular order, were numbered as follows:

1. ORGANIZATION
2. MATERIALS
3. APPROACH
4. HOSTILITY

I next classified each of the 923 themes using numbers assigned to these crude preliminary categories. For example, the themes above were classified as follows.

3 weak: economic & political dev't

3 wonder if economics & politics left out on purpose

3 political & economic dev't important here now

2 elder's program: doubts from medical end

2 but elder focus wonderful

2 respect for traditions: excellent. no doubt about them

2 r.f.t. staff seem overtired

2 r.f.t. responsibilities huge; could wear themselves out

The breakthrough came when the 923 themes were sorted by category. All the themes tagged with the same category code were instantly brought together into the same area of the list. Simply by inspection, a new level of classification seemed reasonable among the categories. For convenience, these new categories were identified by adding a digit to the original numerical code. For example, the themes dealing with organization were all tagged with the number "1"; they seemed to fall easily into the following subdivisions:

- 10 ORGANIZATION
- 11 STAFF
- 12 FUNDING
- 13 EFFICIENCY
- 14 SUGGESTIONS

All 923 themes were thus numbered with this new level of precision. Thematic analysis continued iteratively and recursively with more detailed classifications as required. For example, section 11, dealing with the staff within the organization, was easy to classify further as follows:

110 STAFF
 111 LEADER
 112 OPENNESS & FLEXIBILITY
 113 COMMITMENT
 114 PRACTICAL, DOWN TO EARTH
 115 GENEROUS WITH TIME, MATERIALS
 116 XX ARE ROLE MODELS

By this point, if the themes from the passage shown above had been sorted together, they would have looked like this:

308 weak: economic & political dev't
 308 wonder if economics & politics left out on purpose
 308 political & economic dev't important here now
 204 elder's program: doubts from medical end
 204 but elder focus wonderful
 211: respect for traditions: excellent. no doubt about them
 211 r.f.t. staff seem overtired
 211 r.f.t. responsibilities huge; could wear themselves out

By the end of the cycle, themes were ordered into a comprehensive structure reflecting the many comments made by respondents. Throughout the sorting and resorting, the references to origin and location followed the themes. By the end of CATA, not only could I locate every reference at once, but I could see patterns showing clusters of interviews that discussed similar themes. The clustering helped me make more sense of the complex information collected.

EXAMPLE FROM NEUROLOGICAL RESEARCH PAPER

My wife, Dr Deborah N. Black, MDCM, FRCP(C), wrote a review paper using CATA. Here are notes on two pages from a specific report ("A") taken from her spreadsheet during CATA:

paper & page – code – notes
 a71 – e – unknown whether transient paraplegia spinal or peripheral or vascular in origin
 a71 – h – great diversity in immediate effects shock individual threshold; amperage; state of brain – sleep, anesthesia...)
 a72 – b1 – intracranial bleeding, edema, single or multiple vascular lesions responsible for neurological sequelae
 a72 – c1 – ms-like picture
 a72 – c1 – hemiplegia, aphasia, choreoathetosis (rare), headache, giddiness, insomnia, forgetfulness, epilepsy (rare)

Here is her final set of categories.

A	GENERAL
B	PATHOLOGY
B1	BRAIN PATH
B2	CORD PATH
B3	PNS PATH

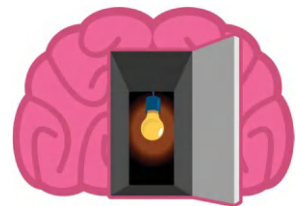


FIGURE 9.31
 Neurological CATA.

C1	CLINICAL SYNDROMES – BRAIN
C1.A	EARLY BRAIN SEQUELAE
C1.B	LATE BRAIN SEQUELAE
C1.B.1	PARKINSONIAN SYNDROME
C1.C	NEUROPSYCH SEQUELAE
C2	CLINICAL SYNDROMES–CORD
C2.A	EARLY CORD SEQUELAE
C2.B	LATE CORD SEQUELAE
C3	CLINICAL SYNDROMES–PNS
D	DNB
E	PATHOGENESIS
F	EPIDEMIOLOGY
G	PHYSICS
H	VARIABILITY OF OUTCOME
I	COMPARISONS TO OTHER CONDITIONS

This example illustrates the flexibility of CATA: there is no need for rigid standards of classification or notation. Furthermore, different sections can easily be subdivided to greater or lesser degrees.

DISCUSSION

Language determines what we see and think. For example, Whorf⁸³ emphasized that ignorance of categories leads to their invisibility. For example, Inuit people recognize many distinct categories of what more southern people lump together as “snow”; expert mushroom hunters see *gill mushrooms*, *bracket fungi* and *boletes* where the untutored see either “toadstools” or nothing at all.

In CATA, the initial step is to define working categories. The specific initial categories do not seem to be as important as simply beginning to group the data. This observation is consistent with evidence from experimental psychology that organizing information enlarges one’s capacity to remember that information.⁸⁴ For example, arranging large numbers of words into categories enhances experimental subjects’ ability to remember the words, and the larger the number of categories, the better the recall.⁸⁵

The next step in CATA is to bring similar ideas or observations into proximity. The contiguity of related information seems to foster further discrimination; it is easier to see patterns among ideas when one’s thought is not interrupted by unrelated information. This impression of what happens in CATA is consistent with research showing that context influences perception. For example, ambiguous figures such as the well-known old/young woman drawing⁸⁶ can be interpreted as either an old woman or a young woman depending in part on which version of a less ambiguous rendition of the figure is shown first or following verbal cues.⁸⁷ The context provided by grouping related information in CATA seems to spark recognition of hitherto-undetected patterns.

Why should the categorization inherent in CATA enhance our ability to work effectively with qualitative information? One factor may be our limited ability to hold in mind more than about five to nine ideas simultaneously.⁸⁸ Faced with many more ideas than this practical limit, we tend to “chunk” the information into fewer but larger categories.

As we’ve mentioned, working memory has a limited capacity. There is, however, enormous flexibility in how we use that capacity – and so, if we can pack the input more efficiently, we can increase the amount of information maintained in this memory.



FIGURE 9.32
Discussion.

For example, consider an individual who tries to recall a series of digits that she heard only once:

177620001066

If she treats this as a series of 16 unrelated digits, she'll surely fail in her attempt to remember the series. But if she thinks of the digits as years (i.e., the year the U.S. Declaration of Independence was signed; the year of the new millennium; and the year the Normans invaded England), the task becomes much easier because now she has just three items to remember.

Cases like this one make it plain that working memory's capacity can't be measured in digits, or words, or kilobytes. Instead, the capacity is measured in chunks.⁸⁹

Ethnographers have for many years used a method described as "cut the interview into topical segments and sort."⁹⁰ Specialized programs exist to help such social scientists classify and sort qualitative data. The method described here parallels the evolution of ethnographic software but can be implemented by anyone having access to computerized sorting.

One additional note: when using a modern spreadsheet, it is easy to include extensive notes that are attached to specific cells. In these notes, which may contain pages of text, the user can insert extracts of quoted material and personal thoughts and comments about the theme indicated in that particular cell. If the user runs out of room, additional notes can be attached to cells in the same row corresponding to the points of origin of each theme.

SUMMARY

CATA is a technique using simple and readily available computer software to organize non-numerical information quickly. The core of the technique is iterative sorting and classification of notes. Sorting brings similar information together, allowing one to see relationships that are otherwise not evident. The iterative component allows progressive refinement of structure as additional categories intuitively become evident.

A computer allows one to sort and edit categories quickly. Such flexibility encourages experimentation, which may lead to unexpected juxtapositions that encourage new ways of thinking.

No external framework need be imposed upon the data. One does not need an *a priori* structure into which the data are forced; CATA lets one impose such a structure or not as one chooses. Reports virtually write themselves: their organization arises from the CATA categories and their content appears in the references.

In summary, this method is useful to all computer-literate writers who wish to organize their thoughts, observations and references in preparation for essays and reports.

A narrated PowerPoint about CATA is available online.⁹¹



FIGURE 9.33 CATA overview.

CONCLUDING REMARKS

In summary, managers must understand that security cannot come simply by buying and installing a gadget, no matter how good. Security is a process, much like quality assurance. Security can and must be woven into the corporate culture of every organization, with due attention to the changing landscape of market advantage, threats, vulnerabilities, risks of damage, and extent of damage.

Keeping up-to-date is not a luxury, it's a necessity. Getting buy-in from every part of the organization is a key



FIGURE 9.34 Conclusions.

to success in security as it is in quality. Ensuring that employees are chosen with an eye to honesty and reliability, and then managing employees carefully to prevent dissatisfaction and to identify those at risk of becoming dishonest are crucial to securing information and other corporate assets.

Appropriate tools for securing systems and networks include anti-virus products, firewalls, IDSs, email logging, and proper backups.

NOTES

- 1 [Bagcilar \(2020\)](#).
- 2 [Neumann \(2023\)](#).
- 3 [Schneier \(2023\)](#).
- 4 [Cybersecurity and Information Systems Information Analysis Center \(2023\)](#).
- 5 [Kabay, INFOSEC YEAR IN REVIEW \(2006\)](#).
- 6 [Kabay, IA455 Contemporary Issues in Information Assurance \(2020\)](#).
- 7 [Kabay, CS407: Politics of Cyberspace \(2020\)](#).
- 8 [Kabay, Management Skills \(2006\)](#).
- 9 [Tennant \(2021\)](#).
- 10 [Belyh, Management by Walking Around \(MBWA\) – The Essential Guide \(2020\)](#).
- 11 [HP Alumni Association \(2021\)](#).
- 12 [CIOinsight \(2021\)](#).
- 13 [Cherry, How Extinction Is Defined in Psychology \(2021\)](#).
- 14 [Woodard \(2014\)](#).
- 15 [U.S. District Court for the Central District of California \(1975\)](#).
- 16 [Flory \(1976\)](#).
- 17 [Healy and Palepu \(2003\)](#).
- 18 [Moore, Tetlock, Tanlu, and Bazerman \(2006\)](#).
- 19 [Barnes \(2012\)](#).
- 20 [U.S. Senate Select Committee on Ethics \(n/a\)](#).
- 21 A note on the title: “Who will guard the guards themselves?” – Juvenal, a Roman satirist of around 60-140 CE (“common era” – a term used by non-Christians as equivalent to “AD” which means “anno domini” or “year of our Lord”) who harassed the power structure of imperial Rome. [Five years of Latin in high school have to be good for *something*!].
- 22 [Schneier, Secrets and Lies: Digital Security in a Networked World \(2015\)](#).
- 23 [Amo \(2019\)](#).
- 24 [Schneier, The Process of Security \(2000\)](#).
- 25 [FindLaw \(n/a\)](#).
- 26 [City of Westmount Québec Canada \(2021\)](#).
- 27 [U.S. Code \(1986\)](#).
- 28 [HelpSystems \(2021\)](#).
- 29 [Science \(2021\)](#).
- 30 [American Association for the Advancement of Science \(2021\)](#).
- 31 [Kaiser \(2006\)](#).
- 32 [U.S. Social Security Administration \(2021\)](#).
- 33 [National Institutes of Health \(2021\)](#).
- 34 [Carnegie Mellon University \(2021\)](#).
- 35 [National Institutes of Science and Technology \(2021\)](#).
- 36 [Insureon \(2021\)](#).
- 37 [Riesen \(2021\)](#).
- 38 [Starcom \(2020\)](#).
- 39 [Manx Tech Group \(2019\)](#).
- 40 [U.S. Cybersecurity and Infrastructure Security Agency \(2021\)](#).
- 41 [Harvard University \(2021\)](#).
- 42 [KernelCare \(2021\)](#).
- 43 [Nikolov \(2018\)](#).
- 44 [PaySimple \(2021\)](#).
- 45 [Open Web Application Security Project \(2021\)](#).

- 46 Hanks (2018).
- 47 Software Testing Help (2021).
- 48 N-able (2021).
- 49 HelpSystems (2021).
- 50 U.S. Department of Education (2021).
- 51 European Community (2018).
- 52 Kabay, Computer-Aided Consensus (2011).
- 53 Gilbert Employment Law, P.C. (2020).
- 54 Made up nonsense words.
- 55 Norwich University (2021).
- 56 Kabay, Management Skills (2006).
- 57 Kabay, Leadership Skills (2006).
- 58 Kabay, Applying Social and Organizational Psychology (2008).
- 59 Premier IT Solution (2020).
- 60 Reichert (2020).
- 61 Stockton (2014).
- 62 Aldoriso (2020).
- 63 Kabay, Facilities Security-Audit Checklist (2012).
- 64 International Organization for Standardization/International Electrochemical Commission (2017).
- 65 DNSstuff (2020).
- 66 Sarà (2021).
- 67 Gero (2002).
- 68 Smail (2007).
- 69 Weed (2016).
- 70 Cleveland Clinic (2021).
- 71 Consulting Alliance (2013).
- 72 International Association of Professional Security Consultants (2021).
- 73 IAPSC (2020).
- 74 Thibodeau (2005).
- 75 CAN1 Business (1999).
- 76 HP Computer Museum (2021).
- 77 ZOOM (2021).
- 78 MindTools (n/a).
- 79 Hsu and Sandford (2007).
- 80 RAND Corporation (2021).
- 81 Kabay, Computer-Aided Consensus I Notes (2009).
- 82 Kabay, CATA: Computer-Aided Thematic Analysis (2006).
- 83 Whorf (2012).
- 84 Mandler & Pearlstone, Free and constrained concept learning and subsequent recall (1966).
- 85 Mandler, Organization and Memory (1967).
- 86 Donaldson (2017).
- 87 Leeper (2012).
- 88 Miller (1956).
- 89 BrainKart (2018).
- 90 Agar (1991).
- 91 Kabay, Computer-Aided Thematic Analysis: Narrated Slide Show (2004).

WORKS CITED

- Agar, M. (1991). *The right brain strikes back in fielding* (N. G. Fielding & R. M. Lee, Eds.) Sage Publications. Retrieved September 29, 2021, from [https://www.scirp.org/\(S\(i43dyn45teexjx455qlt3d2q\)\)/reference/ReferencesPapers.aspx?ReferenceID=15449](https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=15449)
- Aldoriso, J. (2020, August 17). *Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]*. Retrieved September 23, 2021, from SecurityScorecard: <https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit>
- American Association for the Advancement of Science. (2021, September 14). *AAAS Home Page*. Retrieved September 14, 2021, from <https://www.aaas.org/>

- Amo, T. (2019, March 6). *The Negative Effects of a Lack of Training in the Workplace*. Retrieved September 14, 2021, from Small Business Chronicle | Managing Employees | Employee Performance: <https://smallbusiness.chron.com/negative-effects-lack-training-workplace-45171.html>
- Bagcilar, S. (2020, September 2). *The Competitive Advantage of a Strong Security Program*. Retrieved September 13, 2021, from BITSIGHT: <https://www.bitsight.com/blog/why-you-need-to-build-a-strong-security-program>
- Barnes, R. (2012, August 12). *The High Court: When Is a Campaign Contribution a Bribe?* Retrieved December 8, 2021, from Washington Post: https://www.washingtonpost.com/politics/the-high-court-when-is-a-campaign-contribution-a-bribe/2012/08/12/68cdd94e-e2f9-11e1-a25e-15067bb31849_story.html
- Belyh, A. (2020, July 28). *Management by Walking Around (MBWA) – The Essential Guide*. Retrieved September 30, 2021, from CLEVERISM | Magazine: <https://www.cleverism.com/management-by-walking-around-mbwa/>
- BrainKart. (2018). *Acquisition: Working Memory, Long-Term Memory*. Retrieved September 29, 2021, from BrainKart | Psychology | Memory: https://www.brainkart.com/article/Acquisition-Working-Memory,-Long-Term-Memory_29330/
- CAN1 Business. (1999, October 26). *JINBU CORPORATION*. Retrieved September 28, 2021, from CAN1 Business | Company | Dissolved: <https://www.can1business.com/company/Dissolved/Jinbu-Corporation>
- Carnegie Mellon University. (2021, August 10). *Vulnerability Notes Database*. Retrieved September 15, 2021, from CERT Coordination Center: <https://www.kb.cert.org/vuls/>
- Cherry, K. (2021, Jun 27). *How Extinction Is Defined in Psychology*. Retrieved September 30, 2021, from VERYWELMind | Theories: <https://www.verywellmind.com/what-is-extinction-2795176>
- CIOinsight. (2021, May 12). *Management by Wishful Thinking Is More Common than You'd (Wish to) Think*. Retrieved September 30, 2021, from CIOinsight | Leadership: <https://www.cioinsight.com/news-trends/management-by-wishful-thinking-is-more-common-than-you-d-wish-to-think/>
- City of Westmount Québec Canada. (2021). *Pool*. Retrieved September 30, 2021, from City of Westmount | Recreation & Culture: <https://westmount.org/en/recreation-culture/sports-recreation-department/pool/>
- Cleveland Clinic. (2021). *Antisocial Personality Disorder (ASPD)*. Retrieved from Cleveland Clinic | Health | Diseases: <https://my.clevelandclinic.org/health/diseases/9657-antisocial-personality-disorder>
- Consulting Alliance. (2013, September 9). *Code of Ethics*. Retrieved September 24, 2021, from Consulting Alliance: <https://web.archive.org/web/20130909160116/http://www.consultingalliance.org/Default.aspx?pageId=106159>
- Cybersecurity & Information Systems Information Analysis Center. (2023, August 8). *Cybersecurity & Information Systems Digest of the Information Analysis Center of the US Department of Defense*. Retrieved August 27, 2023, from CSIAC | Digests: <https://csiac.org/digests/>
- DNSstuff. (2020, March 10). *What Is an IT Security Audit?* Retrieved September 23, 2021, from DNSstuff: <https://www.dnsstuff.com/it-security-audit>
- Donaldson, J. (2017, July). *Young Woman or Old Woman: My Wife and My Mother-in-Law*. (F. Macpherson, Ed.) Retrieved September 29, 2021, from The Illusions Index | Explore Illusions: <https://www.illusion-sindex.org/i/young-woman-or-old-woman>
- European Community. (2018, May 25). *General Data Protection Regulation (GDPR)*. Retrieved October 3, 2021, from Intersoft Consulting: <https://gdpr-info.eu/>
- FindLaw. *Suing for Emotional Distress at Work*. Retrieved December 10, 2021, from FindLaw | Learn About the Law | Accidents and Injuries | Torts and Personal Injuries: <https://www.findlaw.com/injury/torts-and-personal-injuries/suing-for-emotional-distress-at-work.html>
- Flory, S. M. (1976, August). *An Inquiry Into Selected Problems of Auditing Computer-Based Accounting Systems*. PhD Dissertation, Louisiana State University and Agricultural and Mechanical College, Graduate School | Department of Accounting. Retrieved November 16, 2021, from Louisiana State University | LSU Digital Commons: https://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=3962&context=gradschool_disstheses
- Gero, J. (2002, January REVIEWED WORKS: Gender and material culture in archaeological/historical perspectives by Donald & Hurcombe. *American Journal of Archaeology*, 106(1), 118–120. <https://doi.org/10.2307/507200>
- Gilbert Employment Law, P.C. (2020, August 31). *How Do I Know If I'm in a Hostile Work Environment?* Retrieved September 23, 2021, from Gilbert Employment Law | Employment Law Basics: <https://gelawyer.com/how-do-i-know-if-im-in-a-hostile-work-environment/>
- Hanks, G. (2018, April 29). *E-Business Ethical Issues on Selling Personal Information*. Retrieved September 20, 2021, from Small Business Chronicle: <https://smallbusiness.chron.com/ebusiness-ethical-issues-selling-personal-information-65718.html>

- Harvard University. (2021). *How do I check to see if I have the latest critical patches for my computer?* Retrieved September 15, 2021, from Harvard University | Student Computing Services | FAQs: <https://projects.iq.harvard.edu/student-computing-services/faq/how-do-i-check-see-if-i-have-latest-critical-patches-my-computer>
- Healy, P. M., & Palepu, K. G. (2003, April). The Fall of Enron. *Journal of Economic Perspectives*, 17(2), 3–26. <https://doi.org/10.1257/089533003765888403>
- HelpSystems. (2021). *How to Use Social Engineering Penetration Tests to Protect Against Phishing Attacks*. Retrieved September 21, 2021, from CORESECURITY | Blog: <https://www.coresecurity.com/blog/how-build-effective-phishes-social-engineering-penetration-tests>
- HelpSystems. (2021). *Penetration Testing*. Retrieved September 21, 2021, from CORESECURITY: <https://www.coresecurity.com/penetration-testing>
- HP Alumni Association. (2021). *The HP Way*. Retrieved from HP Alumni: <https://www.hp alumni.org/hp-way.htm>
- HP Computer Museum. (2021). *Portable 110*. Retrieved September 28, 2021, from HP Computer Museum | Business Desktops/Calcs: https://hpmuseum.net/display_item.php?hw=48
- Hsu, C.-C., & Sandford, B. A. (2007, August). The Delphi technique: making sense of consensus. *Practical Assessment, Research & Evaluation*, 12(10), 1–8. Retrieved September 28, 2021, from <https://scholarworks.umass.edu/pare/vol12/iss1/10/>
- IAPSC. (2020, February 4). *IAPSC Code of Ethics & Unacceptable Behavior Code of Conduct*. Retrieved September 27, 2021, from IAPSC | Code of Ethics: https://iapsc.org/site/assets/files/1071/iapsc_code_of_ethics_unacceptable_behavior.pdf
- Insureon. (2021). *Professional Negligence vs. Ordinary Negligence: Is Your Small Business at Risk?* Retrieved September 15, 2021, from Insureon Small Business Blog | Professional liability insurance: <https://www.insureon.com/blog/professional-negligence-vs-ordinary-negligence>
- International Association of Professional Security Consultants. (2021). *About the IAPSC*. Retrieved September 27, 2021, from IAPSC | About: <https://iapsc.org/about/>
- International Organization for Standardization/International Electrochemical Commission. (2017, March 18). *ISO/IEC 27001 family - Information security management systems*. Retrieved September 23, 2021, from ISO | Popular Standards: <https://www.iso.org/isoiec-27001-information-security.html>
- Kabay, M. E. (2004). *Computer-Aided Thematic Analysis: Narrated Slide Show*. Retrieved September 29, 2021, from M. E. Kabay | Methods: <http://www.mekabay.com/methodology/cata.ppt>
- Kabay, M. E. (2006, October 5). *CATA: Computer-Aided Thematic Analysis*. Retrieved December 8, 2021, from M. E. Kabay | Methodology: <http://www.mekabay.com/methodology/CATA.pdf>
- Kabay, M. E. (2006, Jun 20). *INFOSEC YEAR IN REVIEW*. Retrieved December 8, 2021, from M. E. Kabay: <http://www.mekabay.com/iyir/index.htm>
- Kabay, M. E. (2006). *Leadership Skills*. Retrieved September 24, 2021, from M. E. Kabay | Courses | Academic | MSIA: http://www.mekabay.com/courses/academic/norwich/msia/msia_s6_leadership_skills.pptx
- Kabay, M. E. (2006). *Management Skills*. Retrieved September 24, 2021, from M. E. Kabay | Courses | Academic | MSIA: http://www.mekabay.com/courses/academic/norwich/msia/msia_s6_management_skills.pptx
- Kabay, M. E. (2008). *Applying Social & Organizational Psychology*. Retrieved September 24, 2021, from M. E. Kabay | Courses | Academic | MSIA: http://www.mekabay.com/courses/academic/norwich/msia/msia_2008_organizational_psychology.pptx
- Kabay, M. E. (2009). *Computer-Aided Consensus | Notes*. Retrieved September 28, 2021, from M. E. Kabay | Methods: <http://www.mekabay.com/methodology/cac.pdf>
- Kabay, M. E. (2011, November 4). *Computer-Aided Consensus*. Retrieved September 23, 2021, from M. E. Kabay | Methodology: <http://www.mekabay.com/methodology/cac.pdf>
- Kabay, M. E. (2012, Jun 19). *Facilities Security-Audit Checklist*. Retrieved September 23, 2021, from M. E. Kabay | INFOSEC Management: http://www.mekabay.com/infosecgmt/facilities_checklist.pdf
- Kabay, M. E. (2020, September 24). *CS407: Politics of Cyberspace*. Retrieved December 8, 2021, from M. E. Kabay: <http://www.mekabay.com/courses/academic/norwich/cs407/index.htm>
- Kabay, M. E. (2020, December 5). *IA455 Contemporary Issues in Information Assurance*. Retrieved December 8, 2021, from M. E. Kabay: <http://www.mekabay.com/courses/academic/norwich/ia455/index.htm>
- Kaiser, J. (2006, March 17). Rule to protect records may doom long-term heart study. *Science*, 311(5767), 1547–1548. <https://doi.org/10.1126/science.311.5767.1547>
- KernelCare. (2021, March 14). *Ultimate Guide to Linux Patch Management*. Retrieved September 15, 2021, from KernelCare: <https://blog.kernelcare.com/the-ultimate-guide-to-linux-patch-management>
- Leeper, R. (2012). A study of a neglected portion of the field of learning - the development of sensory organization. *The Pedagogical Seminar and Journal of Genetic Psychology*, 46, 41–75. <https://doi.org/10.1080/08856559.1935.10533144>

- Mandler, G. (1967). Organization and Memory. (K. Spence, & J. T. Spence, Eds.) *Psychology of Learning and Motivation*, 1(1), 327–372. Retrieved September 29, 2021, from <https://www.elsevier.com/books/psychology-of-learning-and-motivation/spence/978-0-12-543301-3>
- Mandler, G., & Pearlstone, Z. (1966, April). Free and constrained concept learning and subsequent recall. *Journal of Verbal Learning and Verbal Behavior*, 5(2), 126–131. <https://www.sciencedirect.com/science/article/abs/pii/S0022537166800051>
- Manx Tech Group. (2019, January 7). *Internal Network Firewalls (INFW)*. Retrieved September 15, 2021, from mtg | Blog: <https://www.manxtechgroup.com/internal-network-firewalls-infw/>
- Miller, G. A. (1956, n/a n/a). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), 81–97. <https://doi.org/10.1037/h0043158>
- MindTools. *Brainstorming: Generating Many Radical, Creative Ideas*. Retrieved September 28, 2021, from MindTools | Creativity Tools | Brainstorming: <https://www.mindtools.com/brainstm.html>
- Moore, D. A., Tetlock, P. E., Tanlu, L., & Bazerman, M. H. (2006, January). Conflicts of interest and the case of auditor independence: moral seduction and strategic issue cycling. *Academic of Management Review*, 31(1), 10–29. <https://doi.org/10.2307/20159182>
- N-able. (2021, March 15). *Intrusion Detection System (IDS): Signature vs. Anomaly-Based*. Retrieved September 21, 2021, from N-ABLE | Engage | Blog | Security: <https://www.n-able.com/blog/intrusion-detection-system>
- National Institutes of Health. (2021). *NIH: Turning Discovery into Health*. Retrieved October 3, 2021, from U.S. Department of Health & Human Services | NIH: <https://www.nih.gov/>
- Neumann, P. (2023). *ACM RISKS Forum*. Retrieved August 27, 2023, from Association for Computing Machinery | About-ACM | Risks-Forum: <https://www.acm.org/about-acm/risks-forum>
- Nikolov, I. (2018, May 18). *Why An SSL Certificate Is Important for Your Company Website*. Retrieved September 20, 2021, from Forbes | Tech Council: <https://www.forbes.com/sites/forbestechcouncil/2018/05/18/why-an-ssl-certificate-is-important-for-your-company-website/>
- Norwich University. (2021). *Master of Science in Cybersecurity*. Retrieved September 24, 2021, from <https://online.norwich.edu/academic-programs/masters/cybersecurity>
- Open Web Application Security Project. (2021). *Testing for Browser Cache Weaknesses*. Retrieved September 20, 2021, from OWASP | Web Security Testing Guide (WSTG) | Latest | 4-Web Application Security Testing | 04-Authentication Testing: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses
- PaySimple. (2021). *6 Tips for Proper Handling of Credit Card Information*. Retrieved September 20, 2021, from PAYSIMPLE | Payments & Billing: <https://paysimple.com/blog/handling-customer-credit-card-information/>
- Premier IT Solution. (2020, February 17). *External IT Security Audit – What It Is and Why You Need One*. Retrieved September 23, 2021, from Premier IT Solution | Business Services: <https://premieritsolution.co.uk/external-it-security-audit/>
- RAND Corporation. (2021, September 22). *Delphi Method*. Retrieved September 28, 2021, from RAND | Topics: <https://www.rand.org/topics/delphi-method.html>
- Reichert, A. (2020, August 8). *Is QA Necessary, or Should Developers Do Their Own Testing?* Retrieved September 23, 2021, from TechBeacon | App Dev & Testing | Testing: <https://techbeacon.com/app-dev-testing/qa-necessary-or-should-developers-do-their-own-testing>
- Riesen, M. (2021). *Firewalls 101: 5 Things You Should Know*. Retrieved September 15, 2021, from SecurityMetrics | Blog Home | Cybersecurity: <https://www.securitymetrics.com/blog/firewalls-101-5-things-you-should-know>
- Sarà, M. (2021, February 9). *Sponge*. Retrieved September 24, 2021, from Britannica Encyclopedia: <https://www.britannica.com/animal/sponge-animal>
- Schneier, B. (2000, April). *The Process of Security*. Retrieved September 14, 2021, from Schneier on Security | Essays: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html
- Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World* (15th ed., Vol. 1). John Wiley & Sons, Inc. Retrieved December 8, 2021, from AMAZON: <https://smile.amazon.com/Secrets-Lies-Digital-Security-Networked/dp/1119092434/>
- Schneier, B. (2023, August 15). *Schneier on Security | Crypto-Gram Newsletter*. Retrieved August 27, 2023, from *Schneier.com*: <https://www.schneier.com/crypto-gram/>
- Science. (2021, September 14). *Science Magazine*. Retrieved September 14, 2021, from Science: <https://www.science.org/>
- Smail, D. L. (2007). *On Deep History and the Brain*. University of California Press. Retrieved September 24, 2021, from <https://www.amazon.com/gp/product/0520258126>

- Software Testing Help. (2021, September 17). *Top 10 BEST Intrusion Detection Systems (IDS) [2021 Rankings]*. Retrieved September 21, 2021, from Softwaretestinghelp: <https://www.softwaretestinghelp.com/intrusion-detection-systems/>
- Starcom. (2020, 01 30). *The Reason Behind 95% of Firewall Failures*. Retrieved September 15, 2021, from Starcom Blog: <https://starcom.node4.co.uk/firewall-failure/>
- Stockton, N. (2014, September 12). *What's Up with That: Why It's So Hard to Catch Your Own Typos*. Retrieved September 23, 2021, from WIRED | Science: <https://www.wired.com/2014/08/wuwt-typos/>
- Tennant, D. B. (2021). *How an American Company You're Too Young to Remember Used Hilarious Marketing to Become a Household Name & Sail Through the Great Depression*. Retrieved September 29, 2021, from NEILPATEL | Blog | Marketing: <https://neilpatel.com/blog/sail-through-the-depression/>
- Thibodeau, P. (2005, July 19). *Interex Founder Discusses Group's Demise, End of HP World*. Retrieved September 27, 2021, from NetworkWorld: <https://www.networkworld.com/article/2312694/interex-founder-discusses-group-s-demise-end-of-hp-world.html>
- U.S. Code. (1986, October 16). *18 U.S. Code § 1030 - Fraud and Related Activity in Connection With Computers*. Retrieved September 30, 2021, from Legal Information Institute | U.S. Code | Title 18 | Part I | Chapter 47: <https://www.law.cornell.edu/uscode/text/18/1030>
- U.S. Cybersecurity & Infrastructure Security Agency. (2021, August 20). *Top Routinely Exploited Vulnerabilities – Alert AA21-209A*. Retrieved September 15, 2021, from CISA | National Cyber Awareness System | Alerts: <https://us-cert.cisa.gov/ncas/alerts/aa21-209a>
- U.S. Department of Education. (2021). *Family Educational Rights and Privacy Act (FERPA) Family Educational Rights and Privacy Act (FERPA)*. Retrieved October 3, 2021, from U.S. Department of Education: <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- U.S. District Court for the Central District of California. (1975, December 8). *In the Matter of EQUITY FUNDING CORPORATION OF AMERICA...*. Retrieved November 16, 2021, from JUSTIA | US Law: <https://law.justia.com/cases/federal/district-courts/FSupp/416/132/1500698/>
- U.S. National Institute of Science and Technology. (2021, September 8). *National Vulnerability Database*. Retrieved September 15, 2021, from NIST | ITL | NVD <https://nvd.nist.gov/>
- U.S. Senate Select Committee on Ethics. *Conflicts of Interest*. Retrieved December 8, 2021, from U.S. Senate | Ethics | Topics | Basic Principles: <https://www.ethics.senate.gov/public/index.cfm/conflictsofinterest>
- U.S. Social Security Administration. (2021). *Social Security Number and Card*. Retrieved October 3, 2021, from SSA: <https://www.ssa.gov/ssnumber/>
- Weed. (2016, June 28). *Why Did the Chicken Cross the Road?* Retrieved September 4, 2023, from WUSSU | Humour | Chicken: <https://www.wussu.com/humour/chicken.htm>
- Whorf, B. L. (2012). *Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf* (2nd ed.). (J. B. Carroll, S. C. Levinson, & P. Lee, Eds.) MIT Press. Retrieved September 29, 2021, from <https://www.amazon.com/Language-Thought-Reality-Selected-Writings/dp/0262517752>
- Woodard, S. (2014, April 22). *Positive Reinforcement: Training With Praise and Rewards*. Retrieved September 30, 2021, from BestFriends Network Partners | Lifesaving Library: <https://network.best-friends.org/lifesaving-library/dog-resources/positive-reinforcement-training-praise-and-rewards>
- ZOOM. (2021). *Simplified Video Conferencing and Messaging Across Any Device*. Retrieved September 28, 2021, from ZOOM | Solutions: <https://explore.zoom.us/en/products/meetings/>

10 Employment

EMPLOYMENT PRACTICES AND POLICIES

There's nothing new in pointing out that people are the core of any organization. This section reviews practical advice for picking the right candidates for specific jobs and managing them so well that they become champions.

This chapter reviews

- Organizing employment procedures to hire candidates who will help secure our systems.
- Managing employees effectively for improved security.
- Policies for protecting privacy of customers, visitors, employees, and suppliers.
- How to terminate employment with minimal risks.



FIGURE 10.1 Managing the workforce.

How can we best use our investment in IS? As we all know after countless articles and seminars, we must

- Identify how information helps us attain our strategic objectives (e.g., for a car fleet servicing operation, this might be to provide the most timely and precise preventative maintenance schedules to individual corporate clients);
- Define our information processing methods accurately (e.g., requiring our computer system to bring up a customer's full dossier for a particular car within one second of entering its license plate number);
- Choose our computers and peripherals wisely (e.g., selecting a computer with the highest ratio of throughput to cost of ownership calculated over three years).

Although these are surely sound principles, they all assume that the people who operate our data centers will be competent and motivated to make the best use possible of our valuable systems. Good staff can make a success of IS operations even when budgets are less than optimal by courteous, sensitive, imaginative, and competent professionalism. For instance,

- An intelligent operator can notice and question anomalies such as jobs which read scratch tapes before writing to them (a security violation known as “scavenging”).
- A good quality control supervisor can catch and correct reports with illegible printing, find the corresponding spoolfile, and reprint the pages where the printer ribbon failed.
- A creative system manager can find workarounds to keep a mainframe running even if a bug in the operating system threatens to cause system failures.
- On the other hand, people can make mistakes with disastrous consequences, for example,
 - A bored, tired, drugged, or stupid operator can destroy magnetic tapes by simply mounting the wrong unlabeled tape on a tape unit – overwriting information quite possibly worth more than a decade of his or her salary.
 - A malicious system manager can make life hell for every programmer in the shop by insisting on following rules in emergencies even though the consequences of normal procedures are worse than the consequences of breaking the rules.

- A neurotic quality-control supervisor can offend everyone in the company – including the VP of finance – by snarling defensively at them on the phone whenever the system is slower than usual.

EVALUATING RESUMÉS

Hiring new employees poses a particular problem; growing evidence suggests that many job candidates inflate their resumés with unfounded claims:

According to recent surveys conducted by Checkster, more job applicants may be engaging in unethical behavior than you think. Checkster conducted two surveys: one with 400 hiring managers, recruiters, and HR employees and another with 400 individuals who had applied for or received job offers in the past six months. We asked about their opinions on a variety of ways to misrepresent themselves in the hiring process. These behaviors ranged from claiming a degree from a university they didn't attend to inflating their role on a project. The recruiters and hiring managers then reported their likelihood to hire an individual who had made one of these inflated claims, while the participants in the applicant survey reported whether they had or would consider making these claims in their own job search.

The applicant survey revealed alarming widespread willingness to misrepresent information during the hiring process. Across a list of inflated claims in the job application process, 40% of individuals reported that they would or had engaged in each behavior on average. Applicants were most likely to report claiming mastery in skills they had no knowledge of (60% claimed they had or would do this at least once) and working at some jobs longer than they had in order to omit an employer (over 50%)—that's a majority of respondents reporting willingness to misrepresent in these ways.¹

Be especially careful of vague words such as “monitored,” and “initiated” in the resumé – find out what the candidate did in specific detail, if possible. Be sure that references are followed up at least to verify that the candidate really worked where the resume claims they did.

Unfortunately, there is a civil-liberties problem when considering someone's criminal record. Once someone has suffered the legally mandated punishment for a crime (fines, community service, imprisonment), discriminating against them in hiring may be a violation of their civil rights in many jurisdictions.²

- Can you exclude convicted felons from any job openings?
- Can you exclude candidates from job openings similar to areas in which they abused their former employers' trust?
- Are you permitted by applicable law to require that prospective employees approve of background checks?
- Can you legally require polygraph tests?
- What about drug tests?

You must consult your corporate legal staff to ensure that you know your rights and obligations in your specific legal context and are not violating any laws that protect the candidates.

Even checking references from previous employers is fraught with uncertainty. Employers may hesitate to give bad references even for incompetent or unethical employees³ for fear of lawsuits⁴ if their comments become known or even if the employee fails to get a new job. Today, you can't even be sure you'll get an answer to the simple question, “Would you rehire this employee?”

Ex-employers must also be careful not to inflate their evaluation of an ex-employee. Sterling praise for a scoundrel could lead to a lawsuit from the disgruntled new employer.⁵



FIGURE 10.2 Hiring.

For these reasons, a growing number of employers have corporate policies which forbid discussing a former employee's performance in any way, positive or negative.⁶ All you'll get from your contact in such cases is, "Your candidate did work as an Engineer Class 3 from 2019 to 2021. I am forbidden to provide any further information."

It is a commonplace in the security field that some people who have successfully carried out crimes have been rewarded by a *golden handshake*⁷ (a special payment in return for leaving) and even positive references in return for a non-disclosure agreement to prevent embarrassment. The criminals can then move on to victimize a new employer. For the same reasons that we cannot know exactly how many crimes are carried out, we can't tell how often this extortion takes place.

To work around such distortions, question the candidate closely about details of their education and work experience. The answers can then be checked for internal consistency and compared with the candidate's written submissions. Liars hate details: it's so much harder to remember which lie to repeat to which person than it is to repeat the truth. Ask experienced employees to interview the candidate.

Before allowing new employees to start work, they should sign an employment agreement which stipulates at the very least that they will not disclose confidential information or trade secrets from their previous employer nor reveal confidential employment from their new employer at any time. Another clause must state that they understand that you are explicitly refusing to receive information misappropriated from a previous employer or stolen from any other source.⁸ (In the United States, the *Uniform Trade Secrets Act* (UTSA) explicitly defines and regulates traffic in valuable secret information.⁹) Every employment contract for every new hire must be approved by the employer's corporate counsel.

SELECTING GOOD CANDIDATES FOR IT

One might think that data-center operations must involve primarily relationships with machines. On the contrary, all of my experiences as a data-center operations manager and consultant convince me that personality is the key to long-term success in computer operations. Personality implies, in the words of a dictionary,

...[T]he complex of characteristics that distinguishes an individual or a nation or group; *esp*: the totality of an individual's behavioral and emotional characteristics.¹⁰

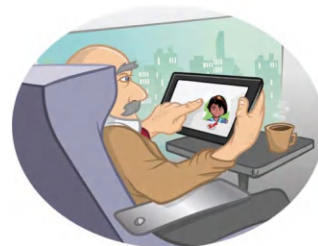


FIGURE 10.3 Selection.

Operations staff are mediators between large computer systems and their users; therefore, a large part of their work must involve contact with human beings. Personality informs not only how we approach all aspects of our work with computers, it is the fundamental basis of all human interaction as well.

It is a commonplace that differences of upbringing, socio-economic status and culture can cause misunderstandings; what is business-like in one milieu is considered brusque in another, and conversely what is friendly in a second may be considered inefficient in the first.¹¹

Social differences are superimposed on a base of personality and individual development; it should not surprise us, then, that personality is a major factor in how well we run our data centers operations.

So what kinds of personality traits can be particularly helpful in the business of running an IS operation?

Look for candidates who

- Focus on the overall goals of their organization rather than looking only to the short-term, here-and-now demands of filling the requirements of a job description. For example, if a system manager often sees accounting employees laboriously re-entering data from a printed

report into a microcomputer spreadsheet, she should suggest to upper management that they either authorize a change in the printed report to meet the obvious needs of the accounting department or provide support for evaluating, buying, and installing a package to select and download data from mainframe DBs, files or reports to microcomputer packages.

- Can suspend rules when faced with unusual situations. For example, if a user is desperately waiting for a major report, there's a bug in the program, and the programmer wants to run a compilation in high priority, it would be inappropriate for a system manager to refuse to even consider the request because of rules forcing compiles into the batch processing queues.
- Want to improve their methods. For example, an employee might see an opportunity to create an online system documentation system rather than continuing to use outdated paper copies.
- Help other people accomplish their goals by sharing knowledge. Such a shift supervisor might, for example, respond to a junior operator's interest in how a tape drive works by showing her the appropriate section in a reference manual and encouraging further questions.

The above traits are not guarantees of excellence; they are merely my impression of what seems to help people work effectively in operations.

A final note on racism, sexism, hostility to LGBTQIA people, and other forms of bigotry: make sure that all managers involved in selecting candidates are *not* being influenced by prejudice. For example, many governments have passed and enforce anti-discrimination laws that preclude rejecting candidates on the basis of "race," sex, gender-identity, age, marital status or religion. Provide detailed instructions to those making employment decisions; check the legal frameworks in effect for all the locations in your organization. For example, the U.S. Federal Trade Commission has explicit prohibitions against many forms of discrimination in the workplace.¹²

AVOIDING BAD CANDIDATES

The other side of the hiring question is whom to avoid.

Avoid hiring people with counter-productive personality traits, many of which were identified as part of the "authoritarian personality" in the late 1940s and early 1950s by social psychologists such as Theodore W. Adorno and Gordon W. Allport.¹³ Beware of those who are

- Process-oriented rather than goal-oriented. Such people often fear the unknown so much they'd rather follow accepted procedures even when conditions are inappropriate than risk the consequences of breaking the rules or parting with precedent.
- Intolerant of ambiguity. That is, people who can't say or accept that someone else could reasonably say, "I don't know" are likely to cause problems in data-center operations. They will waste time and effort either denying the possibility of alternatives or criticizing colleagues for asking for more information.
- Judgmental (quick to attribute blame or to devalue a person after a disagreement). This trait leads to grudges and resentments which can poison not only the individual's relations with others, but which may also contaminate the atmosphere for the whole work group.
- Excessively sensitive to structural power (e.g., those who flatter their "superiors" and harass their "inferiors" in a hierarchy). A supervisor who glories in finding fault with his employees causes poor performance and higher turnover. One who humiliates her employees in public is asking for sabotage. By the same token, employees who dare not question their supervisor's decisions when they disagree with them are partly responsible for "group-think." Organizations in which dissent is punished are missing the full value of the salaries they pay – the insights available from the range of perspectives and knowledge of their employees.



FIGURE 10.4 Bad candidate.

- Apt to form excessively strong in-group affiliations (e.g., those who tend to make us/them distinctions readily and refer to out-groups in derogatory terms such as “those dumb users”). A sense of teamwork and pride in excellence is laudable; but beware the potential employee who speaks disparagingly about the worthlessness of other groups. Such people may respond automatically to suggestions with “not invented here” (meaning that if the idea were any good, someone in their group would have thought of it by now).
- Likely to follow charismatic leaders and apt to confuse personality, reputation, or authority with infallibility (e.g., members of doctrinaire cults and racial-supremacy movements).
- Prejudiced (form judgments about individuals based on membership in identifiable groups or on external appearance instead of based on behavior or performance).

Many fine operations staff members show *some* of the traits above, and no one should be rejected simply because they show a few of the problems listed above. In any case, people may show this undesirable behavior because of troubles they have experienced in their childhood and youth. Psychologists tell us that rigid, authoritarian behavior is often a response to insecurity. At the root of this insecurity is a feeling of inadequacy – sometimes the fear of falling short of displeasing an all-powerful parent. Many people have been traumatized by their experiences in schools, where some teachers unfortunately humiliate some children for making mistakes; sadly, these children come to believe that authority figures hold all the answers, and that there’s something wrong in not knowing those answers. Such people can be helped by various kinds of therapy to become aware of their fears, face them, and rebuild their self-esteem and confidence.

Everyone with access to organizational information must be trustworthy; furthermore, it makes sense to put extra care into the hiring process for all employees such as operators, technical support personnel, programmers, managers, and security officers: they will be involved in supporting mission-critical systems.

A degree of background checking is appropriate, but one must respect applicable laws against discrimination in hiring. With the permission of the candidate, one can look for criminal records, and credit records as well as verifying claims of educational attainment and professional experience. Don’t expect former employers to reveal much detail about the candidate beyond the dates of her employment; organizations are now highly sensitive to the risk of violating privacy laws or of stumbling into lawsuits for defamation.

During the hiring process, successful candidates must be thoroughly briefed on corporate policies such as non-disclosure agreements for intellectual property, compliance with all regulations, and penalties for non-compliance. Some organizations have found it helpful to have a simple examination (usually automated) for the candidate to demonstrate knowledge of applicable policies once they’ve completed the overview.

A technique I used in my own work as *Director of Technical Services* at a company in the mid-1980s was to have candidates who passed my initial interview spend time with the staff with whom they would be working. I recall one candidate who claimed to have worked on the HP3000 for several years – but my staff reported that he did not know how to log on to the MPE system. Ironically, had he told the truth, he might have been hired anyway because we were prepared to provide full training on our systems to good candidates.

ESSENTIAL SKILLS

What are the essential skills we should look for in our potential operations employees? Some of the most critical are the ability to

- Comprehend technical information quickly from text and from discussion
- To notice anomalies (e.g., “Why is this job taking 20 times longer than ever before?”);



FIGURE 10.5 Skills.

- Question outliers (unusual or extreme cases, e.g., “Why is this program taking 20 times more CPU than the next most intensive program?”)
- Keep detailed records (e.g., “Just before the system failure, I typed a file equation and misspelled the device class name.”)
- Break down problems into operational questions (e.g., “The bizarre characters on screen could be due to the terminal, the cable between the terminal and the modem, the modem, the phone lines, the ... [etc. through the data communications chain] ... or finally, the software”)
- Formulate models (hypotheses) that can be falsified (e.g., “If the problem resides in the terminal, then switching the terminal to another data communications channel will leave the problem on the terminal”)
- Remain free of ego-involvement in problem solution, allowing the person to discard an hypothesis without resistance once it’s disproved (e.g., “Oh, it’s not that, then. So much for that theory. Now, the next idea is....”)
- Adapt to different operating environments (e.g., mainframe vs mini vs micro)
- Capable of switching quickly among different tools and appreciating their different strengths and weaknesses without complaint or resistance; for example, command sets, fourth-generation languages vs third-generation languages, and different editors or debuggers

On the last point, I recall an astounding case of resistance to progress from my days managing technical services in the 1980s. In one of my regular system-performance analyses, I found that one particular programmer – let’s call him “Jacques” – had reports which consistently consumed an order of magnitude more CPU system resources than any other set of routines. I examined his source code, which was in a new *fourth-generation language* (4GL) but did not use the 4GL’s commands for printing. Instead of letting the 4GL handle the automatic alignment of headings and detail lines in reports, Jacques was bypassing the 4GL and coding every detail of the placement of each column in detailed routines. When I asked him why he was doing that, he answered that it was how he had been writing COBOL for decades. I politely informed him that if he continued ignoring the features of the 4GL, I would have him fired. He changed his style right away.

ACADEMIC BACKGROUND

For some people, computer skills seem almost independent of academic training. Some expert TS and SM staff have little or no formal training in computer science – they taught themselves. One should evaluate the candidate’s current skills rather than paying overmuch attention to theoretical implications of academic background. However, other factors being equal, one might favor different academic disciplines in order of preference as, for example,

computer science > engineering > science > general arts

However, it would be a mistake to refuse a good candidate merely on the grounds that they had completed a university degree in a “soft” subject (e.g., psychology, anthropology, literature, or art). Clear thinking and self-discipline are not the exclusive properties of people from the “hard” sciences. Research consistently shows a wide variety of options available for success in information-technology careers, with some form of bachelor’s degree most widely found among respondents.¹⁴

On the other hand, there are many well-respected programs in computing¹⁵ and IA.¹⁶ Graduates from such programs deserve particular attention so that their potential employers can benefit from their intelligence and knowledge. Students with graduate degrees in these subjects can bring detailed knowledge to bear on important issues; potential employers should discuss these candidates’ research with them during the hiring interviews.



FIGURE 10.6
Academics.

JOB EXPERIENCE

Ideally, one should look for experienced operations staff to fill senior positions. In contrast, lower levels such as operators can be hired with less experience because their required skill set is less complex, and the learning curve is much shorter than for management skills.

In particular, the operations manager should have a direct knowledge of technical support or operations, not just programming management. Managing operations is distinctly different from managing programming:

- Operations-planning timescales are longer than programming timescales. Programmers have control over their implementation schedules (to the extent that development is on time) but operations have to take into account long-term capacity planning (usually measured in years) and hardware- and software-acquisition lead times (usually measured in months).
- Operations problem-solving timescales are shorter than programming timescales. Operations problems arise hour by hour; interruptions arise minute by minute.
- Operations staff must handle multiple problems at the same time because there are usually tests to be run or actions to be taken in sequence during problem solution. Programmers usually work on one program or system at a time because it doesn't usually make sense to interrupt programming to do a bit on another program.
- Operations must adopt a global view of the entire system or network; they cannot benefit only one user group at the expense of another. Programmers must make their own client community's needs paramount.



FIGURE 10.7 Résumé.

ADMINISTRATION AND PRODUCTION

Another distinction to consider when evaluating a candidate's job experience is the contrast between the *administrative manager* and the *line manager* (someone responsible for some kind of production). Administrators who have not experienced the joys and terrors of having 800 users waiting for the system to come back up after a failure cannot reasonably be expected to empathize with operations staff's typical emphasis on getting the job done instead of worrying about what the procedures should be. The temperamental differences between career administrators and career problem-solvers only complicate the task of managing operations. An administratively oriented manager may conflict with technically oriented staff:



FIGURE 10.8 Problem-solvers.

- Administrative managers may emphasize building an administrative staff within operations because paper-pushing is inherently more comfortable for them to manage than technical demands; technical managers will push for adequate staffing of problem-solvers and problem-preventers.
- Administrative managers may de-emphasize contacts with technical personnel because of insecurity about the technical concepts and vocabulary used in discussing their operations

staff's needs; technical managers will relish the chance for nuts-and-bolts discussions of options and solutions.

PROBATION? PROBABLY NOT

In discussions of employee management and security, some key areas of concern are hiring and firing. However, ongoing management also provides challenges to IA; for example, how should IA professionals handle proposals to offer an employee a *probationary period*?

There are two kinds of probationary period:

- At the start of employment designed to evaluate a new employee's skills and decide on permanent employment.
- Following a serious problem, possibly leading to termination of employment if the problem or its equivalent recurs.

Both types of probation raise problems for IA.

In the preliminary probationary period, the candidate's employment is contingent on approval. When assigning access privileges to such a candidate, security staff should evaluate managers' natural desire for productivity but weigh the benefits of thoroughgoing access against the possibility that the employee will soon disappear.

As for probation for the error-prone or the lazy, I can accept the idea of a probationary period for under-performing employees who may be making too many mistakes or who need a kick in the pants to be motivated for better performance. However, a probationary period for an untrustworthy employee who has given cause to worry about security violations is far more problematic.

When would it make sense to allow an employee who violates clearly stated security policies to be put on probation? There's certainly nothing wrong with correcting someone's behavior using advice, criticism or even reprimands if appropriate and there's nothing wrong with providing a period of reevaluation for employees who are not directly involved in high-security work.¹⁷

What doesn't make sense to me, though, is telling someone who has committed such a serious violation of security that they *should* be fired, "Well, we won't fire you right now: we'll give you <period> and fire you at the end of that <period> if we don't like your behavior." If someone is not worthy of trust, why would you give them access to sensitive and critical resources at all, let alone do so while putting them on notice that they may lose their job soon?

I recommend that probation for employees you don't trust simply not be an option. Either express your support and trust in your employees or fire them right away if they no longer merit your confidence in their honesty.

USING COLLEGE STUDENTS AS SECURITY STAFF

I received the following interesting letter in 2003 from a reader of my newsletter who kindly permitted me to quote it in a subsequent column:

I work for one of the largest cities in the U.S. Due to the tightness of the budget, there is a plan to use computer science student interns to setup and manage the network security for various city agencies. Most of these agencies do not currently have the expertise or resources to dedicate to security.

I feel that it is a very bad idea for many reasons. There will be no oversight of the intern's work. Moreover, it doesn't help the agencies become any more security-savvy when the internship ends. I am also uncomfortable



FIGURE 10.9 Probation.



FIGURE 10.10 Students.

with the idea that the age bracket that is most common to hack is the same as most of these college interns. So, while the interns will have the knowledge to tighten security, this knowledge could also be used to leave/create backdoors that will be hard to find. I guess I am concerned about their lack of vested interest in the agencies and the lack of possible accountability. Am I out of line?

I would like the city to think of all of the consequences of this proposal before it goes into affect. I sense it could have the potential to be PR and security catastrophe.

I responded that the reader's concerns were reasonable. In addition, I wrote, I'd add to the memo that the system *could* work and be a wonderful opportunity for both the students and the city if

- The students were vetted using detailed phone conversations with their academic references.
- Each candidate was interviewed to discuss their attitudes toward hacking and to evaluate their maturity.
- They wrote logs and prepare weekly reports on their findings and their actions so that others can learn from them.
- They provided teaching sessions at the end of their projects where they summarized the lessons learned and left a permanent record of their work.
- The students were supervised by their college professors in weekly status meetings.
- Clear policies were in place on acceptable use of city resources.
- All the students understood to whom they were reporting in their work so that there would be no confusion about lines of responsibility.
- All the permanent staff understood to whom the students were reporting for the same reason as the previous point.

As a university-professor myself, I think that internships are a wonderful way for both the employer and the students to learn; in addition, the students' reports can serve as case studies (with suitable masking of sensitive information) for lectures by the students and as fresh material for professor's lectures.

My own experience with many university students interested in security is that they are committed to genuine security, not to childish hacking games. The criminal hackers either don't have the discipline to excel in university studies or they are very good at fooling their professors into believing that they're not criminal hackers.

Finally, I note that the *National Initiative for Cybersecurity Careers and Studies* (NICCS) cybersecurity scholarship programs, in which Norwich students have particularly distinguished themselves by winning an unusually high number of seats, include internships in government departments:

CyberCorps®: Scholarship for Service (SFS) is a unique program designed to recruit and train the next generation of information technology professionals, industrial control system cybersecurity professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

The program provides scholarships through qualified institutions of higher education to students who are enrolled in cybersecurity degree programs or cybersecurity-related fields, including artificial intelligence, quantum computing, and aerospace. Students identified by their institutions for SFS Scholarships must meet selection criteria based on prior academic performance, likelihood of success in obtaining the degree, and suitability for government employment. Upon graduation, scholarship recipients are required to work a period equal to the length of their scholarship in federal, state, local or tribal Government or in other approved organizations as cybersecurity professionals. Scholarships include tuition, stipend, professional allowance stipend (travel for job fair) and up to three years of support. To date, over five thousand students have received scholarships and committed to work for government organizations across the country.¹⁸

Clearly somebody thinks that college students can be a real security asset!

POLY WANT A HACKER?

When I was updating the chapter on employment policies for improving security in the *Computer Security Handbook*,¹⁹ I decided to include some information about the use of polygraphs as a tool for screening applicants and employees.

According to the *Frequently Asked Questions* (FAQ)²⁰ pages of the *American Polygraph Association*, a polygraph is a device which records a number of physiological markers such as respiration, heart rate, blood pressure, and galvanic skin response (sweating). Used by trained professionals, the device displays a chart of subject responses to questioning by law enforcement agents, attorneys involved in both civil and criminal legal procedures, and employers (subject to legal restrictions).

A comprehensive report about the use and abuse of polygraph testing was published in 2003, when the *Committee to Review the Scientific Evidence on the Polygraph*, a group organized by the *National Research Council of the US National Academy of Sciences*, published a scholarly report entitled *The Polygraph and Lie Detection*, which I am referring to as the “NAS Report.” The approach to detecting deception using physiological markers dates back to research in the late 19th century. Unfortunately, the scientific basis for such analysis is weak:

A solid theoretical base is necessary to have confidence in tests for the psychophysiological detection of deception, particularly for security screening. This is the case, as we have noted, because theory suggests that polygraph tests may give systematically erroneous results in certain situations and with certain populations (e.g., expectancy and stigma effects); because purely empirical assessment of the accuracy of test procedures cannot be conducted in important target populations such as spies and terrorists; and because of the need to have tests that are robust against a variety of countermeasures, some of them unanticipated. A research effort appropriate to these challenges would have been characterized by a set of research programs, each of which would have attempted to build and test a theoretical base and to develop an associated set of empirically supported measures and procedures that could guide research and practice. It would have focused on the psychophysiology and neuroscience of deception and sought the best physiological indicators of deception and the best ways to measure each one.

There are a few research programs that exhibit some of these characteristics. However, for the most part, polygraph research has focused on a few physiological responses for which measures have been available since at least the 1920s and tried to make the best of them by testing variations of them in practice, without doing much to develop the underlying science. The research has tended to focus on the application without advancing the basic science. In recent years, the same sort of approach has been tried with newer measures (see [Chapter 6](#)). There has been no systematic effort to identify the best potential physiological indicators on theoretical grounds or to update theory on the basis of emerging knowledge in psychology or physiology.²¹

Nonetheless, a wide range of studies confirms that polygraph results can *help* to evaluate the trustworthiness of the people being examined for positions in law enforcement or government offices:

Preemployment Test Accuracy – To date, there has been only a limited number of research projects on the accuracy of polygraph testing in the pre-employment context, primarily because of the difficulty in establishing ground truth. However, since the same physiological measures are recorded and the same basic psychological principles may apply in both the specific issue and pre-employment examinations, there is no reason to believe that there is a substantial decrease in the accuracy rate for the preemployment circumstance. The few studies that have been conducted on pre-employment testing support this contention.

While the polygraph technique is not infallible, research clearly indicates that when administered by a competent examiner, the polygraph test is one of the most accurate means available to determine truth and deception.²²



FIGURE 10.11
Polygraphs.

A report dated September 2006 on “Use of Polygraph Examinations in the Department of Justice” from the *Office of the Inspector General of the U.S. Department of Justice* stated that

During fiscal years (FY) 2002 through 2005, Department components conducted over 49,000 polygraph examinations. The examinations were used for a variety of reasons, including making pre-employment and personnel security decisions; investigating criminal, administrative, and security violations; ensuring witness security; providing sex offender treatment; and providing operational support in examining or ‘vetting’ foreign task force members and validating intelligence sources.²³

One of the most controversial applications of the polygraph is in pre-employment screening. Such applications are generally forbidden under U.S. law for private employers under the *Employee Polygraph Protection Act of 1988* (29 USC § 2001)²⁴ and the *Rights and Protections under the Employee Polygraph Protection Act of 1988* (3 USC § 414).²⁵

However, security officers in public employers (government agencies, police forces) who are trying to strengthen pre-employment screening to improve security for their organizations in collaboration with their HR teams should be cautious about recommending polygraph examinations as a *primary* or *standalone* criterion for accepting or rejecting candidates (the emphasis in this warning is critically important).

The *American Polygraph Association* quoted the “Model Policy for Law Enforcement Pre-Employment Polygraph Screening Examinations” to warn against depending solely on polygraph results in pre-employment research:

As with any polygraph examination, law enforcement pre-employment polygraph examinations do not take the place of an investigation. Instead, the pre-employment polygraph is used to enhance the background process. A thorough background investigation should always be conducted in conjunction with the pre-employment polygraph examination.... The decision to hire, or not to hire an applicant, should never be based solely on the results of the polygraph examination.²⁶

SURFING BRAIN WAVES: FMRI FOR LIE DETECTION

A new technology for telling truth from fiction is *functional magnetic resonance imaging* (fMRI).

fMRI is yet another development in the evolving study of brain function. Martha J. Farah and Paul Root Wolpe have an excellent overview of these technologies in their article, “Monitoring and Manipulating Brain Function: New Neuroscience Technologies and Their Ethical Implications” from the *Hastings Center Report* (May–June 2004, pp. 35–45). Using strong external magnetic fields, fMRI systems measure blood flow – and thus the level of neuronal activity – with a resolution of a millimeter or less and a response time of about 1 second.²⁷

One interesting application of fMRI has been to identify patterns of brain activity associated with truthful statements compared with lies. Early results were inconclusive: “Specific brain regions were activated during deception, but the present technique lacks good predictive power for individuals.”²⁸

Reporting on later research, reporter Beth W. Orenstein wrote, “The fMRI study found that when the subjects were telling lies, more areas of their brains activated than when they were being truthful.”²⁹ She quoted the researcher’s summary: “Indeed, what we found was that approximately twice as many areas of the brain—14 vs. seven—are activated when one is lying as compared to when one is telling the truth.”

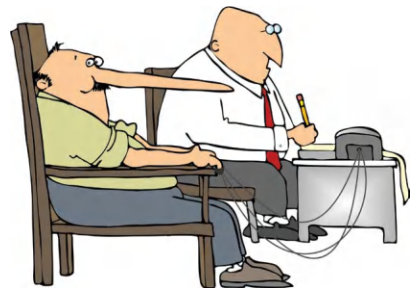


FIGURE 10.12 fMRI.

Steve Silberman describes his experiences being scanned using fMRI and discusses some of the growing controversy about the ethical implications of equipment that scans brain activity in the service of the state:

So what began as a neurological inquiry into why kids with ADHD blurt out embarrassing truths may end up forcing the legal system to define more clearly the inviolable boundaries of the self.

“My concern is precisely with the civil and commercial uses of fMRI lie detection,” says ethicist Paul Root Wolpe. “When this technology is available on the market, it will be in places like Guantanamo Bay and Abu Ghraib in a heartbeat.

“Once people begin to think that police can look right into their brains and tell whether they’re lying,” he adds, “it’s going to be *1984* in their minds, and there could be a significant backlash. The goal of detecting deception requires far more public scrutiny than it has had up until now. As a society, we need to have a very serious conversation about this.”³⁰

At a symposium entitled “Will brain imaging be lie detector test of the future?” held at *Harvard University* in February 2007, several participants expressed skepticism about fMRI’s applicability and reliability. For example, critics pointed out that some of the studies of reliability failed to use realistic scenarios involving stressful situations; they also ignored well-established “countermeasures for defeating the fMRI, like performing mental arithmetic – or simply fidgeting....” Participants also commented that:

Science also has no commonly accepted theory of how blood flow in the brain relates to deception... and fMRI studies so far do not reflect the complications and anxieties of real-life crime and criminals.

Among those complications - not considered in current fMRI/deception studies - is substance abuse. In the top 50 U.S. cities, 55 percent to 95 percent of all those arrested for felonies test positive for drugs or alcohol, a fact that would confound any fMRI, said lawyer and psychologist Stephen J. Morse J.D. ‘70, Ph.D. ‘73, a professor of law at the *University of Pennsylvania*.

Any new lie detection technology must have both good science and legal relevance, he said - and so far the fMRI fails on both counts. An fMRI could someday have “weight” in court, said Morse, but not admissibility.³¹

No Lie MRI, Inc. offered fMRI lie-detection services; their overview pages offered a number of interesting details, including this list of restrictions:

Currently the only known limitations to the technology developed by No Lie MRI are:

- Individuals cannot have metal inside their body.
- Individuals cannot be claustrophobic.
- Individuals cannot be brain damaged.
- Individuals cannot move around during the MRI scanning process³²

Recent reports continue to cast doubt on the reliability of fMRI for detecting lies, for example,

In the new study, participants were asked to conceal information about a ‘secret’ digit they saw inside an envelope.

Researchers taught 20 participants two mental countermeasures. The first was to associate meaningful memories to the control items, making them more significant. The second was to focus on the superficial aspects of the item they were trying to conceal, rather than on the experience of familiarity it evokes, in order to make it less significant.

The results showed that these countermeasures lowered the accuracy of the test by about 20% because it was more difficult for fMRI to find any differences in brain activity. Thus, participants were more likely to be able to hide their concealed information item when using the mental countermeasures.

The research team concluded that in order to improve the robustness of the test, future work needed to identify a way of detecting mental countermeasures, and potentially look at conducting whole-brain analyses, rather than just examining regions of interest.

Lead author Dr Chun-Wei Hsu, a researcher in the CogNovo research programme at the University of Plymouth, said: “fMRI tests are not currently used by law enforcement in the same way as polygraph tests, but they have been considered for scientific and criminal use as a way of detecting when someone is concealing information. This study shows that the process can be manipulated if someone associates meaningful memories to the control items, or focuses on the aesthetics, rather than the memory, of the item they’re trying to hide.

None of our participants were seasoned liars or criminals, they were just everyday people, so before this test can even be considered for forensic use, there must be further studies carried out to help identify when someone is using mental countermeasures.

Deception is a really challenging area of psychology, and the more we can find out about the techniques used to detect it, the better.³³

Security practitioners will want to continue monitoring (no pun intended) developments in fMRI to see if the technology can provide useful, reliable indications of truthfulness and deception in our hiring and in investigations.

SUMMARY OF HIRING ISSUES

Staff selection makes a big difference to the success of a data center. Operations staff have direct responsibility for the availability of computer services; nonetheless, they also have direct contact with users and decision makers. Personality plays a major role in how well our staff interact with our users. Candidates should focus on overall goals, be flexible about applying rules, and enjoy sharing knowledge. Avoid those who are process-oriented rather than goal-oriented, intolerant of ambiguity, judgmental, excessively sensitive to structural power, apt to form excessively strong in-group affiliations, prejudiced, and likely to follow charismatic leaders.

Some of the essential skills for operations staff include an ability to assimilate information quickly, meticulous attention to detail, penchant for analysis, and flexibility.

Academic background should not be the sole determinant of candidate selection.

Experience in operations, as distinct from programming, is highly desirable because of the differences in planning and problem-solving timescales, and the global view required for operations. Another useful background is line management, which can help operations managers handle the technical demands of support and planning.

EMPLOYEE MANAGEMENT

One of the key attributes of successful security officers is the ability to assume an attitude of paranoia. You don’t have to *be* paranoid: You just have to be able to *act* paranoid when it’s appropriate.

Analyzing how employees might abuse security systems and regulations is a constructive exercise in critical thinking. Security teams can benefit from exercises in thinking through how abuses could be carried out, how to respond, and how to improve processes to reduce risk. The



FIGURE 10.13 Summary.



FIGURE 10.14 Paranoia on demand.

organization should foster a belief in *continuous process improvement* (CPI),³⁴ with suggestions for improvement welcomed, not criticized, and perhaps even rewarded.

In one of my client sites, a factory, I remember seeing a poster that showed one of the employees with a big check – literally big: It was a meter wide – made out for C\$25,000. That amount (even more impressive in 1983 than today) was *10% of the savings* the employee had fostered in the first year of application of a suggestion for modifications in the production environment. I was told how much that program for CPI was appreciated by the employees.

Another critical tool in training employees is how to respond to attempted collusion. An employee can practice dealing with such an uncomfortable situation in training sessions to get used to the idea that the first response should be to appear interested; the second is to report the attempted collusion to management so they can decide on appropriate actions (e.g., create a sting operation, record interactions with the criminal, and contact law enforcement).

REDUNDANCY

For most areas of information processing, redundancy is generally viewed as either a Bad Thing or an unavoidable but regrettable cost paid for specific advantages. For example, in a DB, indexing may require identical fields (items, columns) to be placed in separate files (datasets, tables) for links (views, joins) to be established. However, in managing personnel for better security, redundancy is a requirement. Without shared knowledge, our organization is a constant risk of a breach of availability.

Redundancy in this context means having more than one person who can accomplish a given task. Another way of looking at it is that *no operationally significant knowledge shall belong to only one person in an organization*.

Unique resources always put our systems at risk; that's why companies like *Tandem* (now part of HP), *Stratus Technologies* and others have so successfully provided computer systems for critical-task functions such as stock exchanges and banking networks. Such redundant or *fault-tolerant* computer systems^{35,36} and networks have multiple parallel processors, channels, memory arrays, disk drives, and controllers. Disk mirroring (RAID 1) reduces the likelihood of data loss due to mechanical failures.

Similarly, a fault-tolerant organization will invest in cross-training of all its personnel. Every task should have at least one other person who knows how to do it – even if less well than the primary resource. This principle does not imply that you have to create clones of all your employees; it is in fact preferable to have several people who can accomplish various parts of any one person's job. Spreading knowledge throughout the organization makes it possible to reduce the damage caused by absence or unavailability of key people and also support CPI.

If only one employee is the only person who knows about a critical function in your organization, you are at risk. Your organization will suffer if the key person is away, and it may suffer if the key person decides to behave in unauthorized and harmful ways. Do you have anyone in your shop whose absence you dread? Are there any critical yet undocumented procedures for which everyone has to go ask Joe?

A client in a data-center operations-management class volunteered the following story.

There was a programming wizard responsible for maintaining a key production program; unfortunately, he had poor communication skills and preferred to solve problems himself rather than training and involving his colleagues. "It'll be faster for me to do it myself," he used to say. During one of his rare vacations, something went wrong with "his" production program, shutting down the company's operations. The wizard was in the north woods, out of reach of all modern communications; the disaster lasted for a week until he returned.



FIGURE 10.15 Sharing knowledge and skills.

Not only does your organization suffer, but also Mr/Ms Indispensable suffers from the imbalance of knowledge and skill when no one else knows what they know. Some indispensable are dedicated to the welfare of their employer and of their colleagues. They may hesitate to take holidays. If their skills are needed from hour to hour, it becomes more difficult to allow them to participate in committee meetings. These are the people who wear beepers and cannot sit undisturbed even in a two-hour class. If the Indispensable's skills affect day-to-day operations, they may find it hard to go to offsite training courses, conferences, and conventions. Despite their suitability for promotion, indispensable people may be delayed in their career change because the organization finds it difficult or expensive to train their replacement. In extreme cases, the newly promoted manager may find themselves continuing to perform specialized duties that ought to be done by their staff. I remember my amazement when the newly promoted VP of IS at a service bureau informed me that he was the only person on the technical support and operations team who was competent to reconfigure the mainframe computer.

There was a horrible example of the consequences of violating this principle in a case I was involved in the mid-1990s. A network administrator for the three offices of a law firm was increasingly erratic in his behavior – and we consultants had to meet offsite with the firm's managers because there was reason to believe that he was reading all the email of the executives! He was the only person who knew the root-access password, and he had never documented it in a way that his colleagues could have accessed.

Dealing with an indispensable employee can be difficult. The norm must be that all operationally significant information must be documented; appropriate security for such documentation can include sealing passwords into opaque envelopes stored in the organization's safe and accessible only when two high-placed executives sign for it. Periodic testing of such repositories is appropriate.

On the procedural side, everything that affects the mission-critical operations of the organization must be part of the institutional knowledge of the group. At least two people should always be able to accomplish any given critical task; they don't have to be perfect at it, but the disappearance of the prime should not put the organization in jeopardy.

CROSS-TRAINING

Sometimes a person insists on being indispensable because of fear that their value to their employer resides in their private knowledge. Such employees resent and resist training others. The best way to change their counter-productive attitude is to walk what you talk: share knowledge with them and with everyone else in your group. Make education a normal part of the way you work. Encourage cross-training by allocating time for it. Make cross-training a factor in your employee evaluations. Have discussions of current topics from the trade press and academic journals. Start a journal club where people take it in turn to present the findings from recent research in areas of interest.

Reluctance to explain their job to someone else may also mask unauthorized or illegal activity. Take for example the case of Lloyd Benjamin Lewis, assistant operations officer at a large bank. He arranged with a confederate outside the bank to cash fraudulent checks for up to \$250,000 each on selected legitimate accounts at Lewis' branch. Using a secret code stolen from another branch, Lewis would scrupulously encode a credit for the exact amount of the theft, thus giving the illusion of correcting a transaction error. Lewis stole \$21.3 million from his employer between September 1978 and January 1981, when he was caught by accident. For unknown reasons, a computer program flagged one of his fraudulent transactions so that another employee was notified of an irregularity. It did not take long to discover the fraud, and Lewis was convicted of embezzlement. He was sentenced to (only!) five years in a federal prison.



FIGURE 10.16 Cross-training.

Since Lewis was obliged to be physically present to trap the fraudulent check as they came through the system, he could not afford to have anyone with him watching what he did. I doubt that Lewis would have been enthusiastic about having to train a backup to do his job. If anyone had been cross-trained, I doubt the embezzlement would have continued so long and been so serious.

Anyone consistently blocking attempts to have them document their work and cross-train replacements warrants increased attention and in extreme cases, investigation by experts to determine if there is chicanery going on.

MANDATORY VACATIONS

Another guide for managers is to enforce mandatory vacations. There are two reasons for insisting on vacations. First, vacations offer an opportunity for live testing of the principles of operational resilience described above. Second, vacations offer an opportunity to see if someone has been carrying out secret operations that must be continued to avoid discovery. For example, if an accountant has been embezzling money by paying fake companies for non-existent services or goods (and using the fake bank accounts for his own benefit), a two-week absence may reveal the crime when another employee notices the fake entries and investigates what they were supposedly for.

Lloyd Benjamin Lewis, mentioned in the previous section, took his unauthorized duties (stealing money from his bank) so seriously that during the entire period of his embezzlement, about 850 days, he was never late, never absent, and never took a single vacation day in over two years. As a data-center manager, I would have been alarmed at having an employee who had failed to be absent or late a single day in more than two years. How would you know what would happen if Mr Perfect really were away? The usual rule in companies is that if an employee fails to use vacation days, they can be carried over for a limited time and then they expire. This is supposed to be an incentive to take vacation time. For normal, honest employees it probably works fine. For dishonest employees who have to be present to control a scam, losing vacation days is irrelevant.

I recommend that every employee be *required* to take scheduled vacations within a definite – and short – time limit. No exceptions should be permitted. Excessive resistance to taking vacations should be investigated to find out why the employee insists on being at work all the time.

The problem is that the devoted, dedicated employee can get caught up in a Web of suspicion precisely because of exceptional commitment. The only ways I can think of to avoid difficulties of this kind are (1) to make the reason for the policy well known to all employees so no one feels singled out; (2) to rely on the judgment and discretion and good will of the investigating manager to avoid hurt feelings in their most loyal employees.

CHANGES IN BEHAVIOR AND MOODS

If employees change their interpersonal style radically – whether for good or ill – supervisors might want to look into the situation. Suddenly becoming *unexpectedly* friendly, hostile, happy, angry, cheerful, or depressed does not mean necessarily that an employee is involved in anything bad, but managers will do well to investigate.



FIGURE 10.17 Mandatory vacations.



FIGURE 10.18 Changes.

Any kind of unusual *behavior* should pique the curiosity of a manager. Even more important from a security-management standpoint, any *consistent* change in behavior should stimulate interest. Is Miss Punctual suddenly late – day after day? Did Mr Casual start showing up regularly in hand-tailored suits? Why is Miss Charming snarling obscenities at her staff these days? What accounts for Charles' working overtime every day all of a sudden – in the absence of any known special project? Is Yosuf, that paragon of perfection, now producing obvious errors in simple reports? How is it that the formerly complaisant Waclav is now a demanding and bitter complainer?

Any radical change in *personality* should elicit concern, too. If the normally relaxed head accountant now has beads of sweat on her forehead whenever you discuss the audit trails, perhaps it's time to look into her work more closely. Mr Bubbly is now a morose whisky-swilling sourpuss: why? The formerly grim Schultz now waltzes through the office with a perpetual smile on his face. What happened? Or what is happening?

All of these changes should alert you to the possibility of subterranean changes in the lives of your employees. Although these changes do indeed affect the security of your organization, they also concern managers as human beings who can help other human beings. Mood swings, irritability, depression, euphoria – these can be signs of psychological stress. Is your employee becoming alcoholic? a drug addict? abused at home? going through financial difficulties? having trouble with teenagers? falling in love with a colleague? Of course you can't help everyone, but at least you can express your concern and support in a sensitive and gentle way. Such discussions should take place in private and without alarming the subject or exciting other employees. If you feel out of your depth, by all means involve your HR or personnel department. They will either have a psychologist or trained counselor on staff or be able to provide appropriate help in some other way such as an Employee Crisis Line.

There are sad cases in which employees have shown signs of stress but been ignored, with disastrous consequences: suicides, murders, theft, and sabotage. Be alert to the indicators and take action quickly.

With so much of our organizations' financial affairs controlled by IS, it is not surprising that sudden wealth may be a clue that someone is committing a computer crime. A participant in a session of my *Information Systems Security Course* reported that an accounting clerk at a U.S. government agency in Washington, D.C. was arrested for massive embezzlement. The tipoff? He arrived at work one day in a Porsche sports car and boasted of the expensive real estate he was buying in a wealthy area of the Capital region.

Another case where an embezzler's change of lifestyle should have given him away was that of Nathan J. Mueller, who accidentally got permission to write checks of up to \$250,000 without supervision and stole about \$8.5 million from his employer. Unfortunately,

...[T]he evidence that he was living far beyond his means—the expensive cars and watches, the lavish nightlife, the frequent trips from Minnesota to Las Vegas—could have raised a few eyebrows among his co-workers, but nobody voiced any concerns for years.

Not all thieves are that stupid. A healthy curiosity is perfectly justified if you see an employee sporting unusually expensive clothes, driving a sleek car after years with a rust-bucket, and chatting pleasantly about the latest trip to Acapulco when their salary doesn't appear to explain such expenditures. On the other hand, being a *Nosy Parker*³⁸ who butts into people's private lives will win you no friends. It's a real bind but ignoring the issue doesn't make it disappear.

The other kind of change – toward the negative – may also indicate trouble. Why is your system manager looking both dejected and threadbare these days? Are they in the throes of a personal debt crisis? in the grip of a blackmailer? beset with a family medical emergency? a compulsive gambler on a losing streak? Again, on humane grounds alone you would want to know what's up in order to help. As a manager concerned with security, you have to investigate. In these days of explosive rage and ready access to weapons, ignoring employees with a dark cloud hovering over their heads may even be irresponsible and dangerous.³⁶

The manager's job is a tough one: you must walk the thin line between laissez-faire uninvolve-ment (and risk lifelong regrets or even prosecution for dereliction of duty) and overt interference in the private affairs of your staff (and risk embarrassment and prosecution for harassment).

Written policies will help you; so will a strong and ongoing working relationship with your HR staff. Making it clear to all employees that managers are available for support and expected to investigate unusual behavior will also help avoid misunderstandings.

SEPARATION OF DUTIES

The principle of *separation of duties* means that no *critical operation* should be completed by a single person.³⁸ In the embezzlement scenario discussed above, it was a problem that the accountant was able to create invoices, approve them, and pay them without supervision.

The same principles that apply to the control of money should apply to control of data. Watch the tellers at a bank: when you deposit a large check, you'll see the teller going to a supervisor, and having that person look the check over and initial the transaction. When bank tellers empty the ATMs at night and fill the cash hoppers, there are always two people present. In accounting departments, the person who creates a check is not the person who signs it.

In well-run IS departments, data entry is distinct from validation and verification. For example, a data-entry supervisor can check on the accuracy of data entry but cannot enter a new transaction without having their direct supervisor check their work. There is no excuse for allowing the supervisor to enter a transaction and then, effectively, authorize it. What if the entry were in error – or fraudulent? Where would the control be?

In quality assurance for program development, the principles of separation of duties are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. Test systems are separate from production systems; programmers must not have access to confidential and critical data which are controlled by the production staff. Programmers must not enter the computer room if they have no authorized business there; operators must not modify production programs and batch jobs without authorization.

When I ran operations at a service bureau in the mid-1980s, I trained two systems managers as soon as I could to take over the day-to-day management of the computer systems. When they were ready, I asked them to remove system-manager capabilities from my account. I had no wish to intrude on their province of responsibility. My meddling with system parameters would have caused more trouble than it would solve. Were there to be an emergency, I could be granted system-management permissions and resume my former role. We also stored the root passwords in a safe in a sealed envelope and required two executives to sign for release of that information. This approach exemplifies the concept of separation of duties.

In early 1995, the financial world was rocked by the collapse of the *Barings PLC* investment banking firm. The Singapore office chief, Nicholas Leeson,³⁷ was accused of having played the futures market with disastrous consequences. The significant point in our context is that he managed to carry out all the orders without independent overview. Had there been effective separation of duties, the collapse would not have occurred.

A related approach is called *dual control*. As an example of dual control, consider the perennial problem of having secret passwords that are not known to management yet sometimes needing emergency access to those passwords. This problem does not generally apply to ordinary users' passwords, which are normally reset by a security administrator without knowing either the old passwords or the new ones (which are then changed to truly secret and undecryptable strings in system storage). However, there may arise situations when only one person has the root password



FIGURE 10.19 Checking each other.

for a system (say, because the other system manager is on vacation). What if they're unavailable (unreachable, sick, dead)? We should always store a secured copy of the root password; for example, the holder of the critical password can write down and place it in a truly opaque envelope which is then sealed. The owner of the password signs the seal, tapes over the seal with non-removable transparent tape, and then stores the envelope in a corporate safe. The principle of dual control dictates that such a copy of the root password should be accessible only if *two* officers of the organization simultaneously sign for it when taking it out of the corporate safe.

In conclusion, think about the structure of control over information as you design your INFOSEC policies and make sure you are providing separation of duties or dual control throughout your systems.

JOB ROTATION

I was chatting with my friend Hamid one day and he told me about how he had just come back from a little gathering in the departmental office at the university where he works. Seems the janitor, Sandy, had been moved from the Computer Science (CS) building to the Humanities building despite roars of protest from the entire CS faculty and staff. Sandy had been working for CS for over 18 years and was beloved by everyone there. She was always ready to help in any way possible and kept the building spotless. She and the departmental secretary, also called Sandy, would have coffee every morning at 09:45 and were a pleasant sight as they chatted amiably.

Well, it wasn't a pleasant sight for everyone, apparently.

The people in charge of facilities management decided unilaterally, without consulting anyone, that Sandy the janitor was *too friendly* with the faculty and staff at CS. They moved her suddenly to Humanities and ordered her not to spend any more time chatting with people. "Just do your job," they said.

Sandy was heartbroken. All the people who smiled at her and stopped to chat every day at CS were also pretty displeased; they organized a petition, formed a committee, and got the department chair to protest to Facilities demanding the return of Sandy.

No result.

Eventually, as I said at the beginning, Hamid and all the other faculty and staff chipped in some cash and got Sandy a nice farewell card. The department chair said a little speech and then read out a letter that the chair of Humanities had already written even though it was only a month since Sandy had switched. In that short time, Sandy had already so impressed the new group that the Humanities chair had written a letter of thanks saying that she had never seen the building so clean! Hamid and his colleagues all wished Sandy well and told her to come back to visit them.

And what, pray, does this charming tale have to do with security management?

The relevance is that two of the suggestions commonly heard in IT management circles are that

- One should assign a specific technical support or security person to a specific department or other group so that the IT person can form bonds with the personnel and get to know their needs; and
- One should rotate personnel from department to department periodically to prevent collusion.

The problem is that these recommendations lead in opposite directions. It's very nice to talk about forming bonds and it's no doubt very efficient to talk about preventing collusion, but how do we reconcile these diverging goals?

I don't have easy answers, as you can probably tell from the way I'm framing the story and the question. I think that part of the problem is expectation; another part is timing. Now, I'm going to



FIGURE 10.20 The friendly janitor.

speculate that Sandy the janitor was never told that she would be moved from building to building. My guess is that none of the janitors were told that there was any reason to avoid being friendly—who would reasonably think that being a friendly employee could be viewed negatively? So suddenly moving her must have been a real shock. If it is true that the move was sudden and exceptional, then it was also a slap in the face: presumably Sandy felt that she was being told she had done something wrong. Clearly Sandy wanted to do the right thing, so such a judgment and punishment must have been doubly painful.

As for timing, 18 years is a long time to wait before being rotated. Rotating staff can be viewed as positive; there can be benefits for everyone. For example, thinking now about security management, one can spread knowledge through the entire security team by having people learn about the work habits and security needs of a wide range of work units and individual people. Getting to know colleagues as individuals and becoming friends with many of them can really make a difference in developing and implementing security policies, emergency-response plans and disaster-recovery plans. So switching people around is not inherently bad and can be constructive.

The question is, how long should a security team member be assigned to the same beat?

My own guess is that it should be on the order of many months—maybe even a year. Much shorter than that and it seems to me that one would cause more disruption than growth. It takes time to earn trust and develop constructive relations; I'd let my personnel become acclimated to the new social environment and then enjoy the friendly relations for some time before gently moving them on to the next area. And I'd make sure that everyone knew what the plan was, that the new team member could be personally briefed and then introduced by the outgoing team member, and that occasional visits to the "old" beat were encouraged and praised. And most important, everyone should be confident that a move would not be a slap in the face.

With that kind of policy, moving would be more fun and less pain.

PROTECTING PRIVACY

Many organizations strive to protect the confidentiality of prospects and clients. In this section, I explore issues relating to privacy policies and sometimes problematic relations between legitimate, well-meaning institutions, and the commercial organizations with which they do business.

In the United States, privacy laws cover a variety of areas such as consumer information,³⁹ medical information,⁴⁰ judicial-system information,⁴¹ and tax information.⁴²

In Europe, the GDPR is a comprehensive set of laws governing how *personally-identifiable information* (PII) is to be restricted.⁴³

The regional laws apply to all organizations doing business in the particular zones in question regardless of the ownership or headquarters of the organizations. Thus U.S. firms, for example, which are doing business in Europe must comply with the GDPR just as (say) Asian firms doing business in the United States must comply with U.S. privacy regulations.

Every organization's legal department *must* collaborate with policy-makers to ensure that all relevant privacy requirements are reflected accurately in corporate documents and enforced without exception by well-trained managers. Such requirements are particularly important not only to protect employees but also to protect the PII of customers and users of corporate Web pages.

Training employees to understand and implement privacy requirements is essential. For several years after the U.S. HIPAA regulations were enacted, I noticed that receptionists at the local medical center where I was a regular user were calling out the full names of patients in the waiting room when they were to be treated by the medical staff. I had to explain to many receptionists that they were violating HIPAA and should be using only the first names of the patients in a public space.



FIGURE 10.21 Privacy at work.

Eventually I spoke with the Personnel Office of the Center and warned them about the infringements of patient confidentiality. The problem gradually disappeared once the staff were properly informed of the law.

SAMPLE PRIVACY POLICY ON A WEBSITE

Norwich University's *Privacy Policy* for the *College of Graduate and Continuing Studies*⁴⁴ stands as an excellent example of a clear, well-written, and comprehensive document – an example that could usefully be considered by readers of this section who may need a sample policy for their own organization's use. Links to the *Privacy Policy* are available wherever visitors may enter PII; for example, the admissions-related pages have links at the bottom of every page with a data-entry form. Specifically, the policy makes the following essential points (quoting with added commentary in square brackets):



FIGURE 10.22

The privacy policy.

- “Our *Privacy Policy* was developed to respect the privacy of all website visitors and to inform you what information Norwich University collects through its websites, web applications, and telecommunications, how we use that information, and how we protect your information.” [A privacy policy should begin with a statement of the purpose of data collection.]
- “We collect information in order to help us serve your needs better and to inform you of our programs. We collect personal information that you choose to give to us, as well as other information that is automatically collected when you visit our websites and web applications and/or opt in to receive telecommunications (i.e. SMS messages).” [The *Policy* is put in an operational context.]
- “Information you choose to give to use includes, but is not limited to, the following:
 - contact and identification information, such as your name, address, telephone number and email address;
 - information concerning your education history, including degrees granted and universities attended and employment history;
 - application information relating to Norwich University's programs, including credit information for payment of application or deposit fees; and
 - business relationship information including information related to your preferences, feed-back and information requested by or provided to you.” [These are useful clarifications of the intended applications for the collected data.]
- “We collect this information when you send it to us by various means, including but not limited to, submitting application information for our programs, requesting to be contacted by us, or responding to email requests./We also have your information that is automatically collected when you visit our websites through web visit logs and cookies.”
 - Web Visit Logs: We collect and store information from online visitors to help manage our sites and improve our services. This information includes the pages visited on the site, the date and time of the visit, the internet address of the referring site, the domain name and IP address from which the access occurred, the device used, the version of browser used, the capabilities of the browser, general demographics and interest categories of users, and search terms used on our search engines.
 - Cookies: Cookies are pieces of information stored by your web browser on behalf of a website and returned to the website on request. Our websites may use cookies for two purposes: to carry data about your current session at the site from one web page to the

next, and to identify you to the site between visits. If you prefer not to receive cookies, you may turn them off in your browser, or may set your browser to ask you before accepting a new cookie. However, some pages may not function properly if the cookies are turned off.” [Details of how the PII is collected – encourages confidence in the data subjects because there should be no surprises for them.]

- “How do we protect your information?
 - We protect your information by using encryption/security software to safeguard the confidentiality of personal information we collect. This software provides a limited degree of protection against unauthorized access or disclosure, as well as accidental loss, alteration or destruction.
 - We protect our records in accordance with applicable Vermont and U.S. federal laws.
 - We do not sell or rent any of your personal information to any third party. However, we may need to disclose your personal information when required by law.
 - Furthermore, if you enroll in an online program, to the extent the personal information you provide to us is considered an educational record under the federal Family Educational Rights and Privacy Act (FERPA), it is considered confidential and is protected from disclosure under the provisions of FERPA.
 - At any time, you may request to discontinue receiving email or text message communications from us about our programs by clicking on the opt-out ‘unsubscribe’ link in the email to unsubscribe from further email communication, and/or by replying ‘Stop’ to the text messages.” [These are specific constraints on how the data are to be used.]

CONTROLLING BUSINESS PARTNERS

First of all, any site which is under contract to your organization for marketing your products or services must have contractual obligations stipulating compliance with *your* privacy policy.

For example, suppose you have contracted with a company that runs a website for serving possible customers who enquire specifically about your products, programs, and services. Imagine how horrified you would be to find that the company were selling or otherwise sharing the names and contact information of such potential customers to your competitors! On economic grounds alone, such behavior would be counterproductive for your organization; worse, it could tarnish *your* reputation as an institution of integrity by erroneously giving prospects and even clients the impression of improper behavior. Therefore, your organization should periodically audit sites marketing information about you on the Web.

In researching this question I found sites whose privacy policies do little to protect visitors’ privacy. For example, some of these policies explicitly state that information collected on the site may be shared with business partners, service providers, sweepstakes and promotions organizers, subsidiaries, law enforcement, and non-affiliated companies.

One text about *non-affiliated companies* would raise concerns for anyone (I am deliberately not publishing the names of these firms). The policy begins reassuringly,

We do not share Information with any non-affiliated third party except: (1) in select circumstances when Our business partner refers you to Us and you give Us permission to share specific Information, such as your name and email address, with such business partner on your order form....

Unfortunately, it continues with

... or (2) when our business partner provides a product or service that we feel may be of interest to you.



FIGURE 10.23 Partnership.

That second part makes the assurance meaningless. The statement means that the company will share personally identifiable information with anyone it chooses to do business with – or more bluntly, to whom it will sell prospects’ names for profit. Give them enough money and I’m sure that practically anything will seem interesting.

The lesson I draw from this cursory investigation is that no one can afford to do business with people who do not use the same strict policies of privacy protection as their own organization. Readers should perform a systematic audit of all their organizations’ links to third parties to verify that deviations from their privacy policies do not lead to embarrassment and legal liability.

OPTING OUT

In this section, I look at some of the issues that can occur when you work with other organizations whose policies may differ from yours.

One of the marketing companies’ sites I investigated where interested parties could fill in a form to request information included some information on opting out of receiving commercial email and other unsolicited marketing materials from itself, its business partners, and anyone to whom it chose to sell enquirers’ names.

That privacy policy included the following information:

- Email Opt-Out Options: Each marketing email we send includes instructions and an opt-out link.
- Refusing Cookies: Subject to the section below pertaining to cookies and Web bugs, you have the ability to prohibit being served an advertisement based on cookie technology. We utilize reputable third-party vendors to serve advertisements. If however, you are not comfortable with cookies, you can adjust the settings within your browser to further prohibit being served a cookie. Please see the browser’s instructions to perform this task.
- The National Advertising Initiative (NAI) has developed an opt-out tool with the express purpose of allowing consumers to “opt-out” of the targeted advertising delivered by its member networks. You can visit the NAI opt-out page and opt-out of this cookie tracking. Please visit: http://www.networkadvertising.org/optout_nonppii.asp.
- Other Options: If you would like to opt-out of our promotional marketing, and would like to contact us, please send us an email at privacy@<suppressed>.com.

Most people in the security field with whom I have discussed the issue argue strongly against requiring only *opting-out* as an acceptable form of control over the abuse of PII. The *European Coalition Against Unsolicited Commercial Email* (EuroCAUCE) <<http://www.euro.cauce.org/en/>> had a succinct explanation of the arguments:

“Opt in” is the scheme of choice of EuroCAUCE, because it is the only scheme that ultimately works. The party interested in sending out bulk email must put in some effort up front, but it pays off in the long run to be able to acquire and maintain a list of potential customers. Problems of scale and administration (not to mention honesty and integrity) render virtually all “opt-out” schemes ineffective, both “individual” and “global”.

“Individual” opt-out schemes, where the recipient is expected to answer with a “remove” request, suffer from problems of scale. If only 1% of the EU’s 18.4 million businesses decided to operate in this way, it would be possible to have someone employed full-time for a whole year doing nothing else but issuing “remove” requests at nearly two per minute [see below]. And that’s just for one email address. There are considerations of honesty and integrity as well: one sending entity may well honour a “remove” request, whilst passing the address onwards to another entity as a “confirmed live” address, thus the hapless recipient ends up getting more UCE than might otherwise have been the case. Experience suggests that this despicable practice is more often the rule rather than the exception.



FIGURE 10.24
Opting out.

So-called “global” opt-out schemes are at least tempting to consider for all forms of advertising communication directed to individuals. These, too, suffer from problems of administration, honesty and integrity. As the British Department of Trade and Industry states,

“In order for an opt-out scheme to provide effective consumer protection, it would have to fulfil certain criteria. It would be necessary for:

- all subscribers to be aware of it.
- it to be simple and free to join.
- it to become effective within a reasonable time of joining.
- it to require companies engaged in telemarketing to update their lists regularly in the light of subscribers’ notifications.
- it to have adequate complaints handling mechanisms.”⁴⁵

Here is my own summary of the issues:

- Opt-out schemes cannot cope with the sheer scale of spamming. Spreading email addresses from one spammer to another inevitably outraces attempts to react to each new source after the fact.
- It is impossible to ensure that permanent do-not-spam lists are consulted by spammers.
- There is no mechanism for supervision of compliance efforts.
- There are no enforcement mechanisms to prevent abuse.

In my view, opt-out schemes for protecting privacy are usually legitimate attempts to balance marketing departments’ needs for productivity with privacy advocates’ preference for better protection. However, for some unscrupulous marketers, opt-out policies may mask deliberate programs to capture user information that can be used or sold at a profit before the users can stop the abuse. Your organization should carefully examine the advantages and disadvantages of opt-out schemes before signing contracts with firms that use such methods.

WHO’S ACTUALLY REQUESTING MY INFORMATION?

The problem of protecting privacy is greatly complicated by the web of relationships that can develop in the world of marketing. The relationships can involve remote firms that have contracts with your marketing division or contracts with firms that are one or more levels removed from direct interaction with your organization. Worse still, some sites may even be run by rogue organizations which have never had any contractual links whatever with you or with any of your legitimate agents. These facts make it almost impossible to protect PII against *nasty* visitors interested in your products, services or programs from being spread to other institutions.

You are left with a distasteful duty to warn all applicants that you can control the use of their PII only when they enter data into forms directly under the control of your own staff or of firms which have contractual obligations to follow your privacy policy. Examine your privacy policies to see if you should include explicit warnings that they apply only to your clients and not to people asking for information. It may make sense also to include a warning about the impossibility of your controlling privacy policies on websites outside your own domain.

In terms of response to complaints, you will have to continue being prepared to respond, basically, “Caveat emptor” (buyer beware). You can prepare general texts regretting (and repudiating) the impression that your organization has violated any privacy policy and explaining that anyone entering data on *any* website would do well to examine the local privacy policy for clarification of what degree of protection is offered for PII. If the privacy terms seem too loose, privacy-conscious



FIGURE 10.25

Hiding
corporate identity.

individuals may decide to skip using those websites; instead, they can look for safer, more trustworthy alternatives that provide the same access to the desired information.

As mentioned above, an additional and probably intractable problem is that not everyone who uses your name, and your logo necessarily has any business relationship with your organization at all. *Phishing* (using fake email that looks like legitimate messages from well-known organizations) and *pharming* (using fake webpages that look like legitimate websites belonging to well-known organizations), for example, are based on impersonation of business entities. Someone could easily use your organization's name and logo on a form claiming to be related to providing information about your organization, products, services, or programs – and then simply use the collected PII for their own purposes. Failure to send the victim the requested information reflects badly on your perfectly innocent and unknowing organization; selling the PII to spammers makes you look terrible. And what are you going to do about it?

If someone is abusing your trademark or your servicemark, you can sue them for misappropriation – if you can find them. With fraudulent websites appearing and disappearing with lifetimes sometimes measured in days or hours, it may be hard to locate the criminals who are ruining your reputation. Going after the service providers is going to be tough because many jurisdictions have laws protecting *Internet Service Providers* (ISPs), including some Web hosting services, from legal liability if they pay no attention to the content of what their clients are putting on the Web (a stand called *disintermediation*).⁴⁶ From a practical perspective, what can a CISO do to stop this kind of abuse?

In practice, your organization can hope to obtain redress only from responsible, stable firms with which you have signed contracts. Such firms will care about their own reputation as well as yours and will respond to both notification of abuse and the possibility of legal pressure. Criminals, however, are out of your control, especially if there are international boundaries in the way. The chances of getting any response, let alone cooperation, from law enforcement agencies in many parts of the world where criminals abuse the Internet are virtually nil.

Readers concerned with measuring the extent of the PII-violation problem for their corporate identity may want to institute a systematic program of regularly scanning the Web using search engines. In addition, you can test third-party sites that mention your corporate name or claim to be offering managed marketing information by using a list of fake unique identifiers (M. F. Kabay, M. Q. Kabaye, N. B. Kabbay ...) and their corresponding one-time use email addresses ([mfkabay@<\\$string1>.com](mailto:mfkabay@<$string1>.com), [mqkabay@<\\$string1>.com](mailto:mqkabay@<$string1>.com), [nbkabbay@<\\$string1>.com](mailto:nbkabbay@<$string1>.com) ...). The unique identifiers can be assigned to the specific webpages under test and recorded in a list, a spreadsheet, or a DB for later reference. Any email to a test address originating from an organization other than the managers of the place where the unique identifier was originally used indicates potential abuse or violation of contracts. Similarly, filling out a form (using fake info) that claims to be sending people information about your organization but finding that you never receive a response tells you that there's something fishy about the site. If there are many test names and one-time email addresses, you can consolidate the traffic for the compliance officer by having all email that is sent to the test addresses auto-forwarded to a single mailbox for easier analysis.

It's not going to be easy, but at least you can put your privacy-protection measures in place before you face a major PII disaster. Keep your eyes open, follow-up on abuse of your corporate identity, and make your own policies clear and effective.

I wish I had something better to offer, but that's about it for now.

THE VULNERABLE URL

A privacy-breaching error related to URLs involves using a numerical code to locate PII without imposing strict authentication on requesters for a link. For example, suppose Albert logs on correctly and securely to [INFOSOURCE.ORG](http://www.infosource.org) <not a valid domain at the time of writing> and has access to his own information using, say, <http://www.infosource.org/123456> and then enters <http://www.infosource.org/123457>, that link must *not* bring up information about, say, Betty.

In one case, a colleague of mine told me with embarrassment that he had committed a violation of 18 USC 1030(a) when he was irritated by spam addressed to his email address. He noticed that the *unsubscribe* link that was available in the spam used a numerical code that (supposedly) allowed him to remove his own email address from the spammers' list. Out of curiosity, he changed the numerical code and was shown an unsubscribe link for a different person.

Actually, there's no guarantee that *any* "unsubscribe" link actually does remove the victim's address; even if it blocks further email from the original sender, it is possible that the use of the page actually confirms that the victim's email is correct – whereupon it can be sold to other spammers for profit.

The colleague made a stupid mistake: He wrote a script with thousands of unsubscribe links by including the numbers in sequence from 000,000 to 999,999. He either *unsubscribed* thousands of addresses which happened to use numbers in his list or *confirmed* them – no one knows. But imagine the disaster if entering digits in the URL had brought up actual PII about the people involved! A simple script for Acrobat would have captured all the pages with valid IDs.

Webmasters must definitely *not* use simple numerical codes in URLs to allow access to confidential data without authentication of the user.



FIGURE 10.26 Numerical URL.

TERMINATION OF EMPLOYMENT

Well, things haven't gone as well as they should. One or more employees must be fired for reasons such as workforce reductions, mergers and acquisitions, or inadequate individual performance. The basic rule is that absolutely everyone must be treated with the same procedure and the same respect, regardless of manager's emotions about the termination. If Albert is frog-marched to the exit by a security guard whereas Betty is treated to a joyful party, the message is clear: Albert is bad and Betty is good. Such implicit criticism and praise can lead to lawsuits for defamation (by the Alberts). It is best to maintain strict even-handedness when firing people; then the employees can organize a farewell party privately, on their own time, off the organization's premises.



FIGURE 10.27 Termination.

Taking our security mandate in the widest sense, we have to protect our employer and ourselves against potential damage from unethical, disgruntled, or incompetent employees and against the legal consequences of improper firing procedures. Common sense and common decency argue for humane and sensitive treatment of people being fired and those who are resigning.

RESIGNATIONS

What about resignations? What if old Charlie has worked diligently for 30 years and is beloved by all? Can't we have a farewell party on the organization's premises? Well, it's a pity, but in a litigious environment, it's best to have the party off premises and without sponsorship by the organization itself. Now, Charlie probably let people know about his pending resignation months or years before the event (for example, I told my dean to expect my resignation at the end of December 2020 a full year in advance), so there

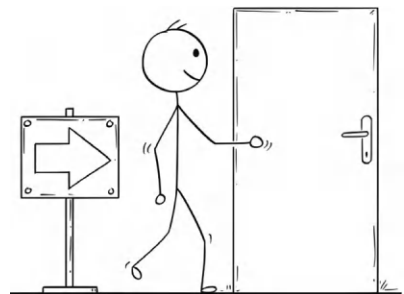


FIGURE 10.28 Resigning.

is no need for any surprise in how he is treated. Furthermore, it may be valuable for Charlie to help document details of his work that may not have made it into institutional knowledge and to train his replacements. Nonetheless, exactly the same process as for anyone else would apply to Charlie on the last day of work – the exit interview, clearing the desk, returning identification cards, and returning other corporate property.

An exit interview can be either a painful exercise or a positive experience. If the separation is amicable, the departing employees may be able to contribute insights that might have been more difficult to impart to managers while they were employed. Even if there is some friction underlying the departure, it's still possible to extract useful information from the employees if they are willing to speak their mind.

Finally, the termination process must be tightly coordinated between the HR group and the IT and IA groups. As the exit interview is underway, the employee's access privileges must all be revoked and assigned to appropriate replacement personnel who will take up the tasks of their former colleague.

The potentially most dangerous form of employment termination is the resignation. The problem is summed up in the caption of a cartoon I once saw. A savage attack is in progress against a medieval town; a clan war chieftain confronts a singed and dirty warrior. "No, no, Thor! Pillage, THEN burn!" Like the warriors, employees rarely resign without planning. An employee may have an indefinite period during which he or she knows that resignation is imminent, whereas the employer may remain unaware of the situation. If the employee has bad feelings toward or evil designs on the current employer, there is a period of vulnerability unknown to management. Dishonest or unbalanced employees could steal information or equipment, cause immediate or delayed damage using programmatic techniques (the so-called *logic bomb*), or introduce faulty data into the system (*data diddling*).

The policies discussed in previous sections for ongoing management should reduce the risks associated with resignations. Your goal as a manager should be to make resignations rare and reasonable. By staying in touch with your employees' feelings, moods, and morale, you can identify sources of strain and perhaps resolve problems before they lead to resignations and their associated security risks.

FIRINGS

Firing people is a stressful time for everyone concerned and leads to increased security risks. Managers should do everything in their power to ensure a courteous, respectful, and supportive experience when terminating employment.

Firings give the advantage to employers. The time of notification can be controlled to minimize its effects on the organization and its business. For example, employers might find it best to fire an incompetent or unacceptable employee before beginning an important new project or after a particular project has finished.

Some people argue that to reduce the psychological impact on other employees, they fire people at the end of the day, perhaps even before a long weekend. The theory is that the practice gives everyone a cooling off period outside working hours. These managers say they don't want the buzz of conversation and speculation that often follow a firing to intrude on the workday. This policy fails to regard the psychological stress to employees who have a ruined weekend and no way of responding constructively to their potentially catastrophic loss of a regular income.

A better approach to this stressful task is to fire people early on Monday morning in order to provide an unrushed exit interview and job counseling to help the employee prepare for job hunting. In this scenario, the regrettable necessity (from the manager's point of view) of terminating employment is buffered by professionals in the HR department who can give the departing employee a sense of hope and some practical as well as emotional support in their difficult time. This humane



FIGURE 10.29 Fired!

attitude is particularly important when there are many people being fired – one of the worst experiences possible for both employees and managers and an event that has serious security implications.

DOING IT WRONG

A participant in one of my professional seminars told the following horrifying tale of a firing gone wrong.

In a large company, the personnel department asked information-security staff to suspend the access codes for more than 100 people who were to be fired at 18:00 on Tuesday.

On Wednesday at 08:00, the security staff began receiving phone calls asking why the callers' logon IDs no longer worked.

It turned out that the personnel staff had failed to inform the "victims" on time.

The psychological trauma to both the employees who were fired and to the security staff was severe. Several security staff members were sent home in tears to recuperate from their trauma. The harm done to the fired employees was even more serious, and the effect on morale of the remaining employees was a disaster.

It's a wonder that there was no violence in that situation. There could have been lawsuits!



FIGURE 10.30 Distressed employee.

CROSS-TRAINING AGAIN

One of the key organizational issues in planning or responding to termination of employment is training replacements for the departing employee. Such needs are voiced to justify policies allowing a more graceful, civilized, and friendly approach to firings and resignations.

An earlier section in this chapter discusses the need for cross-training to avoid disasters.

In the context of termination of employment, it *may* be reasonable to encourage a voluntarily departing employee to train the colleagues or new employees who will assume his or her responsibilities. However, such arrangements cannot be forced on a departing employee. Cross-training should be part of the normal operations of all organizations and absolutely *not* dumped on an employee who is going to be *fired*!



FIGURE 10.31 No, not *that* kind of cross-training!.

HOW TO SAY GOODBYE

Let's suppose the time has arrived for an employee and the employer to part company. In both resignations and firings, security consultants unanimously advise instant action. Not for them the leisurely grace period during which employees wind down their projects or hand them off to other staff members. No, security officers are a hard lot, and they advise the following scenario:

- In a formal exit interview, and in the presence of at least two managers, an officer of the employer informs the employee politely that his or her employment is at an end.
- During the exit interview, the officer explains the reasons for termination.



FIGURE 10.32 Farewell.

- The officer gives the employee a check for the period of notification required by law or by contract (e.g., this could be at least the same period as that between pay checks) plus any severance pay due by contract or law.
- Under supervision (preferably in the presence of at least one security guard), the employee is escorted to their work area and invited to remove all personal belongings and place them in a container provided by the employer.
- The security staff need an up-to-date checklist to ensure that the employee returns all company badges, IDs, business cards available, credit cards, and keys.
- The employee is then ushered politely outside the building.

At the same time as all this is happening, all security arrangements must be changed to exclude the ex-employee from access to the building or secure campus and to all IS. Such restrictions can include:

- Striking the person's name from all security post lists of authorized access;
- Explicitly informing guards that the ex-employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- Changing the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;
- Removing or changing all personal access codes known to have been used by the ex-employee on all secured computer systems (microcomputers, networks, mainframes);
- Informing all outside agencies (e.g., tape storage facilities, publications with company advertising) that the ex-employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;
- Requesting cooperation from outside agencies in informing the employer if ex-employees attempt to exercise unauthorized functions on behalf of their former employer.

The task is made more difficult by seniority or if the ex-employee played an important role in disaster recovery or security. The employer's team should be assiduous in searching out all possible avenues of entry resulting from the person's position of responsibility and familiarity with security procedures.

In May 2021, a part-time employee was fired. Unfortunately, no one removed her user ID or changed its access privileges, so she was able to log into her previous employer's system two days later. A news report summarized the events:

...[A] former employee of a New York credit union destroyed over 21 gigabytes of company data as a revenge plot after getting fired. The data included around 20,000 files and 3500 directories consisting of customers' mortgage loan applications and anti-ransomware protection software.

...[The] credit union had some of the deleted data backed up but they still had to spend more than \$10,000 to recover the lost files all because of one employee's petty behavior.⁴⁷

PSYCHOSOCIAL ISSUES IN FIRING PEOPLE

What, no farewell party? Alas, security does interfere with the more obvious signs of friendliness. The problem with a farewell party is that there may be litigation if employees leaving under a cloud feel humiliated when most people get a party but they don't. Generally, it makes sense to treat all departing employees the same if the termination is involuntary.



FIGURE 10.33
Psychological distress.

However, nothing stops a humane and sensitive employer from encouraging *employees* to arrange an after-hours party even for people who have been fired. However, having the employer arrange and pay for parties only in some cases raises the specter of perceived (or real) discrimination and damage to some employees' reputations.

A firing or a resignation on poor terms has two psychological dangers: effects on the individual concerned (embarrassment, shame, anger) and effects on the remaining staff (rumors, resentment, fear).

Both kinds of problems can be minimized by

- Publishing termination procedures in organization documents provided to all employees;
- Requiring all employees to sign a statement confirming that they have read and agreed to the termination procedures; and
- Consistent application of the termination procedures.

The personal shock of being fired can be reduced by politeness and consideration consistent with the nature of the reasons for being fired – although even nasty people should not be subject to verbal or physical abuse no matter how bad their behavior. Treatment should be consistent with that meted out to other fired employees; for terminations not involving punishment, organizations can evaluate generous severance arrangements as part of its employment-termination policies.

I once had to leave a wonderful company because of reasons beyond the control of the employer and myself. Neither the company nor I wanted to terminate my employment. The owner of the company offered to continue paying my salary until I found a job – and urged me to take all the time necessary to find a satisfactory job. His generosity eased the shock of having to leave my friends and colleagues.

Organizational turmoil can be reduced by convening organization-wide or departmental meetings to brief remaining employees on the details of significant termination; open discussion, including understanding how people respond to rupture of relationships.

The remaining employees may also have to suffer grief (a process, not a state). Grief is a normal and healthy response to disruption of relationships (e.g., death of a loved one, divorce, and even the loss of a coworker). Some people value social relationships more than other aspects of their work and may be especially affected by firings. Grief involves several stages.⁴⁸ Trying to forestall severe responses by denying that people legitimately have feelings is foolish and counterproductive. It is far better to encourage those who are upset to voice their feelings and to engage in constructive discussion than to clamp down pointlessly in a futile attempt to suppress discussion.

STYLE

The way an organization handles job termination affects more than internal relations. It also influences its image in the outside world. Prospective employees will think twice about accepting job offers from an organization that maltreats departing employees. Clients may form a negative impression of a company's stability if it abuses its own people. Investors may also look askance at a firm that gets a reputation for shoddy treatment of employees. Bad employee-management relations are a warning signs of long-term difficulties.

A glaring example of the consequences of bad firings occurred on the 29th of November 2021.

The CEO of the (ironically named) mortgage company [Better.com](https://www.better.com), Vishal Garg, fired 900 employees immediately in a brief video-conference call and then posted insulting accusations about them on social media.⁴⁹



FIGURE 10.34 Bad style for terminations.

An explosion of bad publicity led to the CEO's taking a "leave of absence;" it also led to extensive publicity about his pattern of abuse and even possible dishonesty.⁵⁰

Within a week, disgruntled employees worked with a law firm specializing in class-action lawsuits to explore the possibility of suing the company "for allegedly violating the *Worker Adjustment and Retraining Notification Act*, which requires that certain companies provide written notice to workers at least 60 days before layoffs."

The company doubled its severance pay to 60 days.⁵¹

(If I didn't include references to this case, I think many readers would assume it was a ridiculously exaggerated example I made it up to strengthen my arguments in favor of careful preparation for firings.)

All of the factors mentioned above affect the foundation for sound information security. People are the key to effective INFOSEC, and disaffected employees and angry ex-employees are still important threats according to many current studies. For example, decades of studies support that view that computer-crime threats to large corporations and government agencies come from both inside and outside their electronic perimeters.⁵²

LEGAL ISSUES IN FIRING PEOPLE

There's another dimension to employment termination that depends on local laws and the litigation environment. Contrary to popular belief, the United States is *not* the most litigious country in the world,⁵³ so it's important for readers to study the situations in their own countries, not simply assume that it's only a U.S. problem.

Now, let's be sure everyone understands the obligatory disclaimer to avoid going to jail for dispensing legal advice without a license: *I am not a lawyer and this is not legal advice. For legal advice, consult an attorney.*

However, reading, studying, and simple experience do teach one some principles even without going to law school. Here are some pragmatic guidelines for preventing legal problems related to firings:

- Build a solid, documented case for firing someone before acting.
- Keep good records, be objective, and get the opinions of several trustworthy people on record.
- Give the employee clear feedback long before considering firing.
- Assuming there has been no criminality, offer the delinquent employee all reasonable chances to correct his or her behavior.

Timing

Timing is important in employee relations, as it is in almost everything else we do. In particular, if an employee is found to be behaving improperly or illegally, there must be no marked delay in dealing with the problem. Such a person could theoretically sue the employer and individual managers, arguing in court that the very fact that there was a delay in firing them was proof that the firing was due to other factors such as personality conflicts, racism, sexism or other forms of illegal discrimination. A well-defined procedure for progressing through the decision will minimize such problems.

When terminations are required by organizational changes or external conditions (e.g., drastic financial difficulties), managers



FIGURE 10.35 Legal issues.



FIGURE 10.36 Timing properly.

should still be thinking about avoiding unnecessary stress for all concerned. For example, firing lots of people just before major holidays is unlikely to improve employee morale:

There are a few certainties around the end of the year in my business.

People will complain endlessly about performance reviews - giving them, receiving them, and coordinating the whole process.

Productivity generally takes a dive as people are more focused on their holiday plans and upcoming vacations (though there are ways to avoid it).

It seems to be the most popular time of the year to fire people. Admittedly, this is purely anecdotal, but every year in December two things happen to me: I see a spike in people looking for help, saying, “I was just fired and I don’t know what to do,” and I see a spike in conversations I have with my clients who are fishing for reasons to fire people....

...[T]here are very logical reasons it’s a bad decision:

- It will increase your odds of being sued....
- Your remaining staff will bear the brunt....
- It will have long-term implications....
- It may not have any real impact on the bottom line....⁵⁴

Consistency

As described in the advice in previous sections, the critical legal issue is consistency. If rules such as those described above for the day of the firing are applied haphazardly, there could easily be grounds for complaining of unfairness. Those to whom the rules were strictly applied would justifiably feel implicitly criticized.

How would we feel if we were singled out by having guards check what we took home from our desk – if everyone else got a party and two weeks notice? Such inconsistency could be grounds for legal proceedings claiming defamation of character. The employer might lose and it might win, but what non-lawyer wants to spend time and money in court?



FIGURE 10.37
Consistency.

NDA

Another issue that arises in connection with firings and resignations is *non-disclosure agreements* (NDAs). All such agreements must be included in a contract signed before the prospective employee begins work; it may be difficult or even impossible to force an *existing* employee to sign such an agreement.

I remember one employer approaching me two years into my contract with them and asking that I agree that all patents I might develop – even those resulting from work at home in off-hours – would belong to the employer. I refused, and there was nothing they could do about it (well, fire me, but they didn’t).

Any attempt to threaten an employee with dismissal on such grounds could lead to a lawsuit for breach of contract and, if the dismissal were carried out, wrongful dismissal.

In recent reports, NDAs have been the subject of considerable concern because of growing evidence that they have been exploited to prevent victims of abuse from reporting that abuse. Some NDAs have “non-disparagement” provisions that forbid any public criticism of their current or even former employer, including reporting factual evidence of abuse.⁵⁵

You, your legal department and your personnel department should study the necessity and feasibility of instituting a legally binding contractual obligation to protect your company’s confidential information for a specified period of time after leaving your employ. You cannot impose indefinite gags on people, but one year seems to be normal.



FIGURE 10.38
Don’t talk!.

NCAs

Non-competition agreements (NCAs) require the employee to refrain from working for direct competitors for perhaps a year after termination of employment. The key to a successful clause here is that there be a strict, operational definition of “direct competitors.” Because such limitation can be an onerous impediment to earning a living, many jurisdictions forbid such clauses or are considering doing so.⁵⁶

NCAs are usually intended to support NDAs by preventing employees from taking confidential information or proprietary knowledge to a *competitor*.⁵⁷ They stipulate that an employee shall not accept employment with competitors of the employer for a specified period after termination of employment. NCAs may specify limits on work with direct competitors, competitors in a specified geographic area, or even the industry in which a former employee shall work.⁵⁸

NCAs must be carefully phrased to comply with legal requirements – and these requirements may vary across jurisdictions. The *QuickMBA* website has a useful article about “Employment Law and Duties to One’s Former Employer” which includes several interesting discussions of case law in this area.⁵⁹

From the employer perspective, confidentiality agreements, NCAs, and the other restrictive covenants serve to protect valuable intellectual property and to prevent damage to an organization’s reputation from disgruntled former (or even current) employees. On the other hand, excessively restrictive post-employment terms may discourage talented candidates from accepting employment in the first place. Perhaps listing a few specific firms in the contract is a reasonable compromise.

All sources emphasize the importance of reviewing NCAs with an appropriately trained attorney. Improperly constructed NCAs may be unenforceable; excessively restrictive (but legal) agreements may seriously harm an individual.

In addition, no employer should try to impose a *new* non-compete clause on existing employees. Any such attempt could lead to resignations of key personnel or, if not that, tremendous resentment.

From the employee perspective, these agreements or covenants pose a serious risk to future livelihood. Not being allowed to work in one’s field of expertise for even a single year could be a tremendous hardship. In contrast, agreeing not to work for any of a *restricted* (short) list of direct competitors may be an acceptable trade-off in return for a signing bonus or even just for an employment opportunity. But above all, no one should sign such an agreement without consulting an attorney. The cost will be repaid many times over if one can avoid a disastrous period of unemployment. And if the potential employer puts pressure on the candidate – say, by refusing to allow a reasonable time for consideration of the terms of employment – I would walk away from the job offer immediately. I would not want to work for a firm that tried to bully people into signing employment agreements without appropriate legal advice.

FINAL COMMENTS

One element that strikes me in these discussions is that there is an unhealthy asymmetry today in some managers’ attitudes toward employees. Some managers speak as if *employees* owe the *organization* loyalty and long-term commitments – yet at the same time, these same managers express strong support for the notion that *organizations* have no obligations whatever toward employees’ continued employment. Apparently employees are to be hired and fired at will, as if human beings are fungible automatons who serve the short-term interests of



FIGURE 10.39
Non-compete agreement.

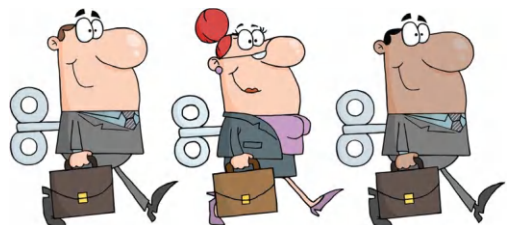


FIGURE 10.40 Not robots.

the organization.⁶⁰ Such a management philosophy ignores an alternative view: that an organization is a group of *people* who have *relationships* that profoundly influence long-term success of the organization.

From an information-security perspective, anything that decreases the solidarity of the organization puts us at increased risk of harm.

We treat human beings as machines at our peril: Dehumanizing each other and treating each other as tools instead of as colleagues and (at least potential) friends inevitably leads to the breakdown of all that is positive and healthy in any social grouping.

NOTES

- 1 [Checkster Better Talent Decisions \(2020\).](#)
- 2 [U.S. Equal Employment Opportunity Commission \(2021\).](#)
- 3 [Ladimeji \(2015\).](#)
- 4 [Lawyer \(2020\).](#)
- 5 [Bishop \(2011\).](#)
- 6 [Johnston \(2021\).](#)
- 7 [Thmoson Reuters \(2021\).](#)
- 8 [ContractsCounsel \(2021\).](#)
- 9 [Legal Information Institute \(2021\).](#)
- 10 [Merriam-Webster \(n/a\).](#)
- 11 [Rose \(2021\).](#)
- 12 [U.S. Federal Trade Commission \(2023\).](#)
- 13 [McLeod \(2021\).](#)
- 14 [U.S. Bureau of Labor Statistics \(2021\).](#)
- 15 [U.S. News & World Report \(2021\).](#)
- 16 [U.S. National Security Agency \(2021\).](#)
- 17 [Renee \(2021\).](#)
- 18 [National Initiative for Cybersecurity Careers and Studies \(2023\).](#)
- 19 [Kabay and Robertson \(2014\).](#)
- 20 [American Polygraph Association \(2010\).](#)
- 21 [U.S. National Academies of Sciences, Engineering & Medicine \(2003\).](#)
- 22 [Behavioural Measures Companies \(2021\).](#)
- 23 [U.S. Department of Justice \(2006\).](#)
- 24 [U.S. Code \(1988\).](#)
- 25 [U.S. Code \(1998\).](#)
- 26 [American Polygraph Association \(2006\).](#)
- 27 [Farah and Wolfe \(2004\).](#)
- 28 [Kozel et al. \(2004\).](#)
- 29 [Orenstein \(2005\).](#)
- 30 [Silberman \(2006\).](#)
- 31 [Ireland, C. \(2007\).](#)
- 32 [NO LIE MRI \(2006\).](#)
- 33 [University of Plymouth \(2019\).](#)
- 34 [SolveXia \(2020\).](#)
- 35 [Dutton and Watts \(2011\).](#)
- 36 [Chun \(2018\).](#)
- 37 [Behr and Coleman \(2017\).](#)
- 38 [Beattie \(2020\).](#)
- 39 [Kłosowski \(2021\).](#)
- 40 [U.S. Health & Human Services \(2022\).](#)
- 41 [United States Courts \(2022\).](#)
- 42 [U.S. Internal Revenue Service \(2022\).](#)
- 43 [Intersoft Consulting \(2018\).](#)
- 44 [Norwich University \(2021\).](#)

- 45 EuroCAUCE (2010).
- 46 Kabay, DISINTERMEDIATION links (2019).
- 47 Khan (2021).
- 48 Great Lakes Psychology Group (2020).
- 49 Lock (2021).
- 50 Jeans (2021).
- 51 Feuer (2021).
- 52 U.S. Cybersecurity & Infrastructure Security Agency (n/a).
- 53 Friedman (2021).
- 54 Borysenko (2018).
- 55 Kurtel (2020).
- 56 Segal (2021).
- 57 Business Owner's Toolkit (2012).
- 58 Mueller (2006).
- 59 QuickMBA (2010).
- 60 Falkowitz (2018).

WORKS CITED

- American Polygraph Association. (2006, October 2). *Model Policy for Law Enforcement Pre-Employment Polygraph Screening Examinations*. Retrieved October 4, 2021, from American Polygraph Association: <https://web.archive.org/web/20061002130651/http://www.polygraph.org/modelpolicy-preemployment.htm>
- American Polygraph Association. (2010). *Frequently Asked Questions*. Retrieved October 4, 2021, from American Polygraph Association: <https://www.polygraph.org/polygraph-frequently-asked-questions>
- Beattie, A. (2020, March 22). *How Did Nick Leeson Contribute to the Fall of Barings Bank?* Retrieved October 6, 2021, from Investopedia | Business | Company Profiles: <https://www.investopedia.com/ask/answers/08/nick-leeson-barings-bank.asp>
- Behavioural Measures Companies. (2021). *Why Do Critics Figures Vary?* Retrieved October 4, 2021, from Behavioral Measures Companies | Polygraph: <http://behavioralmeasures.com/polygraph/why-do-critics-figures-vary/>
- Behr, A., & Coleman, K. (2017, August 3). *Separation of Duties and IT security*. Retrieved October 6, 2021, from CSO United States | Industry | Government: <https://www.csoonline.com/article/2123120/separation-of-duties-and-it-security.html>
- Bishop, J. (2011, April 14). *Giving a Reference Could Get You Sued*. Retrieved October 3, 2021, from Dynamic Business: <https://dynamicbusiness.com/topics/small-business-resources/legal/giving-a-reference-could-get-you-sued-1442011.html>
- Borysenko, K. (2018, December 3). *Why You Should Stop Firing People Around the Holidays*. Retrieved September 19, 2023, from Forbes: <https://www.forbes.com/sites/karlynborysenko/2018/12/03/why-you-should-stop-firing-people-around-the-holidays>
- Business Owner's Toolkit. (2012, May 24). *Protecting Business Information Through Confidentiality and NonCompete Agreements*. Retrieved October 11, 2021, from Business Owner's Toolkit | Office-HR | Managing the Workplace: <https://web.archive.org/web/20131015061656/http://www.bizfilings.com/toolkit/sbg/office-hr/managing-the-workplace/confidentiality-and-noncompete-agreements.aspx>
- Checkster Better Talent Decisions. (2020, February 7). *Is Your Company Hiring Charlatans? A Study of Ethical Standards in the Hiring Process*. Retrieved October 3, 2021, from Checkster: https://www.checkster.com/are_you_hiring_charlatans
- Chun, R. (2018, October). *A Shocking Number of Killers Murder Their Co-Workers: Homicide Is the Third-Most-Prevalent Cause of Workplace Death*. Retrieved October 6, 2021, from The Atlantic: <https://www.theatlantic.com/magazine/archive/2018/10/the-killer-in-the-cubicle/568303/>
- ContractsCounsel. (2021). *Employment Agreement*. Retrieved October 3, 2021, from ContractsCounsel | Types of Contracts: <https://www.contractscounsel.com/t/us/employment-agreement>
- Dutton, R., & Watts, W. H. (2011). *Who Was 'Nosey' Parker?* Retrieved October 6, 2021, from Guardian | Notes & Queries: <https://www.theguardian.com/notesandqueries/query/0,-1469,00.html>
- EuroCAUCE. (2010, August 23). *Opt-In vs. Opt Out*. Retrieved October 11, 2021, from EuroCAUCE: <https://web.archive.org/web/20100823030853/http://www.euro.cauce.org/en/optinvsout.html>

- Falkowitz, R. (2018, October 6). *People Are Not Fungible*. Retrieved December 13, 2021, from <https://www.3cs.ch/people-not-fungible/>
- Farah, M., & Wolfe, P. R. (2004, May). *Monitoring and Manipulating Brain Function: New Neuroscience Techniques and Their Ethical Implications*. Retrieved October 4, 2021, from University of Pennsylvania | Bioethics: https://web.archive.org/web/20070711032016/http://www.bioethics.upenn.edu/pdf/wolpe_hastings.pdf
- Feuer, W. (2021, December 10). *Better.com Hikes Severance Pay as Ex-workers Explore Lawsuit*. Retrieved December 13, 2021, from New York Post | Business: <https://nypost.com/2021/12/10/better-com-hikes-severance-pay-as-ex-workers-explore-lawsuit/>
- Friedman, M. S. (2021, January 14). *Don't Let These 10 Legal Myths Stop Your Doing Business in the U.S.: Myths #6 and 7 – The U.S. Is Very Litigious and That Is Too Threatening to a Small Company Like Ours*. Retrieved October 11, 2021, from European American Chamber of Commerce: <https://eacny.com/news/member-news/dont-let-these-10-legal-myths-stop-your-doing-business-in-the-u-s-myths-6-and-7-the-u-s-is-very-litigious-and-that-is-too-threatening-to-a-small-company-like-ours-as-a-result-the-risk/>
- Great Lakes Psychology Group. (2020, October 27). *The 5 Stages of Grief*. Retrieved October 11, 2021, from <https://www.greatlakespsychologygroup.com/blog/5-stages-grief/>
- Intersoft Consulting. (2018, May 25). *General Data Protection Regulation*. Retrieved September 19, 2023, from GDPR-Info: <https://gdpr-info.eu/>
- Jeans, D. (2021, December 10). *Better.com CEO – Who Fired 900 Workers On Zoom Call – Taking Leave 'Effective Immediately'*. Retrieved December 13, 2021, from Forbes | Editors' Pick: <https://www.forbes.com/sites/davidjeans/2021/12/10/bettercom-ceo-vishal-garg-leave-effective-immediately/>
- Johnston, K. (2021). *Can an HR Department Refuse to Give References?* Retrieved October 3, 2021, from CHRON | Small Business | Managing Employees | Managers: <https://smallbusiness.chron.com/can-hr-department-refuse-give-references-62430.html>
- Kabay, M. E. (2019, August 4). *DISINTERMEDIATION links*. Retrieved October 11, 2021, from M. E. Kabay | Courses | Academic | Norwich | CS407 | Resources | DISINT: http://www.mekabay.com/courses/academic/norwich/cs407/cs407_resources/cs407_links.htm
- Kabay, M. E., & Robertson, B. (2014). Employment practices and policies. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (6th ed., Vol. 2, pp. 45–145–18). Hoboken, NJ, USA: John Wiley & Sons, Inc. Retrieved October 4, 2021, from <https://smile.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Khan, A. (2021, September 3). *Credit Union Employee Gets Fired, Destroys 21GB Of Important Data*. Retrieved October 11, 2021, from Wonderful Engineering: <https://wonderfulengineering.com/credit-union-employee-gets-fired-destroys-21gb-of-important-data/>
- Klosowski, T. (2021, September 6). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. Retrieved September 19, 2023, from New York Times | Wirecutter: <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>
- Kozel, F. A., Revell, L. J., Lorberbaum, J. P., Shastri, A., Elhai, J. D., Horner, M. D., ... George, M. S. (2004, August 1). A pilot study of functional magnetic resonance imaging brain correlates of deception in healthy young men. *Journal of Neuropsychiatry and Clinical Neurosciences*, 16(3), 295–305. <http://doi.org/10.1176/jnp.16.3.295>
- Kurter, H. L. (2020, January 21). *4 Things You Didn't Know About Non-Disclosure Agreements*. Retrieved October 11, 2021, from <https://www.forbes.com/sites/heidilynnkurter/2020/01/21/4-things-you-didnt-know-about-non-disclosure-agreements/>
- Ladimeji, K. (2015, April 15). *Expecting a Bad Reference from Your Former Employer?* Retrieved October 3, 2021, from Recruiter: <https://www.recruiter.com/i/expecting-a-bad-reference-from-your-former-employer/>
- Lawyer, U. (2020, June 18). *Employee Rights: Can I Sue My Former Employer for Giving Bad References?* Retrieved October 3, 2021, from ToughNickel: <https://toughnickel.com/business/Employee-Rights-Can-I-Sue-My-Former-Employer-For-Giving-Bad-References>
- Legal Information Institute. (2021). *Trade secret*. Retrieved October 3, 2021, from Cornell Law School | LII | Wexlaw: https://www.law.cornell.edu/wex/trade_secret
- Lock, S. (2021, December 7). *'Not Great News': US Boss Fires 900 Employees on a Zoom Call*. Retrieved December 13, 2021, from The Guardian | US news: <https://www.theguardian.com/us-news/2021/dec/07/not-great-news-us-boss-fires-900-employees-on-a-zoom-call>
- McLeod, S. (2021). *Theories of Personality*. Retrieved October 4, 2021, from SimplyPsychology | Personality Theories: <https://www.simplypsychology.org/personality-theories.html>
- Merriam-Webster. *Personality*. Retrieved October 4, 2021, from Merriam-Webster Dictionary: <https://www.merriam-webster.com/dictionary/personality>

- Mueller, C. (2006, January 18). *Non Compete Agreement: How Does A Non Compete Clause Affect You?* Retrieved October 11, 2021, from Ezine Articles | Business | Careers Employment: <https://web.archive.org/web/20180527125022/https://ezinearticles.com/?Non-Compete-Agreement:-How-Does-A-Non-Compete-Clause-Affect-You?&id=130644>
- National Initiative for Cybersecurity Careers and Studies. (2023, September 14). *Cybersecurity Scholarships*. Retrieved September 19, 2023, from NICCS | Education & Training: <https://niccs.cisa.gov/education-training/cybersecurity-scholarships>
- New York Times. (1981, August 11). *Ex-Wells Fargo Aide Admits Embezzlement Role*. Retrieved October 6, 2021, from New York Times: <https://www.nytimes.com/1981/08/11/us/ex-wells-fargo-aide-admits-embezzlement-role.html>
- Nigrini, M. J. (2014, August). *Lessons From an \$8 Million Fraud: What the Criminal Was Thinking and What Can Be Done to Prevent or Uncover Similar Crimes*. Retrieved September 19, 2023, from Journal of Accountancy | Feature | Fraud: <https://www.journalofaccountancy.com/issues/2014/aug/fraud-20149862.html>
- NO LIE MRI. (2006). *Process Overview*. Retrieved October 4, 2021, from NO LIE MRI: <https://web.archive.org/web/20061218130921/http://noliemri.com/products/ProcessOverview.htm>
- Norwich University. (2021). *Our Privacy Policy*. Retrieved October 7, 2021, from Norwich University Online | About Us: <https://online.norwich.edu/about-us/privacy-policy>
- Orenstein, B. W. (2005, May 16). Guilty? Investigating fMRI's future as a lie detector. *Radiology Today*, 6(10), 30. Retrieved October 4, 2021, from https://web.archive.org/web/20060423100556/http://www.radiologytoday.net/archive/rt_051605p30.shtml
- QuickMBA. (2010). *Employment Law and Duties to One's Former Employer*. Retrieved October 11, 2021, from QuickMBA | Business Law | Employment Law: <http://www.quickmba.com/law/empl/>
- Renee, M. (2021). *Things to Say When Placing an Employee on Probation*. Retrieved October 4, 2021, from CHRON | Small Business | Managing Employees | Employees: <https://smallbusiness.chron.com/mitigate-wrongful-termination-claims-60433.html>
- Rose, V. (2021, March 12). *Preventing and Addressing Cross Cultural Conflict in the Workplace*. Retrieved October 4, 2021, from PollackPeaceBuilding | Communication Skills | Tips & Advice on Conflict Resolution | Workplace Conflict: <https://pollackpeacebuilding.com/blog/cross-cultural-conflict-in-the-workplace/>
- Segal, E. (2021, July 9). *How Biden's Proposed Ban on Non-Compete Agreements Would Impact Companies*. Retrieved October 11, 2021, from Forbes | Editors' Pick: <https://www.forbes.com/sites/edwardsegal/2021/07/09/how-bidens-proposed-ban-on-non-compete-agreements-would-impact-companies/>
- Silberman, S. (2006, January 1). *Don't Even Think About Lying: How Brain Scans Are Reinventing the Science of Lie Detection*. Retrieved October 4, 2021, from WIRED: <https://www.wired.com/2006/01/lying/>
- SolveXia. (2020, June 24). *What Is Continuous Process Improvement?* Retrieved October 6, 2021, from <https://www.solvexia.com/blog/what-is-continuous-process-improvement>
- Thmoson Reuters. (2021). *Golden Handshake*. Retrieved October 3, 2021, from Thmoson Reuters Practical Law | Glossary: <https://uk.practicallaw.thomsonreuters.com/1-107-6654>
- U.S. Internal Revenue Service. (2022, November 16). *Taxpayer Bill of Rights 8: The Right to Confidentiality*. Retrieved September 19, 2023, from IRS | Newsroom: <https://www.irs.gov/newsroom/taxpayer-bill-of-rights-8>
- U.S. Bureau of Labor Statistics. (2021, September 8). *Computer and Information Technology Occupations*. Retrieved October 4, 2021, from Bureau of Labor Statistics | Publications | Occupational Outlook Handbook: <https://www.bls.gov/ooh/computer-and-information-technology/home.htm>
- U.S. Code. (1988, June 27). *Employee Polygraph Protection Act of 1988 (29 USC 2001)*. Retrieved October 4, 2021, from Legal Information Institute: https://www.law.cornell.edu/topn/employee_polygraph_protection_act_of_1988
- U.S. Code. (1998, October 1). *3 U.S. Code § 414 - Rights and Protections Under the Employee Polygraph Protection Act of 1988*. Retrieved October 4, 2021, from Legal Information Institute: <https://www.law.cornell.edu/uscode/text/3/414>
- U.S. Cybersecurity & Infrastructure Security Agency. *Insider Threat - Cyber*. Retrieved October 11, 2021, from CISA | Infrastructure Security | Insider Threat Mitigation: <https://www.cisa.gov/insider-threat-cyber>
- U.S. Department of Justice. (2006). *Use of Polygraph Examinations in the Department of Justice*. Office of the Inspector General, Evaluation and Inspections Division. Retrieved October 4, 2021, from <http://www.usdoj.gov/oig/reports/plus/e0608/final.pdf>
- U.S. Equal Employment Opportunity Commission. (2021). *Pre-Employment Inquiries and Arrest & Conviction*. Retrieved October 3, 2021, from eeoc: <https://www.eeoc.gov/pre-employment-inquiries-and-arrest-conviction>

- U.S. Federal Trade Commission. (2023). *Protections Against Discrimination and Other Prohibited Practices*. Retrieved September 19, 2023, from FTC | Policy-Notices | No-Fear Act | Protections Against Discrimination: <https://www.ftc.gov/policy-notices/no-fear-act/protections-against-discrimination>
- U.S. Health & Human Services. (2022, October 19). *Summary of the HIPAA Privacy Rule*. Retrieved September 19, 2023, from HHS | HIPAA | Privacy | Lws & Regulations: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
- U.S. National Academies of Sciences, Engineering & Medicine. (2003). *The Polygraph and Lie Detection*. National Academies of Sciences. Retrieved October 4, 2021, from National Academies Press: <https://www.nap.edu/catalog/10420/the-polygraph-and-lie-detection>
- U.S. National Security Agency. (2021). *National Centers for Academic Excellence in Cybersecurity*. Retrieved December 13, 2021, from NSA | Academics: <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/>
- U.S. News & World Report. (2021). *Best Undergraduate Computer Science Programs Rankings*. Retrieved December 13, 2021, from U.S. News | Education | Colleges: <https://www.usnews.com/best-colleges/rankings/computer-science-overall>
- United States Courts. (2022, December 16). *Congress Passes the Daniel Aderl Judicial Security and Privacy Act*. Retrieved September 19, 2023, from US Courts | News: <https://www.uscourts.gov/news/2022/12/16/congress-passes-daniel-anderl-judicial-security-and-privacy-act>
- University of Plymouth. (2019, May 3). *Brain imaging lie detector can be beaten with simple techniques*. Retrieved October 4, 2021, from ScienceDaily: <https://www.sciencedaily.com/releases/2019/05/190503100810.htm>
- Vijayan, J. (2000, November 20). *Fault-Tolerant Computing*. Retrieved December 13, 2021, from COMPUTERWORLD | Retail Industry: <https://www.computerworld.com/article/2589674/fault-tolerant-computing.html>

11 Operations Management in IT

In general, *operations management* is devoted to ensuring that mission-critical functions and infrastructure functions work smoothly, efficiently and effectively in any organization.¹

Mission-critical functions (MCFs) are those directly related to the goals of the organization. For example:

- Hospital MCFs include emergency services, patient registration, patient care, pharmacy supplies, specialized departments such as radiology, and so on.
- Manufacturing MCFs include supply-chain management, equipment, order-entry, quality control, and so on.
- University MCFs include teacher management, course design, institutional certification, evaluations, and so on.

Infrastructure functions (IFs) are those that support the MCFs. For example, IFs for hospitals, manufacturing plants, and universities all include human-resources functions, building maintenance, accounting, legal departments, quality assurance, information technology, helpdesks, computer security, disaster-recovery planning, and so on.

This section concentrates on effective operations of IT departments:

- The value of documentation
- Ensuring continuity of operations
- Using vulnerability analysis and intrusion detection to protect critical systems
- Securing public workstations
- Controlling security on purchased equipment
- Preventing security violations when discarding backups
- Security failures at the Los Alamos Laboratory
- Security issues in a famous movie

DOCUMENTATION FOR LESS WORK

Documentation, far from being a sterile exercise done to conform to arbitrary requirements of nameless, faceless bureaucrats, should be a vital part of any intellectual exercise. Documentation is simply writing down what we learn: the crucial step in human history that changed traditional cultures into civilizations.² By keeping a record independent of any specific individual, we liberate our colleagues and our successors from dependence on our physical availability. Documentation is our assurance that work will continue without us: a kind of immortality, if you will.

Documentation is shared knowledge.

We document what we do as a part of systematic problem-solving. Writing forces us to identify the problem in words, instead of being content to define it in vague, unclear ideas. Writing down each idea we are in the process of testing helps us notice the ideas we missed the first time we tackled the problem. Keeping notes helps us pay attention to what we're doing.

OPERATIONS



FIGURE 11.1 Ops management.

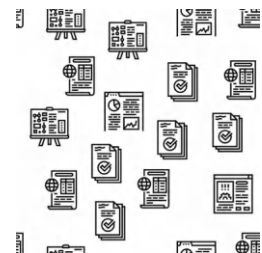


FIGURE 11.2 Documentation is shared knowledge.

Documenting what we do also helps us during training – both our own and that of the people we are helping to learn technical skills. Trainees can review their own notes on how to do something instead of relying entirely on someone else’s description. If taking notes is viewed as a chance to engage one’s mind more thoroughly in what we’re learning, it can be fun. When I studied math as a child, I followed my father’s rule of using a set of symbols entirely different from those the teacher used; it was harder than mere copying, but I sure learned what was going on.

Finally, accurate records can be a boon in legal wrangles. For example, records made long after a problem occurs are worthless in cases such as disputes over termination of employment.³ Such records, if kept consistently, in good times and bad, can be accepted in a court of law as evidence—but only if everything points to a steady pattern of record-keeping as events unfold.

In one case of possible legal conflict that I experienced in my consulting work, upper management seriously considered legal procedures against a supplier for supposed breach of contract. However, their careful records of exactly when meetings were held with whom and with what details permitted us to analyze the problem and resolve the issues by collaboration instead of by confrontation.

THE GREEN LOGBOOK

When I joined *HP (Canada) Ltd.* in 1980, I arrived on the job armed with a green, hard-covered logbook. From my first day as a member of the systems engineering organization, I wrote down what I learned and I logged how I spent my time. When I met clients, I took notes. When I installed new versions of the HP3000 MPE operating system, I kept a chronological record of everything I did, including mistakes. While I taught courses, I kept a list of questions I couldn’t answer right away.

Pretty soon, people began asking me what I thought I was doing – writing a novel?

My colleagues may have been puzzled by what they perceived as a mania for record-keeping, but I was equally astonished that record keeping was not a normal part of their way of doing work. The immediate reason I automatically kept records was my years in scientific research, where logbooks with hard covers, numbered pages, and even waterproof paper were just usual parts of doing serious work. The idea of doing anything of importance without keeping a concurrent record simply didn’t occur to anyone. One could not reproduce an experiment without knowing exactly what sequence one had used in accomplishing the steps. Even adding salts to solutions had to be done in a particular order.

So I just kept on keeping my green logbooks; I found one that I had saved in my library dating from September 1981 through October 1982 and have included a picture of its cover here.

By the time I left HP in 1984, I had trained a few of the younger support personnel to keep careful records, especially while solving problems. They were walking around with green logbooks, too.

They had learned the advantages of documentation.

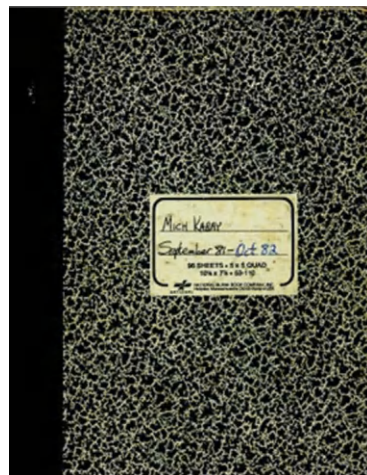


FIGURE 11.3 The green logbook.

KEEP ELECTRONIC RECORDS

The best way of keeping records on specific problems is an easy-to-use DB. Here is the layout of a simple MS-Access DB file I have used in one form or another for forty years (the “notes” field is actually much longer than in this truncated screen copy):

FIGURE 11.4 Electronic records.

The fields shown above are as follows:

- key – keywords such as “Missing key for evidence locker”
- pri – priority (I used 5 for IMMEDIATE, 3 for NORMAL and 0 for DONE)
- on – date started
- by – date closed
- who – primary contact(s)
- what – contact’s organization
- email – primary contact’s email address
- tel – primary contact’s telephone number
- fax – primary contact’s fax number
- select – any key word or value useful for searching the DB
- act_next – concise description of next operation required (by anyone in case)
- maj_acc_last – latest important action (by anyone in case)
- problems – what isn’t going right
- notes – all the details of the steps and interactions, with latest events at the top of the list and the rest sorted downward by date and time.

In no way am I suggesting that this simple design will suit everyone; the point is to encourage everyone to think about storing useful information electronically in an appropriate format for the organization’s needs.

By the time I finished my task of setting up a self-sufficient technical support team in the data center where I was *Director of Technical Services* in Montréal in the mid-1980s, the team was used to logging their support cases (including a unique case identifier). We had two thousand entries archived and instantly available to the entire technical support crew. We had a similar file reserved for system failures and another for summaries of articles from *INTEREX (HP3000 User Group)* proceedings volumes and publications. Every software product we requested information about was logged in the files as well, with a pointer to the folder in which specification sheets and correspondence were stored for the particular entry. These records were in constant use to find data that could help in solving new problems as they arose.

In my personal DB since then, I have stored information that has saved me countless hours' time I would have wasted rediscovering something that I recorded in previous problem-solving sessions. This electronic archive is vastly easier to use than paper records because of the instant FIND function and the ease of fixing mistakes or adding details as necessary.

With easily accessible records, it became possible to solve problems without *me* or any other specific team member. Stored, sharable knowledge meant that it was no longer necessary for staff to depend on the physical presence of any one team member. We were able to take holidays without being called for help by desperate colleagues seeking information that only one person remembered. Part of that freedom from dependence on individuals involved intensive training of the staff, but a good deal was the direct result of proper documentation.

Documentation and the institutional knowledge it creates break the dependency on individuals. Liberate yourselves: share your knowledge.

There are many options for documenting helpdesk cases beyond the simple DB discussed above.⁴ For larger organizations, the features of more sophisticated helpdesk software include easy communications with users, links to human-resources files and vendor files, and compliance with the *Information Technology Infrastructure Library* (ITIL)⁵ standards and their support for *Information Technology Service Management* (ITSM).⁶

INDEXES

Indexes are immensely useful in locating information. Structured indexes can include keywords and specific pointers; unstructured searches can involve special-purpose indexing or brute-force searches.

One form of index that scientists are familiar with but which many business people have not encountered is the *permuted keyword index*. In this technique, one constructs a list such as the titles of a group of articles, but in addition, one shifts the first word to the end and indexes by the second word as well. The cycle continues for all keywords in the titles. For example, consider the titles of the following three articles:

- Computer Envy: Essays on Office Automation
- Facilities Management in the Age of Information Warfare
- Facilities Security

The permuted keyword index might look like this, with a pointer (e.g., a hyperlink) for each entry.

- Age of Information Warfare, Facilities Management in the
- *Automation, Computer Envy*: Essays on Office
- *Computer Envy*: Essays on Office Automation
- *Envy*: Essays on Office Automation, Computer
- *Essays on Office Automation, Computer Envy*:
 - Facilities Management in the Age of Information Warfare
 - Facilities Security
 - Information Warfare, Facilities Management in the Age of
 - Management in the Age of Information Warfare, Facilities
 - Office Automation, Computer Envy: Essays on
 - Security, Facilities
 - Warfare, Facilities Management in the Age of Information

As for unstructured searches, one can always brute-force one's files with the search function of the operating system; however, it is much more efficient to allow the system to create indexes in



FIGURE 11.5 Index.

advance to speed the process of locating files that contain search strings. A search that might take many minutes can be accomplished in seconds.

DocFetcher from *SourceForge*⁷ is an example of software that provides near instantaneous searches on materials on any selected folders on one's disks; the program is available for *Windows*, *Linux*, and *MacOS*. Such products can be set to integrate all changes automatically. They allow not only searches on words in titles but also in the content of the files.

KEEPING TIME SHEETS

I kept time-sheets in my *Day-Timer*[®] starting in 1980 and never regretted the practice. The cost is minor (for example, the two-page per day model I use costs only \$53 a year as of 2021) but the value is high. My practice is to log my activities to the nearest quarter-hour and to mark billable time in red for my consulting clients.

The sheets are immeasurably useful when I am putting together my billings statements; they could also be useful if anyone ever challenged my records and demanded proof that I had actually worked the hours I claimed. Granted, writing the hours down in a paper record does not prove that I am telling the truth, but the consistent pattern, day after day, year after year, would be evidence in my favor.

As you can see in the redacted image above, I even write down what I do for breaks! The fact that the material is written in ink supports the claim that it is a real-time record; the times can also be correlated with electronic records such as the timestamps in electronic mail kept in email files. Finally, the records provide me with a sense of how I am spending my time overall and can also prompt my (failing) memory about times I may have gotten hazy about.

I generally keep the records for at least five years; the 7" × 4.5" × 4.5" (18.5 cm × 11.5 cm × 11.5 cm) boxes take hardly any room in my storage cabinet considering their value to me.

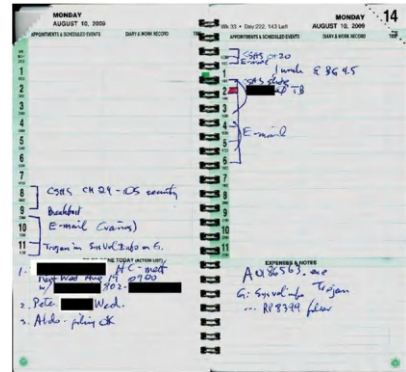


FIGURE 11.6 Paper Day-Timer™.

ALEATORY ALE

One of the most important tools of quantitative risk management is the *annualized loss expectancy* (ALE). The ALE is calculated by using probabilities of events (as the name implied, calculated over a period of a year) and the expected costs associated with those events.

To get a simple illustration of how the ALE works, one can apply it to an insurance or any other loss-management computation. Suppose an insurance-company statistician, called an *actuary*, determines that the likelihood that a particular customer will die in the coming year is about 0.005 (0.5%). For a million-dollar insurance policy, the insurance company is betting the customer that (s)he won't die this year; the customer is betting that (s)he will die this year. If the customer dies, the company will pay the beneficiary \$1M; if (s)he does not die, the insurer keeps all of the premium. Although in reality, the loss to the insurer is the pay-out minus the premium, for simplicity's sake, we can ignore this minor difference in our illustration.

Readers will easily be able to see that with the 0.005/year probability of death, the actuary will be able to calculate a premium of \$5,025.13 as the break-even point for the company (because $0.005 \times -\$1,000,000 + 0.995 \times \$5,025.13 = \$0$). Any premium above \$5,025.13 will make a profit for the company on average for this class of customer and any premium below that amount will, on average, result in losses.

Back to our insurance-company actuary. She knows that the 0.005 probability happens to have been based on (say) 1,000 observations of men of this particular age, health status, occupational



FIGURE 11.7
Probabilities.

status, and other demographic attributes associated with differential mortality. Using standard statistical methods, she can easily compute (as I just did in less than one minute using the well-known *MINITAB* statistical software package)⁸ that the probability of death for this class of customer might be as low as 0.001625 or as high as 0.011629 with a confidence of 95%; i.e., that the calculated interval – what statisticians call the 95% *confidence limits* – would include the real (the *parametric*) population's proportion in 95% of the random samples of 1,000 from the population in question.

Using those numbers, we discover that the break-even points would go down to \$1,627.64 or up to \$11,765.82. So, the actuary would turn the figures over to the financial and marketing experts in the company, who would then evaluate how high they could reasonably put the premium while maintaining their market share – and how low they would be willing to push down the premium given the increasing risks of losses.

What the actuary has done for her company is a *sensitivity analysis*.⁹ I recommend that IA practitioners learn to use sensitivity analysis on all quantitative risk-management techniques that use estimated costs and estimated probabilities. My worry about naïve applications of ALE calculations is that neither the costs nor the probabilities associated with security breaches are known precisely in any given organization or situation. Given the often-large uncertainty (sometimes orders of magnitude) in the numerical values used in these computations, practitioners should apply sensitivity analysis to evaluate the results of such models. As we saw in the insurance example, sensitivity analysis examines the consequences of varying assumptions on the results of numerical models. Rather than assuming that a fixed result of a single calculation should be taken on faith as the basis for making a decision about expenditures, practitioners can make a number of computations using reasonable ranges of probabilities and reasonable ranges of costs. The set of results is typically evaluated using graphical representation and can provide a much more convincing basis for discussion with colleagues than a single estimate with no sense of possible variability or error.

An extension of this manual process is called *Monte Carlo simulation* and can involve thousands of stochastic computations based on underlying probabilistic models for some or all the parameters of a numerical model.¹⁰ Typically we show the results of such aleatory (random) processing as graphs.

CONTINUITY OF OPERATIONS

One of the key principles of *business-continuity planning* (BCP) is to eliminate single points of failure.¹¹

Unless the business keeps its eyes on the principles of BCP, it can easily get itself into a position where it is overly dependent on the services of a few key individuals. Without proper planning, that dependence can result in disaster if one of those key people is not there.¹²

Organizations should develop *succession plans* to cope with the sudden unavailability of key people:

As well as being a good strategy for managing the progression of staff, succession planning is also a good strategy for minimizing the impact on the business of losing a critical member of staff unexpectedly. More broadly it seeks to move the organization to a position where none of its staff actually are critical to its continued operation as individuals.¹³

THE CAPABILITY MATRIX

One of the tools I've long used in evaluating the resilience of organizations is the *capabilities matrix*. One starts by listing (or brainstorming, perhaps using CAC) all the critical functions that the organization requires and all the people in the team. The group then has to decide on a way of rating the capabilities of each person; the figure suggests one way to do it, but in no sense is this suggestion



FIGURE 11.8 Keep the business going.

meant to constrain users. The group can come to a consensus on which of the team members can do which tasks at which level of competence and then examine the overall pattern of skills. Figure 11.9 shows such a matrix with made-up information.

CAPABILITIES MATRIX FOR UNTELECOM CORPORATION										
Total points ≤							Capabilities & Assignments			
	0	1	3	6	9	12	0	1	2	3
EVALUATION	ACK!!!	DANGER!	URGENT	IMPROVE	GOOD	EXCELLENT	NO CAP.	NOVICE	IS/CAN BE BACKUP	CAN BE IN CHARGE
PERSONNEL CAPABILITIES							TOTAL		NEED	
Task	Albert	Betty	Charlie	Dahfla	Edward	Frannie	Golamo	Hur'dath		
application monitoring	3			3			2	2	10	GOOD
application security vulnerabilities	3			3			2	2	10	GOOD
business impact analysis		3		1				2	6	IMPROVE
computer security incident response team			3		3			2	8	IMPROVE
coordination with corporate counsel		3	1		1	2		2	9	GOOD
coordination with human resources group		3	1		1	2		2	9	GOOD
Database performance	1			3			2	3	9	GOOD
Database support	2			3			2	2	9	GOOD
denial-of-service monitoring				1	3			3	7	IMPROVE
denial-of-service response				1	3			2	6	IMPROVE
detect cyber-attacks					3			3	6	IMPROVE
enterprise antivirus								0		ACK!!!
governance decisions		3	1	1		2		2	9	GOOD
identification and authentication			2		2		2	3	9	GOOD
intellectual property protection				2		2		3	7	IMPROVE
intrusion detection systems					3		2	3	8	IMPROVE
intrusion prevention systems			2		3		2	2	9	GOOD
log management systems	1		2	3	3			2	11	GOOD
manage cyber-attacks		2		1	3	2	1	2	11	GOOD
monitor dashboard			2	2	3			2	9	GOOD
network behavior analysis			1	3	2			3	9	GOOD
network discovery			1	2	2			2	7	IMPROVE
penetration testing			1	1	2			3	7	IMPROVE
quality of service measures	1	3		3	1	2		2	12	EXCELLENT
respond to system alarms		2	3	1	3			3	12	EXCELLENT
risk analysis and management				1		3		3	7	IMPROVE
security awareness				1		3		2	6	IMPROVE
security information and event management			3	2				3	8	IMPROVE
service level agreements	2	3	1	3		3		2	14	EXCELLENT
system firewalls			2		3		3	2	10	GOOD
training				1		3		2	6	IMPROVE
unified threat management					3		2	3	8	IMPROVE
vulnerability assessment			2		3		1	2	8	IMPROVE
Web site assessment					2		1	2	5	URGENT
Web site monitoring					3		1	3	7	IMPROVE
wireless intrusion prevention								0		ACK!!!
TOTAL SCORE	13	22	28	42	55	24	23	81		

FIGURE 11.9 Capabilities matrix.

In the spreadsheet I created for this section, I used automatic functions of the spreadsheet function to highlight the danger zones. The red “ACK!!!” flags signal that two functions, “enterprise antivirus” and “wireless intrusion prevention” seem to have been neglected in assignments of duties. Other rows are flagged with other labels such as “DANGER!” up to “EXCELLENT” to give the team suggestions on priorities for improving resilience (overlap of skills) and even identifying experts who can help improve colleagues’ training when indicated by low scores.

In addition to simply identifying lacunae in operational readiness, the rows can also alert the team to potential conflicts. For example, if more than one person is rated at the top of the capabilities (in this example, labeled “CAN BE IN CHARGE”), it’s important to ensure that the actual assignment of duties is crystal clear. One does not want two people *each* thinking that they are in charge (leading to potential conflicts) – or for that matter, that the *other* person is in charge (leaving

the actual responsibility unfilled). Collegial, friendly discussions can resolve such problems and more important, prevent recurrence.

CONTINUITY-OF-OPERATIONS MATRIX

A more detailed application of matrices is the *Continuity-of-Operations Matrix* (COM), a useful technique for organizing information about *who* is capable of doing *what* with what level of *expertise*.¹⁴

First one must prepare a list of all the functions that the organization requires; these are listed in the first column of the spreadsheet. Next one put in a column for every member of the team that is supposed to have shared knowledge. Then one defines an agreed-upon metric to represent how quickly someone can take over the duties for a specific line-item; e.g., one could define the codes as follows:

- 3 = have DONE EXACTLY THIS before
- 2 = could do this with only moderate preparation
- 1 = could do this but only with MAJOR preparation and time investment
- 0 = unlikely to be able to do this even with major preparation

The specific codes are not critically important; they should reflect the approach preferred by the team members. For example, one could use the following codes:

- 3 = can step into the role instantly
- 2 = can start within a day
- 1 = can start within a week
- 0 = can't do this ever.

Figure 11.10 shows an example of such a matrix.

CONTINUITY OF OPERATIONS MATRIX							
< DESCRIPTION OF APPLICATION HERE; E.G., ORGANIZATION >							
ACTIVITY	Personnel / Volunteers						SCORE TOTALS
	Altran	Bartou	Cortuti	Derango	Ertibui	Furdop	
MS-ACCESS database expert/trainer	0	0	0	1	0	1	2
Trainer for canvassing	0	1	0	0	2	0	3
Meeting coordinator	1	0	2	0	1	0	4
Phone-bank manager	0	0	0	1	1	2	4
Fund-raising manager	1	0	0	2	1	1	5
Graphic design	0	0	0	3	1	1	5
Writing white papers	0	1	1	0	3	0	5
Database designer	2	0	3	2	0	2	9
MS-Excel expert/trainer	1	2	0	0	0	3	6
Quicken accounting-software expert/trainer	1	0	1	1	1	2	6
Running errands	1	0	2	1	1	1	6
Accountant	1	1	0	1	0	3	6
Secretary for meetings reports	1	0	3	0	2	1	7
Web designer	1	1	0	2	3	0	7
Copy editor	0	1	0	3	0	2	6
Outreach coordinator	1	1	2	1	1	2	8
Board member	3	1	1	0	2	1	8
Door-to-door canvassing (fund-raising)	2	2	0	1	1	3	9
Office manager	1	1	1	3	0	3	9
Phone bank volunteer	1	1	2	2	1	2	9
Press-release writer	1	0	3	2	0	3	9
MS-WORD expert/trainer	3	0	0	3	3	1	10
Treasurer	3	3	1	1	1	1	10
Door-to-door canvassing (political)	2	3	0	0	3	3	11
Public-relations coordinator	2	1	1	3	3	2	12
Legal counsel	2	1	3	3	3	1	13
Research for white papers	2	0	3	3	2	3	13
Writing flier text	2	3	2	2	1	3	13
Purchasing manager	1	1	3	3	3	3	14
Volunteer manager	3	3	2	1	3	2	14
Volunteer-database manager	3	3	3	1	2	2	14
Web manager	3	1	3	1	3	3	14
AVERAGE SCORE	1.4	1.0	1.3	1.5	1.5	1.8	8.5

FIGURE 11.10 Continuity-of-Operations matrix.

Once the group or the managers have agreed on their scale, every member must fill in the right codes for their response to each function listed in the spreadsheet. The figure below illustrates that approach.

The column totals are also useful. In the made-up example, the automatic color-coding instantly shows that the lowest score is for Albert and the highest score is for Hur'dath. These scores are *not* inherently good or bad: they just point to outliers. For example, perhaps the low-scoring person is a junior member of the team who needs more training to take up more responsibilities; on the other hand, maybe Albert is a slacker who is shunning productive work. Similarly, maybe high-scoring Hur'dath is a senior member of the team who really ought to be thinking about moving to a more senior position – or maybe he's just overworked and due for a heart-attack.

Users must not make the mistake of thinking that this number-heavy approach is somehow going to make decisions for them – the method is just a heuristic tool to help people *think* about the issues, *decide* on solutions, and *act* on their decisions.

Once again, remember the motto I've emphasized to students and colleagues for decades: *Reality overrides theory.*

STOP INFORMATION-HOARDING

One of the principles I've taught for many years in operations-management and security courses can be stated as “No institutional knowledge shall be held by only a single member of the team.” As mentioned in the sections above about using matrices to identify capabilities and support continuity of operations, allowing single repositories of operationally significant knowledge is dangerous. One of the classic examples I cite (I'm sorry that I can't find the specific reference) is of a report published sometime in the late 1980s or early 1990s about a system manager who went on vacation for three weeks on a south-sea island with no external communications. It turned out that critical elements of the operations required knowledge that only he held. The systems were down for the entire period of his holiday.

At one organization where I worked years ago, one of the system managers was a knowledge-hoarder. She kept others from finding out the technical details of how she prevented and solved specific problems, and she refused to document policies so that anyone else could figure out what was permitted and what was not. To find out if something was allowed, the only thing we could do was ask *her*. “Control freak” and “insecurity in action” (in all senses of the word) were kind descriptions for her ham-fisted absolutist control of the production systems.

I interviewed this idiot and she admitted that she concealed information! “Well, I have to make sure I continue to be useful,” she said. I almost suggested that she seek psychiatric help but refrained from risking a lawsuit for harassment. Instead, I had a talk with the president of the organization in which I warned that – as usual – the only question was *when* we would have a disaster, not *if*. Sure enough, a few months after my warnings, the insecure (in every sense) system manager allowed a server to become infected with malware just before she left for the weekend, spreading the toxic code throughout the network. The incident served to demonstrate that not only was she preventing others from taking appropriate security and management precautions, she was actually preventing herself from having her own errors spotted by helpful colleagues.



FIGURE 11.11 Hoarding.

BUSINESS DISCONTINUITY

My old friend Stacy and I were chatting one day about the parlous state of her company's BCP. [All details changed to protect the guilty.] Stacy worked in a sizable manufacturing plant where they made left-handed gzornoplatzes for the export trade. She was one of the sales managers there and supervised 50 sales, of whom about 15 were usually in the office at any one time (the rest were on the road visiting customers except on meeting days).

It seems that a couple of weeks before, electricity had failed at around nine o'clock on a Monday morning. All of the company servers were safely connected to UPSs,¹⁵ so there was no damage to the equipment or to the data. The UPSs allowed a graceful shutdown, but there was insufficient power for continued operation. The mains power came back at about 1100 that morning but the servers stayed down until 1300 that afternoon.

Stacy called the helpdesk to find out what happened: why weren't the servers coming back up now that the power was restored? The answer shocked Stacy even though she was not by any means a technically sophisticated person; she was, however, smart. Here is what she learned.

The servers were not allowed to come back online because the batteries on the UPSs were drained. It took another two hours to recharge them; therefore, the servers were down until 1300. The only allowed source of power was through those UPSs – connection to the mains was deemed unacceptable because of the poor quality of the supplied power.

And why were there no secondary UPSs or even just power conditioners¹⁶ that would at least have permitted safe connection to the mains? Nobody knew.

What about an emergency electric generator?¹⁷ That would support continuous operation. Well, it seems that the IT managers had asked many years before for an emergency electric generator that could kick in quickly when power failures lasted more than a few minutes, thus allowing servers to stay online. Since all of the sales staff were equipped with laptop computers, they had at least a few hours of self-contained power that would allow them to work even without mains power in the office as long as they had access to the DBs and Microsoft Exchange email server. The off-site sales employees could also continue working as long as the network servers were accessible. So it seemed clear to the IT staff using elementary risk analysis that maintaining the continuity of service of their servers ought to be a high priority for the factory. They wrote up their proposal for an emergency generator and the appropriate isolation switches and waited for approval of the relatively moderate outlay (around \$50,000 capital cost).

Unfortunately, their analysis was initially rejected by the factory directors. The factory was still largely under the control of old-time entrepreneurs who had founded and grown the business as a family enterprise a generation before. They were used to taking risks and they didn't like the size of the proposed expenditure, especially for what they perceived as secondary issues such as office work. How could access to computers possibly be mission-critical?

The IT department persevered, however, and after a couple of years they finally got upper management approval for purchase of an emergency generator. Unfortunately, Stacy also learned through the grapevine that the founder's son-in-law had a fit about installing the generator on the roof, which had been identified as the best location for the generator. The scuttlebutt was that he thought it was so hideous that it would make the factory building looked too ugly. He therefore prevailed on the board of directors to maintain the generator as a portable device on a trailer and drag it next to the IT department only when required. This process usually took a couple of hours and was dependent on a single employee who knew how to hook up the generator – and he wasn't always around. As a result, the generator they bought was almost never used.

In addition to the sales staff who were inconvenienced by the server downtime, several hundred other employees dependent on their desktop computers (the ones without batteries) were completely



FIGURE 11.12
Failure.

down during the four hours of system unavailability. There was absolutely no provision for providing emergency power to those employees. The factory didn't even have a contingency plan to allow them to respond to customer phone calls; in fact, their digital *public branch exchange* (PBX) was on the same UPSs as their servers, so they lost outgoing phone service, inbound phone service, and voicemail all at the same time – not exactly great for the company's public image.

Stacy said that the worst part of the whole situation was that nobody in the upper management gave the slightest indication that they were even aware of the problem.

The remainder of the analysis is left to the readers.

VAs AND IDSs

Vulnerability-Assessment (VAs) & IDSs are software or hardware designed to automate surveillance of computers and networks. They collect and analyze records of system and network activity for evidence of security violations.

IDSs can be configured to detect successful intrusions such as unauthorized penetrations of security barriers; they can also detect attacks such as unsuccessful intrusions and DoS attacks.

In contrast, VASs are designed to look for *known* vulnerabilities. VASs scan computer and network security systems and compare gathered data with compilations of standards to spot weaknesses in security configurations. VASs usually run periodically and produce reports, whereas most IDSs run all the time and produce alerts immediately when they notice anomalies.¹⁸

VASs can be useful when new programs are installed, after significant changes are made to software or network configurations, and during or after security incidents. Both VASs and IDSs fit into security management by supporting auditability; they provide information for independent reviews of system records, adequacy of security controls, and compliance with policy and procedures. Their data not only help detect previously unnoticed breaches of security but also help guide changes in security arrangements and in incident handling and recovery plans.

VASs and IDSs are valuable in security management because they document existing threats and help build baseline information for improved risk analysis and risk management. IDSs in particular can detect early stages of possible attacks such as port scans and probes; with appropriate response in place, such information is valuable in helping managers take immediate steps to forestall the anticipated attacks.

IDSs can also supply forensic evidence useful in prosecuting crimes. Most important is that IDS installation on the *outside* of a firewall and also on the *inside* of a firewall provides real-time information on *firewall failures*. If there are 1,000 attacks registered by the IDS on the outside and none by the IDS on the inside, all is likely to be well. Any successful intrusions through the firewall recognized by the inside IDS must stimulate immediate action to analyze the weakness in the perimeter.

On another level, VASs can be useful in training network-security staff. They can serve as an element of quality assurance, such as after the installation of major operating-system upgrades. However, all such applications depend on having the VAS kept up to date; out-of-date VAS will miss newly-discovered but potentially disastrous vulnerabilities and may even contribute to an unjustified and misleading confidence in inadequate security measures.

On the negative side, VASs can be used by attackers as well as by defenders. Some open-source tools are available on the Internet to anyone who wants them and can be applied, at least to some extent, against poorly defended sites to detect specific vulnerabilities that can then be exploited by attackers.

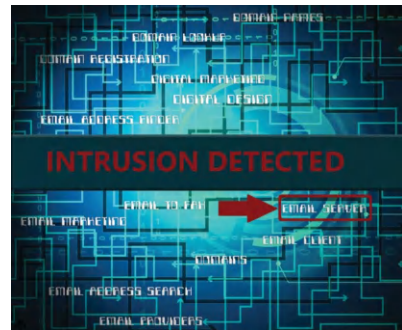


FIGURE 11.13 Detection!.

DEPLOYMENT

IDS sensors can be located anywhere that is interesting to attackers and to defenders. Thus one can install IDS outside the main perimeter firewall, in the *demilitarized zone* (DMZ) between the outer firewall and internal firewalls (the typical location of Web servers), behind internal firewalls, and inside critical subnets in a complex topology that segregates sections of the intranet from each other for security reasons.

The most important rule when installing an IDS is that you must *not* rush the installation. You should let the system accumulate knowledge of normal usage patterns so that you can keep false alarms to a minimum.

Now, defining normal behavior is not as easy as it sounds – a problem that I’m sure parents of teenagers have discovered for themselves. IDSs use *statistical* or *artificial-intelligence* techniques (these are not equivalent, by the way) to spot deviations from the norm; therefore, definition of the norm – what is expected, repeatable, authorized, unexceptional, and unexceptionable – becomes a critical phase in the deployment of these tools. Put another way, it is important *not* to allow the baseline to include unexpected, rare, unauthorized, and exceptional events into the standard data set.

Ah, but here comes a very serious problem indeed: just how are we to prevent such inclusion of nasty data if there is already criminal activity going on inside the network or if there are attacks in progress while the data are being collected? How would one know that these data were being included in the baseline? This is not a trivial problem: we’re talking about a fundamental difficulty here. If we have no particular expertise in detecting attacks and that’s why we are installing an IDS, then how do we tell if the baseline data are contaminated by attacks and internal shenanigans?

I think that one approach to resolving what could become an impasse – a double bind – is to hire outside experts if necessary. Use the services of a managed-security company to establish that the baseline data are in fact acceptable and safe so that the IDS is initialized with clean data. These experts will work with you to verify that you aren’t setting yourselves up with the equivalent of unnoticed back doors through the IDS.

Whether you have external experts involved or handle the initialization (training) phase yourselves, expert this part of the deployment to take weeks or even months to work out the bugs. You’ll not only have to let the system accumulate baseline data as explained above, but also to refine the alarm settings to minimize both false alarms and false negatives (that is, missing real anomalies or attacks). It is appropriate during this wearing-in phase to suspend alarms so that your staff are not constantly kept on edge by erratic reports from the new system. A continuous series of false alarms could not only be disruptive to productivity but could also desensitize your crew so that they simply ignore real alarms later. Finally, this period of adjustment can serve for development and refinement of the computer-emergency response team.

RESPONSE

Responses to intrusion alerts from IDS can be passive, active, or investigative. The IDS can simply announce that there’s a problem and let the users handle the trouble; the IDS produces reports. A more active response still includes human intervention, but the IDS can facilitate a range of actions such as collecting more detailed information about the intrusion or attack; changing the environment to make the attack less likely to succeed; or even (and this is not a good idea) to enable counterstrikes (hack-back) against the perceived attackers.

Automated responses are potentially powerful and therefore potentially dangerous. In the first place, there’s always a danger that any automated system will be misused by people who assume that they don’t



FIGURE 11.14

Deploying
IDS sensors.

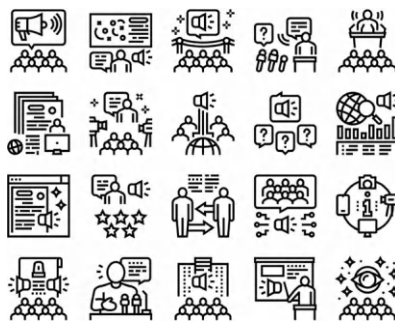


FIGURE 11.15 Responding to
intrusion.

need to tune the parameters to fit their own requirements. These are the folks who install factory defaults on their firewalls and IDSs without even reading the instruction manuals to verify that the defaults actually do something. I remember that in the early days of the old *NCSA's Firewall Product Developers' Consortium* around 1995,¹⁹ we (I was the Secretary of the *Consortium*) hammered away at the concept that default settings on security products should actually provide reasonable security if we were expected to certify the products as having value. At that time (the mid-1990s), some firewall default installations resulted in a bandwidth reduction: the default settings for the firewall didn't actually do very much except put an upper limit on the bandwidth of the communications channel where it was installed.

The second danger from automated responses is that they can sometimes be abused by attackers to create DoS attacks. The classic example of how a well-intended security policy can easily be subverted is the automatic inactivation of accounts when there are more than a critical number of bad passwords supplied in a sequence (e.g., six bad passwords in a row). Some system managers configure their security parameters to lock the account in question automatically and require an administrator to reset the password or the account to allow access. Sounds good – online password crackers cannot possibly achieve their goals with only six (or whatever small number one wants) tries per account.

No, they may not be able to penetrate the system, but they sure can shut it down.

The attack need merely obtain (or guess at) a list of valid account names and then give each account a bad password enough times and the entire system can be locked up. And woe betide the system administrator who allows the automatic lockout to apply to the *root* user as well: then you can *really* have headaches.

By the way, the same goal – slowing down automated online password cracking – can be achieved simply by introducing a modest delay (e.g., a few seconds) after the magic number of bad passwords. Some systems double the delay after each bad guess; one second, two seconds, four seconds and so on. Such approaches *must* set an upper limit, however; for example, the longest delay could be, say, 32 seconds. True, it is possible to inactivate lots of accounts temporarily by bombarding the system with fraudulent logons under such a regime, but it's much harder to lock it up completely and it's still almost impossible to stumble on the right passwords.

So back to IDSs and automated responses: some systems are available today that provide active response to attacks. They not only alert system administrators to attack, they actually deflect attacks before the firewalls can become overloaded. This is a good thing, but one should nonetheless monitor the activity carefully. An attacker could, for example, spoof the originating IP addresses in the flood of attack packets and thus cause the IDS to begin rejecting *legitimate* traffic from specific origins. This might be a minor consideration on an e-commerce site with public utilization, but it could be a disaster for a controlled trading network (an extranet) forming the basis for tightly-coupled supply-chain management or customer-relationship management.

Again, to be sure I'm not being misunderstood (and to avoid angry messages from offended vendors): automated response tools are good – they should simply not be allowed to function unsupervised for extended periods. A human being should take action to understand what's happening as soon as there's an alarm from the IDS to prevent manipulation of the responses that could turn them into self-inflicted denial of service.

HACKBACK AS REVENGE

There's a long-standing debate, mostly underground and informal, about how satisfying it would be to strike back at criminal hackers, industrial spies, saboteurs, and other bad-dies who have the nerve to attack our systems. People have speculated about counter-flooding, using buffer-overflow attacks, sending "explosive" HTML code that could cause system freezes, and so on. Much of this talk is really just good-natured fun – more along the lines of "wouldn't it be

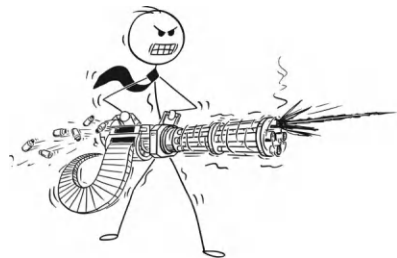


FIGURE 11.16 Revenge.

nice if” than actually serious proposals for corporate responses. But to be absolutely sure that all of the readers of this section, at least, have a chance to think about it, let me flatly state that any such counterattacks *must be formally forbidden* by corporate policy.

First, although I am not a lawyer and this is not legal advice (for legal advice, consult an attorney with appropriate expertise), as far as I know, there is absolutely no waiver in U.S. law that would exculpate anyone who gains unauthorized access to other people’s computer systems. In particular, the *Computer Fraud and Abuse Act of 1986* (18 USC §1030), the *Unlawful Access to Stored Communications Act* (18 USC §2701), and the *Electronic Communications Privacy Act of 1986* (18 USC §§1367, 2232, 2510 and several other sections) do not make any allowance for revenge attacks. Investigation of such crimes (the revenge attacks) could involve the seizure of equipment as evidence.

Second, because IPv4 provided inadequate authentication of packets, it was difficult or impossible to prove the exact origin of DoS attack packets or even of packet streams used in attack sessions. Attacking the wrong target would be an unmitigated disaster. However, the much stronger IPv6 is now increasingly used, providing better authentication of packet sources.²⁰

Third, many attackers subvert poorly-secured intermediary systems to launch their attacks; attacking these hosts would damage other victims but cause no direct harm to the real attackers.

Fourth, unauthorized penetration of anyone’s computer systems and networks can lead to civil lawsuits for damages; even if the lawsuits are unsuccessful, they can rack up expensive attorneys’ fees and also cause expensive computer equipment to be seized as evidence under subpoena.

No, although it might seem like a satisfying tactic that would be the geek equivalent of innumerable Steven Seagal²¹ and Jean-Claude Van Damme²² movies, trying to strike back at attackers through illegal means is a thoroughly bad idea.

Despite these long-standing arguments, there is some agitation from some legislators to provide legal avenues for hackback. Proponents of the *Active Cyber Defense Certainty Act* (ACDCA) introduced in the U.S. Congress in 2017 and returned to the news in 2019²³ have proposed

- Allowing *beacons* that would allow stolen data to install software to send signals allowing identification of the system where the stolen data are stored.
- Providing legal protection for victims who attack the criminals’ systems.²⁴

Such allowances seem to be assuming perfect identification of the source of criminal cyberattacks – still not guaranteed despite the availability of IPv6. Critics of the legislation have also pointed out that these U.S. proposals would cause serious legal and diplomatic problems if the counterattacks were directed internationally.²⁵

FALSE ALARMS

At about 0400 on Sunday 11 May 2003, a thief climbed up some temporary scaffolding on the *Vienna Art History Museum*, entered the Museum through a second-story window, broke the unprotected glass display case, and stole the famous gold and enamel salt-cellar by Renaissance genius Benvenuto Cellini. This unique work of art was valued *pro forma* at about U\$65M (although it could not possibly be sold on the open market because all legitimate dealers would have known it had been stolen).

Now for the interesting parts from a network security standpoint. Ian Traynor, reporting in *The Guardian*, wrote,



FIGURE 11.17 Alarm turned off.

Entry to escape ... can have taken no more than 54 seconds, according to a police reconstruction. Halfway through that brief period the museum’s alarm system rang. The guard switched it off – before it could have

alerted the police – assuming that it was yet another false alarm of the type that occurs in the museum once a week on average. It was left to a cleaning lady to discover the theft more than four hours after the event.²⁶

An *alarm* is any signal that alerts people to some unusual or unexpected condition such as smoke, fire, intrusion, power failure, dropping heartrate, failure to breathe, dangerous blood sugar levels, and so on. In the following discussion, by *alarms* I mean *any kind of alarm*, including signals from IDS, firewalls, physical-security systems, antimalware systems and so on.

False alarms can occur for several reasons:

- A sensor has been set to excessive sensitivity; e.g., a window vibration sensor is responding to wind gusts by reporting glass breakage.
- A fault in the control system is misinterpreting signals; e.g., a normal voltage or a normal pattern of system activity is erroneously configured as a trigger for an alarm.
- A system failure has led to what has been defined as a condition requiring a response; e.g., mains power has failed and systems are switching to generators or UPS.
- Someone or something is generating abnormal inputs but not completing the attack; e.g., a criminal hacker is deliberately sending patterns of packets associated with attacks (attack *prodromes*) but not carrying out the actual attack.

Inappropriate responses to false alarms are a serious problem in all security systems. For example, I have personally seen people milling about discussing whether to respond to fire alarms. In one case in the 1980s, the alarms went off in the apartment building where I lived. A dozen people gathered around the security panel at the main entrance/exit debating what to do. “Do you think it’s a false alarm?” some were asking; “Should we leave?” I peremptorily ordered them out of the building while we waited for the fire trucks. I didn’t care if it was a false alarm or not: deciding that should have come after the building was evacuated. The possible benefits from *not* responding to a *false* fire alarm were far outweighed by the possible losses if there really was a fire.

Professionals understand this balance of pros and cons; I remember one incident where several hundred of us security experts were meeting in a hotel when the fire alarm went off; without a word, every single one of us collected his or her laptop computer, briefcase or purse and immediately filed outside without rushing. The hotel staff were astounded: they usually had to cajole their patrons to pay attention to the alarms and sometimes had to argue with people to leave their rooms.

Many untrained people respond to repeated false alarms by discounting all subsequent alarms (the *cry-wolf syndrome* illustrated by the appalling case in the Vienna Art Museum). A better response is to determine *why* the false alarms are occurring and to *fix* the underlying problems. Similarly, some municipal police forces have taken to putting people or businesses on a blacklist to refuse response when their burglar alarms produce more than a threshold number of false alarms. Burglars have exploited this absurd strategy by deliberately causing alarms (e.g., by rattling windows) until their targets are blacklisted, after which they can pillage at will. A better response from police forces is to fine people for excessive false alarms. The penalties pressure people into fixing faulty alarm systems; those who will not or cannot do so have the option of (stupidly) withdrawing from coverage.

Another observation from the *Guardian* story cited above is that the museum director had been “shifting blame for the fiasco on to the security guards, three of whom were suspended from their jobs.” Although it is possible that the guards flagrantly disobeyed instructions, I am skeptical of that scenario. The story mentions that false alarms were a regular occurrence; in that case, I put responsibility for this fiasco squarely on the shoulders of management. No manager should tolerate repeated false alarms without escalating the problem with staff and vendors to fix the problem; in any such situation, all personnel should know that they are to *increase* their responsiveness to all alarms, not make unfounded judgments about whether a particular incident is a false alarm. Incidentally, it is also possible that the guards (or, for that matter, the management) were colluding with the thief, but that’s pure speculation for the sake of completeness in this analysis.

I hope the applicability of these notes to network IDS is clear. False alarms are a serious challenge to security; they are opportunities for exploitation by attackers. Instruct your staff to treat all alarms as if they are real; increase vigilance and responsiveness if false alarms have become common. Find out why false alarms are occurring, especially if they are frequent or increasing in frequency; fix the underlying problem.

ADDITIONAL TOPICS ON OPERATIONS SECURITY

The following sections discuss specific issues worth considering in managing operations.

PROTECTING PUBLIC WORKSTATIONS

A *public workstation* is part of a network for authorized users including employees, students, and clients.

Lisa Napoli wrote an interesting summary of a computer crime involving public workstations that were compromised using keystroke loggers. Apparently a computer criminal installed keystroke-logging software (*Invisible KeyLogger Stealth*) on public Internet terminals at 13 Kinko's copy shops in Manhattan and used user IDs and passwords collected from innocent users of those terminals to break into their computers and their Internet-related accounts for nefarious purposes. After the accused was arrested in December 2002 and confessed to his crimes, he was released on bail and immediately continued his criminal activity. He pleaded guilty in July 2003 to five counts of computer fraud and software piracy.²⁷

The problem of unauthorized software on public terminals is as old as remote access. One of the first pranks or crimes perpetrated on mainframe systems when remote access was enabled in the 1960s was the classic keystroke-logging Trojan to simulate the logoff message and the initial dialogue of a logon. The victims, sitting down at a terminal that looked logged off, would naturally think that they were interacting with the operating system; they would dutifully enter their own user ID and password, only to be falsely informed by the criminal's software that there had been a problem. At that point, the Trojan would actually log off, so that entering the user ID and password again would log the user on uneventfully. Alert users noticed that a logoff message flashed briefly on screen before being erased; this clue led to the discovery that in fact the initial logon had been recorded by the Trojan in a disk file that could be retrieved by the malefactor later.

The *Invisible KeyLogger Stealth for Windows 2000/XP* (IKS) was a particularly powerful tool for capturing keystrokes; its description from 2016 included this chilling passage which was included in the upgraded version that could run on other versions of Windows:

All keystrokes are recorded, including the alt-ctrl-del trusted logon and keystrokes into a DOS box or Java chat room.

In addition to a flexible and friendly keystroke log viewer, IKS is extremely configurable. We provide an easy-to-use install utility. You can rename the program file, and specify the name and the path of the log file. You only need to copy one file onto the target computer for the logging to take place.

There is almost no way for the program to be discovered once the program file and the log file are renamed by the install utility. An exhaustive hard drive search won't turn up anything. And the running process won't show up anywhere.

We even provide a *Custom Compile Edition* of the program to ensure that nobody will be able to discover IKS thru an anti-spyware program.²⁸

You can understand why the Kinko's administrators did not notice the keylogger.



FIGURE 11.18 Public workstation.

Napoli's wrote, "Making the public aware of the vulnerability of shared Internet access terminals is one thing. Remedying this vulnerability is quite another." She followed this surprising assertion with a quotation from an FBI agent who said, "I don't know how you manage the risk...."

Well, competent network administrators do know how to manage the risk. Public terminals in hospitals, universities, libraries, stores, and other organizations that normally choose not to assign a workstation to every employee are routinely configured for high security – or should be.

Systems with access controls should be configured to preclude access with administrator privileges. But user ID/password combinations are a dreadfully weak method for preventing unauthorized access. Passwords can be compromised by shoulder-surfing (peering at the keystrokes) untrained users. They are weak because they're too often written down (and in too many cases placed under keyboards or mouse pads or in office desks),²⁹ or using brute-force cracking of poorly-secured one-way encrypted password files. MFA³⁰ helps to defeat keystroke loggers, as does today's antimalware software.³¹

Another much more tedious but effective method for reducing potential damage is to install a fresh version of the operating system and other authorized software on the workstations' disks. That is, the disk of each workstation on the network is periodically rewritten with a fresh, uncontaminated copy of the entire contents of the system software and parameters.³² This method works only if the stations are not accessible to users all the time. Normally such systems do *not* permit storage of users' personal data on the workstations. In addition, the systems are vulnerable to contamination between system rewrites.

Imaging software supports not only preservation of data integrity and trustworthiness but also provides a speedy mechanism for restoring functionality of a damaged system: restore the disk image of the operating-system drive and you don't have to reinstall the software.

These tools also support the principle of a *known-good copy* of the operating system: one takes an image immediately after installing a new version of the operating system and before using – and potentially damaging – it. Then before installing new software (applications, drivers, updates...) you can restore the original image, do your installation, and take a new image (properly documented) for the next time you need to start from a clean environment.

LOCKING THE LOCKS

Some friends of mine told me about new LCD projectors that were installed at their university over the summer some years ago. Seems the IT group ordered a bunch of projectors, installed them in the ceilings of classrooms at great expense, and then discovered an unpleasant feature in each projector.

Anyone could set a password on the projector to lock out further configuration changes.

The configuration included such essential elements as the input source; i.e., whether the signal was coming from a computer, a DVD player, or a VCR. If someone locked the configuration, at least two of the sources wouldn't work. The lock would inactivate such essential controls as the color balance settings, adjustments for ensuring a rectangular image, and so on.

Wouldn't you know it? Some unknown person locked one of the \$5,000 projectors the day before classes were due to start.

When my friends called the manufacturer for help, it turned out to be a mess. They had to send proof of ownership by fax (yes, this really was a while ago) and then had to wait almost the whole day before they got an unlock code for that specific projector. Imagine if that had happened on a class day.

They gently suggested to the manufacturer's tech support that letting unauthorized personnel apply a configuration lock was perhaps not the brightest idea in the world. The tech cheerfully



FIGURE 11.19
Unauthorized lock.

responded, “Oh, but you can disable that feature in the configuration.” Yes, you could, but the unauthorized personnel could equally cheerfully re-enable the feature before locking down the projector. Can you say, “denial of service?”

At that point, the administrators had to obtain and file the unlock codes for all their new projectors so that they could unlock them on demand. What they actually did is to return all of those projectors as soon as they had replacements from a different manufacturer whose engineers were a little more thoughtful in their security design.

So what does all this trouble about projectors have to do with network security?

Many organizations configure their user’s company-owned workstations or laptops using centralized policies. Operating-system parameters, network configurations, firewall policies, and antivirus rules are potentially legitimate targets for centralized controls. For example, in some circumstances, firewall configurations can usefully be determined in advance to prevent naïve users from allowing all possible network traffic. Many personal firewalls let the user allow or disallow inbound or outbound traffic for specific processes. Some users unfortunately click “yes” for everything. After a while, their firewalls become tools that reduce bandwidth but offer no security.

Similarly, some users notice that turning off the antivirus scan when transferring large numbers of files between computers can significantly increase speed; unfortunately, it’s easy to forget to turn the scan back on. These are the people who discover they have seven viruses resident in memory when they bring their computer to the shop complaining that it’s “acting funny” because all the letters are falling to the bottom of the screen.³³

If you do decide to control such tools, be sure to apply appropriate access controls to the configurations for two reasons: first, to prevent users from changing the configurations; and second, to prevent users from locking *you* (or even themselves) out of the configurations if you have to fix something for them.

There are dangers in locking such tools. The most serious is that inadequate analysis can produce a dysfunctional setup that reduces user productivity or even stops work altogether. For example, a simple error in firewall configuration can deny access to an internal network that the technician forgot about but that the user desperately needs right now – yes, *now*. Similarly, an overzealous but impractical technician can configure an antivirus product to perform an obligatory scan of all data files on the system at every bootup. This policy works may work flawlessly and take only a few seconds on the technician’s test system (with its 100 data files), only to take 20 minutes on the user’s system (which has 25,000 data files the tech didn’t know about).

So before you go locking locks, be sure you have figured out which ones to lock – and how to lock them safely.

DATA REMANENCE ON DISCARDED DISK DRIVES

Novices often believe that deleting a file using their operating system destroys the data. Actually, the only thing normal delete functions destroy is the corresponding entries in the *file-allocation table* (FAT) that keeps track of where files are stored on disk. The sectors used for the original data are then added to the list of free sectors available for use by the file system. The original data remain in place until overwritten when their sectors are assigned to other files:

Traditionally, deleting a file from a mechanical hard drive didn’t actually delete that file’s contents. The operating system would mark the file as deleted, and the data would eventually be overwritten. But that file’s data was still sitting on the hard drive, and file-recovery tools could scan a hard disk for deleted files and recover them. This is still possible on USB flash drives and SD cards, too.³⁴



FIGURE 11.20 Safe to discard?.

Discarded disk drives with fully readable information have repeatedly been found for sale by computer resellers, at auctions, at used-equipment exchanges, on *eBay* (you might enjoy an animation of Chumbawamba's song of that name³⁵) and even at flea markets and yard sales.³⁶ One of the most important formal studies of the problem was published in the January/February 2003 issue of *IEEE Security & Privacy* by Simson Garfinkel & Abhi Shelat.³⁷

The authors reported on the many failed attempts to destroy data on disk drives (*sanitization*), including

- Erasure (leaves data almost entirely intact),
- Overwriting (good enough or even perfect with enough random data but not always properly applied),
- Physical destruction (evidently, renders what's left of the drive unusable) but must be thoroughly destructive, and
- Degaussing (using strong magnetic fields to distort the magnetic domains into unreadability).

With regard to ordinary file-system formatting, the authors noted,

...[M]ost operating system format commands only write a minimal disk file system; they do not rewrite the entire disk. To illustrate this assertion, we took a 10-Gbyte hard disk and filled every block with a known pattern. We then initialized a disk partition using the Windows 8 FDISK command and formatted the disk with the format command. After each step, we examined the disk to determine the number of blocks that had been written.... Users might find these numbers discouraging: despite warnings from the operating system to the contrary, the format command overwrites barely more than 0.1 percent of the disk's data. Nevertheless, the command takes more than eight minutes to do its job on the 10-Gbyte disk—giving the impression that the computer is actually overwriting the data. In fact, the computer is attempting to read all of the drive's data so it can build a bad-block table. The only blocks that are actually written during the format process are those that correspond to the boot blocks, the root directory, the file allocation table, and a few test sectors scattered throughout the drive's surface.

The most significant aspect of their work was their field research. From November 2000 through August 2002, they bought 158 used disk drives from many types of sources and studied the data they found on the drives. Using special analytical tools, the scientists found a total of 75 GB of readable data. The full report goes into a great deal of detail, but the essential information for purposes of this section is from their last paragraph:

With several months of work and relatively little financial expenditure, we were able to retrieve thousands of credit card numbers and extraordinarily personal information on many individuals. We believe that the lack of media reports about this problem is simply because, at this point, few people are looking to repurposed hard drives for confidential material. If sanitization practices are not significantly improved, it's only a matter of time before the confidential information on repurposed hard drives is exploited by individuals and organizations that would do us harm.

There is extensive documentation available about secure wiping for Windows,³⁸ MacOS,^{39,40} Linux,⁴¹ and other Unix systems – all assuming that the drives are still functional.

A discredited way of wiping disks was degaussing:

Unfortunately, degaussing does not work. It sounds so simple. You take a giant electromagnet, put your hard disk inside and you are done. And we call it a degausser. The hard disk manufacturers, however, have ensured that magnetic disks are protected by something called a *Faraday cage*. This enclosure protects the place where the disks storing information is located from all kinds of radiation.⁴²

To destroy an *inoperable* disk, take it out of the computer and destroy it physically in its entirety. The disk must be converted to small, unusable fragments; drilling holes in them is inadequate

protection because they may allow some of the larger remnants to be read for partial data recovery. Some commercial data-destruction firms have massive crushers and shredders that can physically destroy magnetic disks, enclosures, and all.

The U.S. *DoD 5220.22-M Wiping Standards* stipulate a combination of multiple data wiping including overwriting using random bit patterns to defeat laboratory methods of deriving the original contents by measuring residual magnetic fields.

However, in most cases, this DoD technique is now less effective, more resource demanding, and less economical than more modern standards, so it has fallen out of recommended practice even at federal agencies. Yet because even historical Department of Defense standards are held in high esteem and carry great credibility, organizations' internal policies and information-security teams may still require it.⁴³

LOS ALAMOS REDUX

The U.S. *Department of Energy* (DoE) and the *Los Alamos National Laboratory* (LANL) were in the news back in the 1990s. In 1991, Matt Singer, the near-autistic child hacker calling himself *phantomd* cracked the LANL systems.⁴⁴ Peter Neumann wrote in *RISKS* 19(81):

An internal review of 64,000 unclassified computer systems throughout all major Department of Energy facilities has found serious security lapses, including the presence of classified and sensitive nuclear weapons information on 1,400 systems open to anyone on the Internet. This has stimulated a "contamination clean-up". Los Alamos alone has had 15 security breaches since Nov 1997. Apparently ftp reads – and *writes* – and readable password files are major problems.⁴⁵



FIGURE 11.21
Child hacker.

On Monday the 12th of June 2000, the LANL admitted that two highly classified computer hard drives had disappeared from a vault; the disks contained emergency-response planning information about nuclear weapons and nuclear accidents. About a week later, the two disk drives were found behind a photocopier machine that had been checked twice before.⁴⁶

On Tuesday June 13, 2000, the *Subcommittee on Oversight and Investigations* of the *Committee on Commerce* in the U.S. *House of Representatives* heard testimony about "Computer Insecurities at DOE Headquarters: DOE's Failure To Get Its Own Cyber House In Order."⁴⁷

The *DoE Office of Independent Oversight and Performance Assurance Board* reported scandalously poor security on the DoE networks in general. The report stated that some of the DoE program systems were entirely outside the firewalls and that many firewalls were improperly configured and maintained. These security weaknesses could "allow any Internet user to gain system administrator-level privileges." Glenn Podonsky, the Director of the Office, stated that "Headquarters [i.e., the DoE] has not developed overall cyber security procedures or minimum requirements for each network segment on the network."

The CISO at the DoE, Gen. Eugene Habiger, USAF (Ret'd) accused Congress of refusing the DoE's budget request for \$35M in supplemental allocations to beef up INFOSEC; instead, the DoE got a miserable \$7M – one-fifth of the request. Naturally, said Gen. Habiger, "...[H]eadquarter's unclassified cyber-security initiatives were given low priority in light of more pressing needs at our field sites."

Why Such Bad Management Decisions?

In 2000, after reading about the security failure at the LANL, my late father-in-law, Emeritus Professor of Psychology Dr Percy Black, z”l at *Pace University*, broached an interesting psychological and organizational question. “How is it possible,” he asked, “that intelligent people who have already had security problems can allow two important disk drives to be lost or stolen so soon after their other experiences?”

During the course of our discussion – standing in the gloaming in the rural countryside of Vermont as the peepers resumed their eternal calling for mates (and sounding to my ears like thousands of UPSs when the current cuts off) – we thought up some points that may stimulate discussion among readers of this section.

First, let’s examine the fundamental difficulty of maintaining INFOSEC policies or any other preventative mechanism. If INFOSEC works right, there are no problems; that is, there are no successful break-ins, there are no thefts, there are no espionage cases, there are no losses of disk drives from vaults. It’s the electronic equivalent of flossing: floss day after day and there are no cavities, no gum disease.

The problem is human psychology: in the absence of positive feedback – such as when INFOSEC policies work and flossing prevents disease – the behavior inevitably suffers some extinction.⁴⁸ If we imagine compliance with INFOSEC policies (or flossing) as a graph, I suspect the compliance curve would look like a sawtooth – a spike of high compliance immediately following an incident (or a bad scorecard from the dental hygienist) followed by a gradual decline in compliance. Then another incident and – boom – the compliance rate goes up again.

Secondly, our culture has allowed short-term thinking and monetary valuation to produce a very difficult situation for any preventive measure, including INFOSEC. Several issues are wrapped up in this statement.

We know that in the last twenty years, much of management culture has accepted the pernicious doctrine of employee fungibility; i.e., people are pretty much replaceable, faceless entities whom management can fire and hire at will. Many employees, and especially new employees without any experience of life-long employment by one firm, very naturally responded to the abandonment of loyalty towards them by abandoning loyalty towards employers. Personal relationships, value of individuals, recognition of the importance of creativity and experience – these factors have been pushed to the bottom of the heap of priorities. It’s no surprise that residence time in a particular job has dropped to about four years in the USA⁴⁹ – and some people change jobs from year to year, often with handsome signing bonuses and raises to boot.

The other problem is that many people have been tricked into believing that we can reasonably measure performance primarily (or, in some pathological cases, exclusively) in terms of short-term profit.⁵⁰ The “bottom line” mentality focuses on how much money was earned or saved in a period of time. Couple this attitude towards defining success with the short residence time in a job and you have a disaster for management perspective. If a manager knows (s)he will be leaving in, say, a couple of years, there is less incentive to take a long-term view of business decisions. Quarterly bottom lines are sometimes viewed as the prime measure of a manager’s competence. Now, if raising revenue is difficult, an obvious solution is to reduce costs. In the short run, it can seem reasonable to such a person to gamble: reduce expenditures on preventive mechanisms in the hope that the inflated bottom line will look good, hope that there are no problems, and then leave before the fecal material impacts the air-impelling device.

I think that this combination of factors may very well be at play not only in LANL and the DOE, but also throughout U.S. and Western society. The fact that what would have been normal decades

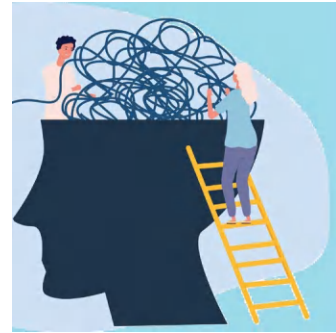


FIGURE 11.22
Psychology of error.

ago is seen as extraordinary now supports this view. Take for example the recession of 1981 through 1982, when U.S. unemployment reached 11%.⁵¹ Many companies, including high-tech companies, fired a percentage of their employees to reduce payroll; sometimes they even simply told managers to cut staff by a fixed percentage and allowed them to fire at will, so to speak.

In contrast, some companies took a different tack. In 1982 I was working for *Hewlett Packard* in the HP3000 systems-engineering group at the Montréal, Québec, Canada office. We were told of the financial pressures on the company and informed that, if we agreed, we would all – every single one of the 88,000 employees world-wide, including top management – have a 10% reduction in pay. We'd also be given every second Friday off as an unpaid leave day. However, *not a single employee would be fired*. Well you know, nobody in the Montréal office resigned, and I don't recall anyone taking those free days off. When the recession ended, other technical firms scrambled to regain their trained staff, invested millions in training new employees, and had to rebuild morale. HP just picked up the slack and roared ahead to low-cost profitable production.

In conclusion, it seems to me that the consistent findings of failure by management to support INFOSEC is a systemic problem that will not be solved with Band-Aids.

Suggestions

In this section, I suggest some practical supports for INFOSEC to help avoid the kinds of repeated failures in security that have been highlighted in the DOE and throughout governments, academia, and the commercial world.

Problem: *people lose interest in following INFOSEC policies because there is nothing to show for successful programs.*

- **Strategies:**

- Use vigorous security-awareness programs;
- Use reward, not just punishment.

- **Tactics:**

- Make your INFOSEC awareness program interesting and fun: use clippings about interesting new cases of INFOSEC breaches and couple them with practical advice on countermeasures; speak to protecting the private interests of employees, not only corporate (e.g., given them monthly tips on protecting their identity, preventing theft of their own laptops, helping them secure their home computers, preventing abuse of and by their kids;
- Check (audit) security in one sector of your organization a day; reward people who are in compliance. For example, give people who have secure screen savers activated when they're away from their desk a pair of tickets to a play or a pair of vouchers for a fine restaurant meal. Use password-cracking software on your network password files and give prizes/rewards/recognition to those whose passwords are not cracked.
- Make INFOSEC a team sport: put together scorecards for participating work-unit "teams" just like factories have banners proclaiming, "This facility has been accident-free for 743 days!" or "Quality Assurance Champions, 3Q2021." Encourage a sense of pride and involvement in security rather than allowing it to be seen as an external imposition.

Problem: *managers take a short-term perspective and focus on the quarterly bottom-line to the exclusion of longer-term thinking and support for preventive mechanisms such as INFOSEC.*

- **Strategy:** make INFOSEC compliance an explicit component of managers' evaluations.

- **Tactics:**

- Use audits, external penetration testing, and even (with careful preparation) simulated social engineering attacks (the subject of another section to come) to measure the level of compliance with INFOSEC policies.

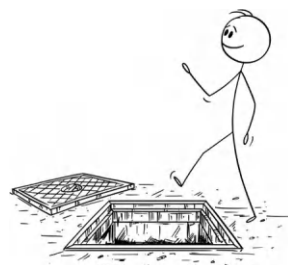


FIGURE 11.23 Avoid the same old traps.

- In manager evaluations that include questionnaires of employees about their manager's performance, include questions about support for and compliance with INFOSEC policies by that manager.
- Discuss support for INFOSEC as a normal part of management reviews for new projects.
- Ensure that top management consistently follow INFOSEC policies and serve as role models for the people reporting to them.

VELOCIHACKERS AND TYRANNOSAURUS SUPERIOR

The 1993 PG-13 hit movie *Jurassic Park*⁵² starred several holdovers from 65 million years ago. It also showed errors in network security that seem to be as old.

For those of you who have just returned from Neptune or who were in diapers in 1980 or later, *Jurassic Park* is about a dinosaur-theme park that displays live dinosaurs created after scientists cracked extinct dinosaur DNA code recovered from petrified mosquitoes. The film has terrific live-action dinosaur replicas and some heart-stopping scenes. It also dramatizes awful network management and security. Unfortunately, the policies are as realistic as the dinosaurs.

Consider a network-security risk analysis for the imagined Jurassic Park. The entire complex depends on computer-controlled electric fences and gates to keep a range of prehistoric critters from eating the tourists and staff. So at a simple level, if the network fails, people turn into dinosaur food.

Jurassic Park's security network is controlled by what was an ultramodern Unix system, but its management structures date from the Stone Age. There is only one person who maintains the programs that control the security network. This breaks *Kabay's Law of Redundancy*, which states, "No knowledge shall be the property of only one member of the team." After all, if that solitary guru were to leave, go on vacation, or get eaten by a dinosaur, you'd be left without a safety net.

Jurassic Park's security system is controlled by computer programs consisting of two million lines of proprietary code. These critical programs are not properly documented. An undocumented system is by definition a time bomb. In the movie, this bomb is triggered by a vindictive programmer who is angry because he feels overworked and underpaid.

One of the key principles of security is that people are the most important component of any security system. Disgruntled and dishonest employees cause far more damage to networks and computer systems than hackers.⁵³ The authoritarian owner of the Park dismisses the programmer's arguments and complaints as if owning a bunch of dinosaurs gives him the privilege of treating his employees rudely. He pays no attention to explicit indications of discontent, including aggressive language, resentful retorts, and sullen expressions. If the owner had taken the time to listen to his employee's grievances and take steps to address them, he could have prevented several dinosaur meals.

Bad housekeeping is another sign of trouble. The console where the disgruntled programmer works looks like a garbage dump; it's covered in coffee cup fungus gardens, historically significant chocolate bar wrappers, and a treasure trove of recyclable soft drink cans. You'd think that a reasonable manager would be alarmed simply by the number of empty calories per hour being consumed by this critically important programmer. The poor fellow is so overweight that his life expectancy would be short even if he didn't become dinosaur fodder.

Ironically, the owner repeats, "No expense spared" at several points during the movie. It doesn't seem to occur to him that with hundreds of millions of dollars spent on hardware and software – not to mention the buildings and grounds and an entire private island – modest raises for the staff would be trivial in terms of operating expenses but significant for morale.



FIGURE 11.24

Velocihacker.

In the movie, the network programmer is bribed by competitors to steal dinosaur embryos. He does so by setting off a logic bomb that disrupts network operations completely. The network outage causes surveillance and containment systems to fail, stranding visitors in, well, uncomfortable situations. Even though the plot is not exactly brilliant, I'd like to leave at least something to surprise those who haven't seen the movie yet.

When the systems fail, for some reason all the electric locks in the park's laboratory are instantly switched to the open position. Why aren't they automatically locked instead? Normally, when a security controller fails, the default should be to keep security high, not eliminate it completely. Manual overrides such as crash bars (the horizontal bars that open latches on emergency exits) can provide emergency egress without compromising security.

As all of this is happening, a tropical storm is bearing down on the island. The contingency plan appears to consist of sending almost everyone away to the mainland, leaving a pitifully inadequate skeleton crew. The film suggests that the skeleton crew is not in physical danger from the storm, so why send essential personnel away? Contingency plans are supposed to include redundancy at every level. Reducing the staff when *more* are needed is incomprehensible.

At one point, the systems are rebooted by turning the power off to the entire island on which the park is located. This is equivalent to turning the power off in your city because you had an application failure on your PC. Talk about overkill: why couldn't they just power off the computers themselves?

Where were the DPMRP (*Dinosaur Prevention, Mitigation and Recovery Planning*) consultants when the park was being designed? Surely everybody should know by now that the only way to be ready for dinosaurs, uh, disasters, is to think, plan, rehearse, refine, and update. Didn't anyone think about what would happen if the critters got loose? Where are the failsafe systems? The UPSs? The backup power generators? Sounds like Stupidosaurians were in charge.

We may be far from cloning dinosaurs, but we are uncomfortably close to managing security with all the grace of a *Tyrannosaurus rex* trying to type.

I hope you see the film. And bring your boss.

NOTES

- 1 [Dhoul \(2021\)](#).
- 2 [Whipps \(2008\)](#).
- 3 [Fealk \(2011\)](#).
- 4 [Rist \(2021\)](#).
- 5 [IBM Cloud Education \(2019\)](#).
- 6 [Bigelow \(2018\)](#).
- 7 [SourceForge \(2021\)](#).
- 8 [Minitab \(2021\)](#).
- 9 [Corporate Finance Institute \(2021\)](#).
- 10 [Palisade \(2021\)](#).
- 11 [Howell \(2012\)](#).
- 12 [Howell \(2012\)](#).
- 13 [Howell \(2016\)](#).
- 14 [Kabay \(2019\)](#).
- 15 [TrustRadius \(2021\)](#).
- 16 [Lowe \(2002\)](#).
- 17 [Miller \(2021\)](#).
- 18 [Software Testing Help \(2021\)](#).
- 19 [International Computer Security Association Labs \(2009\)](#).
- 20 [Bowman \(2020\)](#).
- 21 [Internet Movie Database \(2021\)](#).
- 22 [Internet Movie Database \(2021\)](#).
- 23 [116th Congress of the United States \(2019\)](#).
- 24 [Chesney \(2019\)](#).

- 25 Broeders (2021).
- 26 Traynor (2003).
- 27 Napoli (2003).
- 28 AMECISCO (2016).
- 29 Henry (2012).
- 30 Griffith (2021).
- 31 Kassian (2020).
- 32 Keary (2021).
- 33 onNeutral (2007).
- 34 Hoffman (2015).
- 35 CHUMBAWAMBA (2012).
- 36 Roberts (2003).
- 37 Garfinkel and Shelat (2003).
- 38 Whitney (2020).
- 39 Apple (2021).
- 40 Apple (2021).
- 41 Timme (n/a).
- 42 it-recycling (2021).
- 43 Stinnon (2019).
- 44 Freedman and Mann (1997).
- 45 Neumann (1998).
- 46 Risen (2000).
- 47 Committee on Commerce, Subcommittee on Oversight and Investigations, US Congress (2000).
- 48 Farmer (n/a).
- 49 Kolmar (2021).
- 50 Sampson (2018).
- 51 Sablik (2013).
- 52 Internet Movie Database (1993).
- 53 Rosenthal (2021).

WORKS CITED

- 116th Congress of the United States. (2019, June 13). *H.R.3270 - Active Cyber Defense Certainty Act*. Retrieved November 8, 2021, from CONGRESS.GOV: <https://www.congress.gov/bill/116th-congress/house-bill/3270>
- AMECISCO. (2016, October 12). *Invisible KeyLogger Stealth for Windows 7*/Vista/XP/2000*. Retrieved November 7, 2021, from AMECISCO | KeyLogger 2000: <https://web.archive.org/web/20161012191149/http://www.amecisco.com/iks2000.htm>
- Apple. (2021, October 25). *Use Disk Utility to Erase a Mac with Apple Silicon*. Retrieved November 7, 2021, from Apple: <https://support.apple.com/en-us/HT212030>
- Apple. (2021, October 25). *Use Disk Utility to Erase an Intel-Based Mac*. Retrieved November 7, 2021, from Apple: <https://support.apple.com/en-us/HT208496>
- Bigelow, S. J. (2018, September). *ITSM (IT Service Management)*. Retrieved December 13, 2021, from TechTarget | App Maintenance | Analytics: <https://searchitoperations.techtarget.com/definition/ITSM>
- Bowman, E. (2020, April 20). *The IPv6 Apocalypse is Here: 3 Reasons to Upgrade*. Retrieved December 13, 2021, from No Deploy Friday | Posts: <https://nodeployfriday.com/posts/ipv6-apocalypse/>
- Broeders, D. (2021, March 30). Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, 7(1), 1–14. doi:<https://doi.org/10.1093/cybsec/tyab010>
- Chesney, R. (2019, June 14). *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*. Retrieved November 8, 2021, from Lawfare: <https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act>
- CHUMBAWAMBA. (2012, March 8). *“On eBay” Official Video HD*. Retrieved November 7, 2021, from Youtube: <https://www.youtube.com/watch?v=xu7alpgez7Hg>
- Committee on Commerce, Subcommittee on Oversight and Investigations, US Congress. (2000, June 13). *Computer Insecurities at DOE Headquarters: DOE’s Failure To Get Its Own Cyber House In Order*. Retrieved November 7, 2021, from Federation of American Scientists | Congress | 2000: <https://sgp.fas.org/congress/2000/doecyber.html>

- Corporate Finance Institute. (2021). *What is Sensitivity Analysis?* Retrieved November 5, 2021, from CFI | Resources | Knowledge | Financial Modeling: <https://corporatefinanceinstitute.com/resources/knowledge/modeling/what-is-sensitivity-analysis/>
- Dhoul, T. (2021, October 2). *What Is Operations Management?* Retrieved October 12, 2021, from Top MBA: <https://www.topmba.com/mba-programs/what-operations-management>
- Farmer, A. *Study: One-Third of Americans Don't Floss*. Retrieved November 7, 2021, from Crossroads Dental: <https://www.dramyfarmer.com/study-one-third-of-americans-dont-floss/>
- Fealk, G. S. (2011, November 3). *Importance of Documentation in Employment Disputes*. Retrieved October 21, 2021, from HR Hero Line: <https://hrdailyadvisor.blr.com/2011/11/03/importance-of-documentation-in-employment-disputes/>
- Freedman, D. H., & Mann, C. C. (1997). *At Large: the Strange Case of the World's Biggest Internet Invasion Hardcover* (1st ed., Vol. 1). Simon & Schuster. Retrieved November 7, 2021, from <https://smile.amazon.com/At-Large-Strange-Internet-Invasion/dp/0684824647>
- Garfinkel, S. L., & Shelat, A. (2003, February 1). Remembrance of data passed: A study of disk sanitization practices. *IEEE Security & Privacy*, 1(1), 17–27. <https://doi.org/10.1109/MSECP.2003.1176992>
- Griffith, E. (2021, April 27). *Two-Factor Authentication: Who Has It and How to Set It Up*. Retrieved November 7, 2021, from PC Magazine | How-To | Security: <https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up>
- Henry, A. (2012, November 13). *The Most Common Hiding Places for Workplace Passwords*. Retrieved November 7, 2021, from lifehacker | Tech: <https://lifehacker.com/the-most-common-hiding-places-for-workplace-passwords-5852667>
- Hoffman, C. (2015, November 28). *Why You Can't "Securely Delete" a File, and What to Do Instead*. Retrieved November 7, 2021, from How-To Geek: <https://www.howtogeek.com/234683/why-you-cant-securely-delete-a-file-and-what-to-do-instead/>
- Howell, G. (2012, January 9). *Avoid Single Points of Failure in Your Business*. Retrieved December 13, 2021, from Business Continuity UK: <https://web.archive.org/web/20120109011714/http://www.businesscontinuityuk.net/understanding-the-process/avoid-single-points-of-failure-your-business>
- Howell, G. (2012, March 13). *Succession Planning and Business Continuity*. Retrieved December 13, 2021, from Business Continuity UK: <https://web.archive.org/web/20120313095229/http://www.businesscontinuityuk.net/understanding-the-process/succession-planning-business-continuity>
- Howell, G. (2016, August 8). *Have You Got a Succession Plan?* Retrieved December 13, 2021, from Business Continuity UK: <https://web.archive.org/web/20160808124015/http://www.businesscontinuityuk.net/businesscontinuity/have-got-succession-plan>
- IBM Cloud Education. (2019, May 22). *IT Infrastructure Library (ITIL)*. Retrieved October 21, 2021, from IBM | Cloud | Learn: <https://www.ibm.com/cloud/learn/it-infrastructure-library>
- International Computer Security Association Labs. (2009, April 22). *ICSA Labs Turns 20!* Retrieved November 7, 2021, from ICSAlabs: <https://www.icsalabs.com/press-release/icsa-labs-turns-20>
- Internet Movie Database. (1993). *Jurassic Park*. Retrieved from IMDb: <https://www.imdb.com/title/tt0107290/>
- Internet Movie Database. (2021). *Jean-Claude Van Damme*. Retrieved November 8, 2021, from IMDb: <https://www.imdb.com/name/nm0000241/>
- Internet Movie Database. (2021). *Steven Seagal*. Retrieved November 8, 2021, from IMDb: <https://www.imdb.com/name/nm0000219/>
- it-recycling. (2021). *Degausser and Other Methods for Destroying Data on Hard Disks*. Retrieved November 7, 2021, from it-recycling | Hard Disk Destruction: <https://www.it-recycling.nl/en/hard-disk-destruction/degausser-uk/>
- Kabay, M. E. (2019, June 19). *Continuity-of-Operations Matrix*. Retrieved October 16, 2021, from M. E. Kabay | Operations Management: http://www.mekabay.com/opsmgmt/continuity-of-operations_matrix.xlsx
- Kassian, A. (2020, November 11). *5 Best Antiviruses with Keylogger Protection [2021]: Full Online Security*. Retrieved November 7, 2021, from SafetyDetectives | Blog: <https://www.safetydetectives.com/blog/best-antivirus-that-protects-against-keyloggers/>
- Keary, T. (2021, September 30). *10 Best Disk Cloning Software*. Retrieved November 7, 2021, from comparitech | Net Admin: <https://www.comparitech.com/net-admin/best-hard-drive-disk-cloning-software/>
- Kolmar, C. (2021, May 19). *Average Number of Jobs in a Lifetime: All Statistics*. Retrieved November 7, 2021, from ZIPPPIA: <https://www.zipppia.com/advice/average-number-jobs-in-lifetime/>
- Lowe, S. (2002, May 17). *Keep Your Power Clean with the Right Conditioner*. Retrieved November 5, 2021, from TechRepublic: <https://www.techrepublic.com/article/keep-your-power-clean-with-the-right-conditioner/>
- Miller, R. (2021, July 26). *Beyond Generators: Data Centers Pursue New Approaches to Backup Energy*. Retrieved November 5, 2021, from Data Center Frontier: <https://datacenterfrontier.com/beyond-generators-data-centers-pursue-new-approaches-to-backup-energy/>

- Minitab. (2021). *Take Your Analytics to the Next Level*. Retrieved November 5, 2021, from Minitab: <https://www.minitab.com/en-us/>
- Napoli, L. (2003, August 7). *The Kinko's Caper: Burglary by Modem*. Retrieved November 5, 2021, from The New York Times | Technology: <https://www.nytimes.com/2003/08/07/technology/the-kinko-s-caper-burglary-by-modem.html>
- Neumann, P. G. (1998, June 12). *U.S. Department of Energy computer security risks*. Retrieved November 7, 2021, from The Risks Digest: <https://catless.ncl.ac.uk/Risks/19.81.html#subj1>
- onNeutral. (2007, October 30). *In Action: Cascade Virus*. Retrieved November 7, 2021 <https://www.youtube.com/watch?v=UWLg6tTeQRg>
- Palisade. (2021). *Monte Carlo Simulation*. Retrieved November 5, 2021 from Palisade | Products & Services | @Risk: https://www.palisade.com/risk/monte_carlo_simulation.asp
- Risen, J. (2000, June 17). *Missing Nuclear Data Found Behind a Los Alamos Copier*. Retrieved November 7, 2021, from The New York Times: <https://www.nytimes.com/2000/06/17/us/missing-nuclear-data-found-behind-a-los-alamos-copier.html>
- Rist, O. (2021, September 20). *The Best Help Desk Software for 2021*. Retrieved October 21, 2021, from PC Magazine | Best Products | IT Management | Help Desk: <https://www.pcmag.com/picks/the-best-help-desk-software>
- Roberts, P. (2003, January 16). *MIT: Discarded Hard Drives Yield Private Info*. Retrieved November 7, 2021, from ComputerWorld | Security | Privacy: <https://www.computerworld.com/article/2580013/mit-discarded-hard-drives-yield-private-info.html>
- Rosenthal, M. (2021, June 1). *Insider Threat Statistics You Should Know: Updated 2021*. Retrieved November 5, 2021, from Tessian: <https://www.tessian.com/blog/insider-threat-statistics/>
- Sablik, T. (2013, November 22). *Recession of 1981–82*. Retrieved November 7, 2021, from Federal Reserve History | The Great Inflation: <https://www.federalreservehistory.org/essays/recession-of-1981-82>
- Sampson, R. (2018, January 22). *Short-Term Thinking in U.S. Markets: A Growing Trend with Lasting Implications*. Retrieved November 7, 2021, from Georgetown University | McDonough School of Business: <https://msb.georgetown.edu/news-story/short-term-thinking-us-markets/>
- Software Testing Help. (2021, November 1). *Top 10 Most Powerful Vulnerability Assessment Scanning Tools In 2021*. Retrieved November 7, 2021, from SoftwareTestingHelp: <https://www.softwaretestinghelp.com/vulnerability-assessment-tools/>
- SourceForge. (2021). *DocFetcher*. Retrieved October 21, 2021 <http://docfetcher.sourceforge.net/en/index.html>
- Stiennon, R. (2019, March 28). *Everything You Need to Know About the DoD 5220.22-M Wiping Standard & Its Applications Today*. Retrieved November 7, 2021, from blanco | Resources: <https://www.blanco.com/resources/blog-dod-5220-22-m-wiping-standard-method/>
- Timme, F. *How to Securely Destroy/Wipe Data on Hard Drives with shred on Linux*. Retrieved November 7, 2021, from HowtoForge | Tutorials: <https://www.howtoforge.com/how-to-securely-destroy-wipe-data-on-hard-drives-with-shred>
- Traynor, I. (2003, 05 16). *The World's Dearest Pinch of Salt Taken in 54 Seconds*. Retrieved 04 30, 2021, from The Guardian: <https://www.theguardian.com/world/2003/may/16/arttheft.arts>
- TrustRadius. (2021). *List of Top Data Center Power Solutions 2021*. Retrieved from TrustRadius: <https://www.trustradius.com/data-center-power>
- Whipps, H. (2008, February 10). *How Writing Changed the World*. Retrieved October 21, 2021, from Live Science: <https://www.livescience.com/2283-writing-changed-world.html>
- Whitney, L. (2020, July 2). *How to Wipe Your Hard Drive*. Retrieved November 7, 2021, from PC Magazine | How-To | Operating Systems | Windows: <https://www.pcmag.com/how-to/how-to-wipe-your-hard-drive>

12 Technical Support

A key element of operations in IT is *technical support* (TS). TS must provide support to software designers, programmers and users in their use of computers, network devices, software, and anything else that users need for effective use of what has been supplied by their organization.

However, there should be explicit documentation available to everyone in the organization that TS does *not* support equipment or software obtained privately or being used in violation of corporate policy. For example, if an employee receives a laptop computer and is authorized to use it from home with the corporate VPN, that's perfectly suitable for the TS to help with problems meeting the employee's obligations; however, an identical laptop computer purchased privately or an assigned computer being used without a VPN or for playing games or viewing pornography in violation of policy is *not* to be supported. Support includes



FIGURE 12.1
Tech support.

- Equipment acquisition and maintenance (buying, selling, insuring, and providing repair contracts),
- Resource usage optimization (CPU, mass storage, memory, peripherals),
- Design optimization (improving algorithms and data structures),
- Database administration (managing capacities and structural relationships),
- Quality assurance (testing systems before putting them into production),
- Telecommunications (network expansion and monitoring),
- Problem solving (running a helpdesk, problem diagnosis, keeping track of previous cases, interacting with manufacturers' support services),
- Production (supporting data entry, report generation, updates),
- Quality control (verifying accuracy and appearance of output),
- Training users on central and microcomputer system operating systems, utilities, and communications.

However, there should be explicit documentation available to everyone in the organization that TS does *not* support or software obtained privately or being used in violation of corporate policy. For example, if an employee receives a laptop computer and is authorized to use it from home with the corporate VPN, that's perfectly suitable for the TS to help with problems meeting the employee's obligations; however, an identical laptop computer purchased privately or an assigned computer being used without a VPN or for playing games or viewing pornography in violation of policy is *not* to be supported.

The following sections review *the art of technical support* – which was the name of a course I taught in the 1980s through the 1990s. Lecture slides and review questions are available online.¹ Topics include

- Tools for tracking incidents
- Systematic approaches to problem solving
- Training tech-support staff for effective communications with clients
- Dealing with hostile customers

- Working with vendors
- Principles of effective training.

THE EXPERT IN THE NEXT OFFICE

One of the dangers for TS is the amateur support expert – the *expert in the next office*.

“Marcie, can you spare a minute?” Marcie groans inwardly. This is the sixth time this morning someone has come in from a neighboring office to ask her for “a minute.” Each occasion lasted about a quarter of an hour. The questions all concerned MARVEL 4-5-6, on which Marcie is the acknowledged expert.

However, Marcie is actually the *Assistant* to the *Director of Finance*, not a TS specialist from *Data Processing*. Every time she’s interrupted by a call for help from people in Accounting, Shipping, Engineering, and even occasionally from Data Processing, she falls further behind in her assigned work. She likes helping people, but lately she’s had to stay late after the nominal end of her work day simply to make up for the time she has used acting as informal technical support to her neighbors.

Marcie may have a bad time of it unless something changes in her organization. She may be fired by her boss because her productivity drops too low according to her job description. She may burn out and quit because of overwork and criticism. Or she may cause resentment among her colleagues and neighbors by suddenly declining to help them or by complaining to her own boss and causing a ruckus. Alternatively, she may have a good time and manage to meet all the demands on her quite successfully until the DP department begins to feel threatened and someone either complains to the higher-ups or begins spreading nasty comments about poor, helpful Marcie.

Being *the expert in the next office* (TEITNO) is tough on the expert.

Looking at this situation from a management point of view, there are problems for the recipients of all this free aid. The longer they can persist in getting apparently free help from their unofficial benefactor, the longer they can avoid letting upper management know they need help with their office-automation tools. Then when the bubble bursts and the expert becomes unavailable, managers are confronted with a sudden demand for unplanned resources. In some organizations, unexpected staffing requirements are difficult to satisfy. Managers have a hard time explaining how it is that they were unable to predict the need and budget for it.

I couldn’t resist referencing this essay in naming this textbook.



FIGURE 12.2 TEITNO.

TANSTAAFL

Engineers often say, “There ain’t no such thing as a free lunch” (often abbreviated TANSTAAFL)² to imply that no benefit is without cost.

From a technical support perspective, even the most gifted unofficial expert is necessarily an amateur. True, there are many users whose technical knowledge of their tools exceeds that of their own TS staff. But professional TS consists of far more than just technical knowledge. Almost no amateur expert will

- Have colleagues to discuss the problem with on a technical level.
- Have backup personnel so she can provide faster service to requesters.
- Search the appropriate technical manuals with the user experiencing a problem.



FIGURE 12.3

Not free.

- Have access to all the periodical information provided by manufacturers.
- Document the problems carefully so as to avoid having to solve them all over again later.
- Have access to phone-in consulting services.
- Determine the cause of the problem and ensure that the problem does not recur; and
- Broadcast information about the problem, its workaround, and its fix to unaffected users who may benefit from the information.

Failing to manage knowledge effectively can lead to a breach of availability (systems on which people rely may be inaccessible without a missing expert) or of utility (existing systems may not be fully exploited in the absence of a missing expert). From a security perspective as well as from a general management perspective, it is more sensible for employees to help themselves and each other by letting management know they need technical support.

If you are TEITNO, when someone asks you for technical help in an area that isn't part of your formal job, by all means help them but let your manager know immediately that there's a support problem.

If you find yourself asking TEITNO for technical help even though she isn't really supposed to be spending time on such problems, don't stop this time but tell your own manager that you'd prefer it to be an exceptional case and that you'd much rather have a permanent TS team to work with.

TOOLS FOR TRACKING TS INCIDENTS

This section focuses on some of the advantages and requirements of tools for incident tracking.

There's a wide range of software available for tracking incidents.³ You can build your own, but then you'll have to provide proper documentation and training materials because turnover is a constant problem for support teams. In addition, unless your analysts have experience with the support function, they are likely to miss useful features that have accumulated over the years in products used by thousands of people.

All such tools can be complex; since you don't want people fumbling about in an emergency, be sure that you budget for adequate training for your staff as you implement the tool you select.

Keeping track of all of technical support calls is essential for effective incident handling. Having details available to all members of the TS in real-time and for research and analysis later serves many functions:

- *Communication among team members:* Having the details written down in one place means that team members can pass a case from one to another and share data efficiently.
- *Better client service:* Callers become frustrated when they have to repeat the same information to several people in a row; a good incident-tracking system reduces that kind of irritation.
- *Documentation for effective problem-solving:* A good base of documented experience can help find the right procedure and the right solution quickly.
- *Institutional memory:* When experience is written down and accessible, the organization's capacity to respond quickly and correctly to incidents improves over time.
- *Follow-up with clients:* Managers can use the incident DB to prepare management reports and to follow-up with specific clients to understand and resolve difficulties or complaints.
- *Forensic evidence:* Detailed, accurate, and correctly time-stamped notes can be a deciding element in the successful prosecution of malefactors.

These advantages apply equally well to tracking incidents by CSIRTs as discussed in a later section.



FIGURE 12.4

Tracking incidents.

REQUIREMENTS FOR PROBLEM SOLUTION

Some of the more obvious requirements of any incident-handling system are listed below. Most are self-explanatory but I've added comments to a few of them:

- Unique identifier for case
- Dates and times for all events
- Who currently controls the case: It should be instantly obvious who is in charge of solving the problem.
- Keywords
- *Contact information*: Every person in the case should be listed with room for phone, email and fax numbers
- *Handover of control*: Whenever someone takes over control of the case, that handover should be noted in the record
- Technical details including
 - Diagnostics
 - Tests of hypotheses
- *Resolution*: What was the outcome? When was the case closed?
- *Search facilities*: Full-text search capabilities
- *Knowledge base*: Ability to integrate vendor-supplied entries to speed research
- *Industry-standard DB engine*: Easy to learn, maintain and improve
- Accept input from *comma-separated value* (CSV) files for potential import of data from other systems

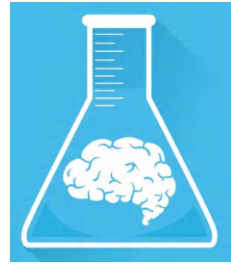


FIGURE 12.5
Problem solution.

PROBLEM-DATABASE ANALYSIS

One of the key benefits of a helpdesk software or even a simple DB is collecting statistics about the problems and responses of the team as a whole and of individuals in the team.

Call-tracking statistics allow us easily to answer important operational questions, e.g.,

- How many calls were there in any given period?
- Is the overall number stable, growing, or shrinking?
- What's the frequency pattern of calls – how many at what time? On what days?
- What's the distribution of *types* of problems (e.g., hardware, software, user error...)
- Which departments or groups are the callers from (e.g., customer service, accounting, factory, order-processing, executives...)
- What are the statistics about the response time (time to first answer by helpdesk)? What are the statistics about how long it's taken to close the cases?
- What are the response-time and closure-time statistics for each member of the helpdesk team?
- What's the pattern of urgency scores for the calls?
- What are the results of the post-closure user-satisfaction surveys?
- Are there statistical interactions among these factors (e.g., does the urgency score vary by type of problem? Do the various statistics vary among personnel?



FIGURE 12.6
Statistics.

Sometimes there may be obviously exceptional cases in these statistics. For example,

- The accounting staff in general tend to ask questions showing lack of training on their new software.
- The engineers ask the fewest questions, but their case-severity scores are very high.

- The helpdesk staff consistently answer calls from the intensive-care unit (ICU) of the hospital most quickly and resolve their problems the fastest.
- One of the helpdesk crew, Leslie, has suddenly shown a drastic increase in delays in answering the calls and a drastic increase in length of time for closing the cases.

These statistics do not in themselves necessarily mean that specific responses are easy to determine. For example,

- The Directors of Accounting have refused to allow adequate training for their staff.
- The Engineering Department recently installed a new version of their production-control software – but investigation reveals that they accepted a test version from the vendor without checking with the IT group.
- The Helpdesk Director spoke with the ICU staff last year and learned about the importance of quick response, so the helpdesk team was carefully instructed on how to respond.
- Leslie has two new twin babies who are suffering from serious congenital disease and is constantly on the phone with their worried partner, perhaps it's time for paid leave for Leslie.

There are many employees who have already studied applied statistics; even if someone needs to learn the basics needed for the kinds of analysis described above, there are free texts and courses widely available. Because of my five decades of enthusiasm for and teaching of statistics, I have made available a free, simple textbook on elementary statistics, including self-grading exercises, on my website.⁴

SOLVING TECHNICAL PROBLEMS

In my decades of work in technical support, I developed some principles for helping to resolve problems reported by users:

- Set Your Goals
- Get the Global Picture
- Distinguish Observation from Assumption
- Distinguish Observation from Hearsay
- Distinguish Observation from Hypothesis
- Challenge Your Hypothesis
- Track the Details
- RTFM
- Use Bug/Patch Reports



FIGURE 12.7
Solving problems.

SET YOUR GOALS

The short-term objective of problem-solving is (duh) to fix the problem. However, staff should always be thinking of the long-term objectives:

- Figure out why the problem happened.
- Make sure it doesn't happen again (if possible).

Eliminating a problem by randomly trying changes is not a reasonable approach for TS. The incompetent support agent who blithely tells every caller to reboot their system on the off-chance



FIGURE 12.8 Setting goals.

that the problem will (temporarily) disappear is not doing the user or the organization a favor. If we don't find out *why* a problem is occurring – or at least, under what specific conditions it occurs – we are simply gambling that the problem won't recur as if it were a game in a casino.

GET THE GLOBAL PICTURE

When gathering information about an incident, staff members should establish a clear picture of what people were doing when they realized that there was a problem. For example, it may be important to know that someone was accessing a rarely-used account and noticed that a file was not available because someone else had it open. Those details will help to characterize the attack and to provide clues that may lead to additional valuable data. However, my approach would include asking why my contact was accessing the rarely-used account; it takes only a minute, but getting a wider picture may give the analyst another perspective that can also lead to new clues. In the scenario I have sketched, one could imagine that a system administrator had become curious about some unexpected resource utilization in a supposedly dormant account. This simple fact might lead to additional exploration of system log files and questions about whether any other dormant accounts had sparked curiosity. So, in general, it is worth your while to explore the situation more broadly at first rather than driving down the very first avenue that presents itself in the initial questions. Sometimes users are so deep in the path they have followed to meet a particular requirement that they forget to let the support tech know the purpose of their work. Here's an example of a dialog in which the user has dropped into details on a roundabout path:



FIGURE 12.9
Global picture.

Prog: How do I write octal data directly in the directory?

Tech: Why would you want to do that?

Prog: Because I have to alter the first 8 bytes of the file block, some parts of the file index block, and data in the group and account index blocks.

Tech: No, I mean, what are you trying to do? How would you describe the problem to someone who didn't know about the directory?

Prog: I have to change the name of the file.

Tech: How about: RENAME?

Tech: Oh yeah... I forgot.

In my TS work, I *always* asked what the caller was trying to do in operational terms before discussing technical details.

Another good practice for TS staff is to ask about the functional reason for using the specifics that have led to a problem:

- Can I have system ALPHA for a production that lasts 3 hours and takes 2,000,000 sectors of space this weekend?
 - Bad answer: Sorry, ALPHA's booked solid this weekend.
 - Better answer: Sorry, ALPHA's booked solid this weekend. But what's the problem—what do you need? Maybe we can solve it some other way—like system BETA, which is free this weekend.
- Oh, sure, I guess BETA would be OK too.

DISTINGUISH OBSERVATION FROM ASSUMPTION

As the TS member listens to the observations of other staff members, it is critically important to distinguish *facts* – that is, personal observations – from *assumptions*. Assumptions are ideas taken for granted or statements that are accepted without proof. For example, imagine the serious consequences of hearing someone say, “And so then they exploited a flaw in the firewall and then they...” and simply writing that statement down as if it were a fact. Such an assumption could profoundly distort the investigation, putting people’s efforts into the wrong track and diverting their attention from a more fruitful line of inquiry. Hearing such a statement, I would write down, “And so perhaps they exploited a flaw in the firewall...”

Sometimes users fail to realize that they are making assumptions that interfere with their own ability to analyze the problem. TS staff must break out of that limiting mindset:

The \$#@*&^%! FORTRAN compiler doesn’t work!

Oh? That’s interesting. What’s the problem?

This program was working fine but now it doesn’t even compile.

So when did you last run it?

Actually, it was another person at another firm – but it was running fine!

Same model as ours? – a HORTENSE 5400?

No, uh, actually, it’s a UFORB series 876.

Well, how exactly did you get this source file, then? Email? USB flash drive?

Um, well, no, I actually typed it in from the listing. Why?

A well-disciplined, polite TS member would *not* burst into laughter or hang up the phone in frustration at this point nor offer the caller explicit instructions for, ah, anatomically-impossible body contortions.

DISTINGUISH OBSERVATION FROM HEARSAY

Everyone has likely played the child’s *Telephone* game of whispering a sentence to another person without checking on what they understood and then hearing the distorted version that comes out the other end of a long chain of transmission without error correction. CSIRT staff must always distinguish between first-person observations (“I read the log file and found...”) and hearsay (“Shalama read the log file and she found...”). Don’t trust hearsay: check it out yourself by tracking down the source of the information.

TS staff must be sure that they are being given *first-hand* knowledge of a problem. Second-hand information is too often missing essential details or includes outright errors. In addition, the person reporting second-hand information may not even have access to the system where the errors are occurring, making problem-solving difficult or impossible.

One of our programs has double softkeys showing up on screen.

What were you doing when it happened?

Running program ABC.DEF; got a second set of softkeys on the screen.

What do these softkeys show? The same as the original set?

I don’t remember.

Well, can you go try it again as we’re on the phone?

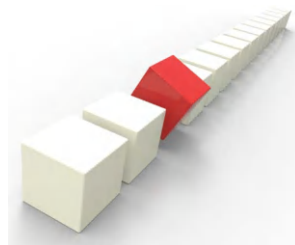


FIGURE 12.10 Spot the assumption.



FIGURE 12.11 Hearsay.

Uh, actually, I didn't see it myself; Charlie told me about it and asked me to call you.

Get Charlie.

[Charlie arrives...]

So Charlie, tell me again what happened.

Well, I was running program ABC.DEG when...

Wait a minute, not program ABC.DEF?

No, that one runs fine. Why?

DISTINGUISH OBSERVATION FROM HYPOTHESIS

Sometimes when people are careless or untrained, they don't distinguish between what they saw and an idea that might explain what they saw: a *hypothesis*. In the previous example about a supposed flaw in a firewall, the person speaking seemed to take the flaw for granted; that was an assumption. A similar problem can occur when someone thinks that *maybe* there's a flaw in the firewall and then proceeds as if that were true without testing their hypothesis. "And so maybe they exploited a flaw in the firewall, so we should patch all the holes right away." Putting aside for the moment the advisability of patching holes and firewalls, merely hypothesizing an exploit doesn't make it true. Maybe it's a good thing to patch the firewall, but it doesn't follow that it's the top priority right now simply from having thought of the idea. TS staff should be careful to think about what they're hearing and note explicitly when people are proposing explanations rather than reporting facts.

Some users (and some TS staff) seem to think that solving technical issues is more a matter of religious fervor than of scientific reasoning. They interpret *ideas* about what might be causing a problem as if what they think are *facts*. The TS team must always distinguish between what a user is claiming are basic facts and what the user *thinks* are facts. For example,

- There's some sort of problem with port 26 on system ALPHA; all we can get is an endless series of the letter "k" in lower case all over the screen. It's a hardwired connection, so it must be the computer.
- No, actually, the problem is the "k" letters all over the screen; we don't know yet whether it's a problem with
 - the screen or
 - the keyboard or
 - the cable between the screen and the keyboard or
 - the cable between the screen and the port or
 - the port or
 - the AIB micro-board or
 - the AIB itself or
 - the SIB or
 - the IMB or
 - the ATP driver or
 - the main memory boards or
 - the CPU boards or
 - the backplane connectors.



FIGURE 12.12
Hypothesis is not
fact.

CHALLENGE YOUR HYPOTHESIS

I hope you will forgive me, Dear Reader, for a brief foray into the philosophy of science. I do have a reason for bringing it up.

In the more than 50 years (as of 2024) I have been teaching college courses, I've taught biology, genetics, biochemistry, embryology, physiology, applied statistics, programming, software engineering, and IA. All of these subjects have involved a concept that some students have struggled to grasp: science depends on *disproof*, not proof. Empirical science (in contrast to logical systems such as mathematics) does not offer "proofs" in an absolute sense. Instead, a scientist formulates an hypothesis, defines a set of conditions and observations with predicted results and sees if there are grounds for rejecting randomness as a simple explanation of the deviation of the observations from the predictions. In many cases, scientists will assume the *absence* of a relationship or phenomenon (thus *null* hypothesis). Many experiments assume the *absence* of the interesting stuff and try to see if there are grounds for *rejecting* the simple explanation that there's nothing there but random activity.

Science works by *disproving* hypotheses, not by *proving* them. Mathematics and logic allow for proof; science does not. Explanations that cannot, by definition, be disproven are not part of a scientific effort.

Even more confusing for people who habitually think in terms of absolutes, even accepting the null hypothesis doesn't necessarily mean that there's nothing there. We may be measuring or counting too few occurrences to spot the cases that will challenge the non-existence of the phenomenon. There may also be confounding factors that obscure a real phenomenon.

But rejecting the null hypothesis does not, however, prove that any *specific* alternate hypothesis is necessarily correct. The evidence just restricts the *range* of reasonable hypotheses. We knock out explanation after explanation until what's left is a smaller set of explanations. In science, the best we hope for is not truth in an absolute sense but an operational equivalent to truth: useful enough to use for now.

OK, so now I want to bring this back to network management and the TS team. When your TS members develop hypotheses, they have to try to shoot them down. Trying to show that an idea is *correct* is – ironically – the wrong approach to testing hypotheses. Just as in quality assurance, we have to come up with ways of showing that our explanation is wrong. If we fail enough times to disprove an hypothesis using genuine, thoughtful, intelligent tests of our ideas, maybe we've got something useful after all. In summary, when we develop an idea about the causes of a problem, it's important to *test* the idea rather than baselessly *assuming* that it must be right and thus possibly wasting time on an irrelevant issue:

So let's see this terminal.

IDEA: If it's the port,

TEST: then detaching the RS-232 connector will stop the repeated "k" characters AHA, it doesn't.
The garbage has nothing to do with the link to the computer. So, we look at something else.

IDEA: Suppose it's the keyboard? Then

TEST: removing the keyboard connection will stop it. Yes indeed, it does. I see the connector's a little bent ... oh, I see: there's a pin out of place because perhaps someone forced the connector into place.

IDEA: If the pin is responsible, then,

TEST: perhaps bending it back will fix the problem.

Yes ... it works now.



FIGURE 12.13 Challenge your hypothesis.

TRACK THE DETAILS

TS staff should encourage the person reporting a problem provide as much detail as they can about how the issue arose. TS can guide the caller as follows:

- Sit down and reconstruct the events before trying out various solutions and workarounds.
- Have the caller write down everything they remember and include times if possible.
- What was the caller trying to do?
- How was the caller trying to do it?
- Were there any unusual events before the caller observed the problem?
- Exactly what did the caller observe?
- What did you the caller do to try to fix the problem and in what sequence?
- What's the current status of the system under discussion?



FIGURE 12.14 Tracking the details.

DON'T PREJUDGE WHAT'S IMPORTANT

TS staff need to be diligent in rooting out details of a problem. When a client calls with a problem description, TS should ask for as much information as the caller can supply. Sometimes what the caller perceives as irrelevant may be the key to understanding and solving the problem. For example,

CUST: We had a system failure AB3 a few minutes ago.

SUPPORT: Exactly what did were you doing?

CUST: The operator was working with spoolfiles. He changed the outfence on ldev 6, then tried to alter the priority of a spoolfile on a remote spooled printer. Oh – he made a typing mistake on the class name: used MAX even though we had removed that class name a week ago. Then he....

SUPPORT: WAIT! That's it! The bad class name! There's a known bug that causes this system failure when you refer to a nonexistent class name. We'll send you a patch.

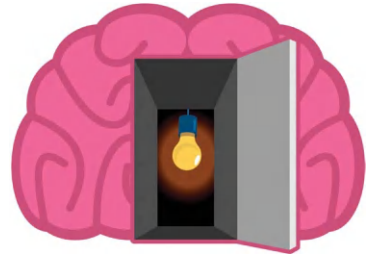


FIGURE 12.15 Keep an open mind.

RTFM - READ THE ... FINE ... MANUAL

Product manuals, whether for vendor systems or home-grown systems, should be electronic, not paper. Paper copies tend to be hard to find and cannot easily be accessed concurrently. They are also hard to keep up to date; having to find pages or sections that have changed and replace them by materials sent by the vendor makes about as much sense as storing the information in Sumerian cuneiform on clay tablets. Paper (and clay tablets) are difficult to search quickly, so if a manual is not available electronically, have it scanned. Store the electronic version with a descriptive name. Make sure that PDF versions are searchable and that all manuals are easily found by the users. There will be no problem with concurrent access.

As a matter of policy, ensure that users do *not* keep copies of the manuals. The copies will become out of date every time the vendor updates them.

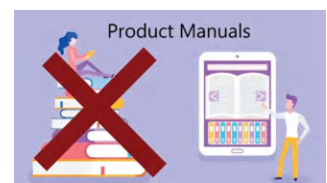


FIGURE 12.16 No more paper manuals.

If a vendor tends to update the manuals frequently, it may be a good idea to provide the users with the appropriate links but to ensure that the organization also downloads and stores the current version of each manual in case the vendors site goes down or the customer's Internet access is down.

USE UP-TO-DATE INFORMATION

Hardware and software vendors publish online bug or patch reports regularly. Be sure your TS staff are familiar with the links to access these reports. Just don't confuse system bugs with hemipteran insects, commonly called *true bugs*.

Keeping up to date with new vulnerabilities and exploits is an essential duty of security staff, especially as the number of new problems increases:

A record number of critical and high-severity vulnerabilities were logged to the NIST⁵ and its *National Vulnerability Database (NVD)*⁶ in 2020. The NVD is a repository of *Common Vulnerabilities and Exposures (CVEs)* reported by security professionals, researchers, and vendors. It is used by security teams around the world to stay up to date with security vulnerabilities as they are discovered.

In January 2021, *Redscan* performed an analysis of the NVD to examine security and vulnerability trends.⁷ Their report focuses on vulnerabilities discovered in 2020, but also highlights wider CVE trends that have emerged since 1989.

Key findings include:

- More security vulnerabilities were disclosed in 2020 (18,103) than in any other year to date – at an average rate of 50 CVEs per day.
- 57% of vulnerabilities in 2020 were classified as being “critical” or “high severity” (10,342).
- There were more high and critical severity vulnerabilities in 2020 than the total number of all vulnerabilities recorded in 2010 (4,639 including low, medium, high, and critical).
- Nearly 4,000 vulnerabilities disclosed in 2020 can be described as “worst of the worst” – meeting the worst criteria in all NVD filter categories.
- Low complexity CVEs are on the rise, representing 63% of vulnerabilities disclosed in 2020.
- Vulnerabilities that require no user interaction to exploit are also growing in number, representing 68% of all CVEs recorded in 2020.
- Vulnerabilities that require no user privileges to exploit are on the decline (from 71% in 2016 to 58% in 2020).
- 2020 saw a large spike in physical vulnerabilities.
- 70% of vulnerabilities expose a network-based attack vector.⁸

CERT/CC Resources

The *Computer Emergency Response Team Coordination Center (CERT/CC)* was developed in the wake of the Morris Worm of 2 November 1988,⁹ when it became clear that the Internet community needed some sort of central data repository and communications service to ensure rapid and effective response to emergencies affecting the Internet. Organized by members of the *Software Engineering Institute (SEI)* at *Carnegie Mellon University (CMU)* in collaboration with many other scientists and professionals, the CERT/CC gave rise to CMU's CERT Division:

The CERT Division is the birthplace of cybersecurity. For nearly 30 years, the CERT Division of the SEI has partnered with government, industry, law enforcement, and academia to advance cybersecurity and improve the security and resilience of computer systems and networks.

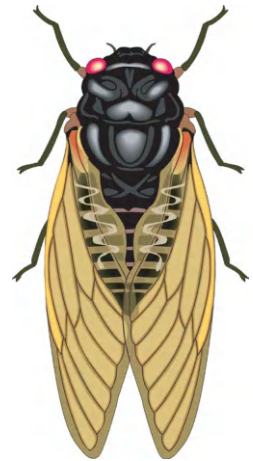


FIGURE 12.17 No, not *that* kind of bug!



FIGURE 12.18
CERT/CC logo.

Originally focused on incident response, we have expanded into cybersecurity areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threats, digital investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management.¹⁰

The CERT is an extraordinary source of unbiased, technically advanced information about security vulnerabilities, exploits, and patches. All CSIRT administrators should ensure that someone in their group is formally tasked with the responsibility of monitoring bulletins from CERT/CC. CERT/CC's *Vulnerability Notes Database* (VND) supplements the information in the *National Vulnerabilities Database* (NVD):¹¹

The *Vulnerability Notes Database* provides information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Most vulnerability notes are the result of private coordination and disclosure efforts.¹²

Other valuable security resources from the SEI include:

- SEI Podcasts – “conversations in software engineering, cybersecurity, artificial intelligence engineering, and future technologies;”¹³
- SEI Blog | CERT/CC Vulnerabilities – current commentaries about security issues,¹⁴
- SEI Blog | Insider Threat – “research, modeling, analysis, and outreach to develop data-driven, socio-technical solutions that help organizations reduce the impact and likelihood of insider threats;”¹⁵
- SEI Digital Library – “access to more than 5,000 documents from three decades of research into best practices in software engineering. These documents include technical reports, presentations, webinars, podcasts, and other materials searchable by user-supplied keywords and organized by topic, publication type, publication year, and author.”¹⁶

CERT/CC's Cybersecurity Center Development offers valuable courses for creating, maintaining, and improving CSIRTs:¹⁷

- *Overview of Creating and Managing CSIRTs*: “This one-day course highlights the best practices in planning, implementing, operating, and evaluating a ...CSIRT;”
- *Creating a Computer Security Incident Response Team*: “This one-day course provides a high-level overview of the key issues and decisions that must be addressed in establishing a CSIRT. Attendees will develop an action plan that can be used as a starting point in planning and implementing their CSIRT;”
- *Managing Computer Security Incident Response Teams*: “This three-day course provides current and future managers of computer-security incident response teams (CSIRTs) with a pragmatic view of the issues that they will face in operating an effective team;”
- *Foundations of Incident Management*: “This four-day course provides foundational knowledge for those in security-related roles who need to understand the functions of an incident management capability and how best to perform those functions;”
- *Advanced Topics in Incident Handling*: “This four-day course, designed for technical personnel with several months of incident handling experience, addresses techniques for detecting and responding to current and emerging computer security threats and attacks.”

CVE and ICAT Metabase

The home page of the CVE (transitioned to [CVE.ORG](https://cve.org) over the course of 2022) includes this succinct description:

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.



FIGURE 12.19

CVE logo.

Vulnerabilities are generally viewed as any aspect of a system or product that allows a breach of security (i.e., a breach of confidentiality, possession, integrity, authenticity, availability, utility or any combination of these principles. The CVE defines vulnerabilities and exposures as follows:

A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components.¹⁸

In the early days of the CVE, experts proposed the following definitions which remain useful in analyzing problems:

- A “universal” vulnerability is one that is considered a vulnerability under any commonly used security policy that includes at least some requirements for minimizing the threat from an attacker. (This excludes entirely “open” security policies in which all users are trusted, or where there is no consideration of risk to the system.)
- The following guidelines, while imprecise, provide the basis of a “universal vulnerability” definition. A universal vulnerability is a state in a computing system (or set of systems) which either:
 - allows an attacker to execute commands as another user.
 - allows an attacker to access data that is contrary to the specified access restrictions for that data.
 - allows an attacker to pose as another entity.
 - allows an attacker to conduct a denial of service.
- The following guidelines provide the basis for a definition of an “exposure.” An exposure is a state in a computing system (or set of systems) that is not a universal vulnerability, but either:
 - allows an attacker to conduct information-gathering activities.
 - allows an attacker to hide activities.
 - includes a capability that behaves as expected, but can be easily compromised.
 - is a primary point of entry that an attacker may attempt to use to gain access to the system or data.
 - is considered a problem according to some reasonable security policy.¹⁹

SANS Newsletters

SANS provides many resources. Among many other useful services, SANS offers three free email publications of interest to network managers:

- *SANS NewsBites* is a semiweekly executive summary of the most important cyber security news articles published recently. Each news item is annotated with important context provided by respected subject matter experts within the SANS community.²⁰
- *@Risk*: A weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data.²¹
- *OUCH! Newsletters* is the world’s leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the SANS Security Awareness team, instructors, and community members.



FIGURE 12.20
SANS.

Each *OUCH!* is developed through a rigorous process involving numerous community volunteers, including translators, subject matter experts, and editors.²²

Risks Forum Digest

The distinguished computer scientist Dr Peter G. Neumann²³ of the *Computer Science Laboratory* at *SRI International* founded the *Risks Forum* (the full name is *Forum on Risks to the Public in Computers and Related Systems*) of the *Association for Computing Machinery* (ACM) in 1985. This regular publication accepts contributions from professionals around the world who report on cybersecurity issues, including attacks, system errors, software vulnerabilities, and so on. The entire collection of tens of thousands of contributions is available and anyone can subscribe to the email version of the reports.²⁴ The Digest also includes comments from readers on previous articles.

Here is the table of contents from Volume 33, Issue 84 (September 2023)²⁵ to provide readers with a sense of the diversity of content available in the publication:

- Pratt Engine Flaw to Idle Hundreds of A320 Planes for Years (Yahoo!)
- China Uses AI to Spread Lies about U.S. fire (NYTimes)
- AI voices are taking over the Internet (The Verge)
- Another group of writers is suing OpenAI over copyright claims (The Verge)
- Some things to talk with your kids about AI (MIT Tech Review)
- How the Navy Spent Billions on Failed Littoral Combat Ship Program (ProPublica)
- Voting rights activists sound alarms over private tool that could lead to canceling voter registrations (CNN)
- Teen's Smart Pill Bottle Reminds People to Take Their Medication on Time (The Institute Alert)
- How to Navigate Apple's Shift from Lightning to USB-C (NYTimes)
- FTC says Elon Musk may have jeopardized data privacy and security at Twitter (Enqadget)
- Susanna Gibson Saga: So, What if a Candidate Livestreamed Sex Acts with Her Husband? (Politico)
- Re: San Franciscans Are Having Sex in Robotaxis (Henry Baker)
- Re: Pedestrian dies after Cruise cars block ambulance (Steve Lamont)
- Re: Vintage Car prices (Anthony Thorn)
- Info on RISKS (comp.risks)

THE RISKS DIGEST

FIGURE 12.21 RISKS logo.

Crypto-Gram Newsletter

Another valuable resource for keeping up to date on security news is Bruce Schneier's²⁶ monthly *Crypto-Gram Newsletter*.²⁷ The issue for September 15, 2023, has the following topics:

- Zoom Can Spy on Your Calls and Use the Conversation to Train AI, But Says That It Won't
- UK Electoral Commission Hacked
- Detecting "Violations of Social Norms" in Text with AI
- Bots Are Better than Humans at Solving CAPTCHAs
- White House Announces AI Cybersecurity Challenge
- Applying AI to License Plate Surveillance
- December's Reimagining Democracy Workshop
- Parmesan Anti-Forgery Protection
- Hacking Food Labeling Laws
- Remotely Stopping Polish Trains

Schneier on Security

Crypto-Gram Newsletter



FIGURE 12.22 Crypto-Gram newsletter.

- Identity Theft from 1965 Uncovered through Face Recognition
- When Apps Go Rogue
- Own Your Own Government Surveillance Van
- Spyware Vendor Hacked
- Inconsistencies in the Common Vulnerability Scoring System (CVSS)
- Cryptocurrency Startup Loses Encryption Key for Electronic Wallet
- The Hacker Tool to Get Personal Data from Credit Bureaus
- LLMs and Tool Use
- On Robots Killing People
- Cars Have Terrible Data Privacy
- Zero-Click Exploit in iPhones
- Fake Signal and Telegram Apps in the Google Play Store
- Upcoming Speaking Engagements

The Privacy Professor

Rebecca Herold has developed a wealth of useful materials including the free *Tips of the Month* and free and premium electronic courses. The newsletters are particularly valuable as free resources that can be distributed to all personnel because they are written in plain language and address issues that affect not only corporate security but personal cyber-safety.

Her *Privacy & Security Brainiacs* site includes the following summary of her work:

Privacy & Security Brainiacs® covers all areas of privacy, information security, cybersecurity, and compliance topics, in all areas of the world. A few of the areas where we have deep expertise, and have hands-on real-life experience, performed research, and have co-authored informative references, such as government standards, guidelines, and directives, include:

- Healthcare and associated industry regulations (e.g., HIPAA, HITECH Act, and others)
- Internet of Things (IoT) and associated environments
- Call centers
- Residential care facilities (assisted living, gated communities, group homes, dormitories, etc.)
- Software development
- Law enforcement
- Agriculture
- Electric grids, and associated critical infrastructure utilities
- Technology vendors
- Financial
- Retail
- Education
- Government agencies....²⁸

Free online courses include:

- Work from Home Security and Privacy
- HIPAA for Business Associates Overview
- HIPAA Privacy Rule Overview
- HIPAA Security Rule Overview
- HIPAA Enforcement Summary for Q3 2020
- HIPAA Enforcement Summary for Q4 2020
- HIPAA Enforcement Summary for Q1 2021
- HIPAA Enforcement Summary for Q2 2021
- HIPAA PHI Use: Overview of When to Protect PHI, and Acceptable PHI Uses.



FIGURE 12.23

Rebecca Herold's logo.

Paid courses (to which she and I are planning to add some of my own contributions) include:

- HIPAA Basics for Business Associates 2023 Edition
- HIPAA Basics for Covered Entities 2023 Edition
- HIPAA PHI in Use
- Call Center Information & Privacy Basics
- HIPAA Privacy Rule Basics
- HIPAA Security Rule Basics
- HIPAA Basics: Noncompliance Penalties
- HIPAA Basics: CEs, BAs, and PHI.²⁹

HANDLING DIFFICULT CALLS

Not only should managers look for and ensure adequate technical knowledge, but also they should select and enhance interpersonal skills and disciplined work habits.

TS members inevitably work with some users who are stressed by the problems they are facing. It is no help to have a technical wizard who so offends the users that they stop cooperating with the problem-resolution team. Sometimes, TS staff forget that their job includes not only resolving a technical issue but also keeping the clients as happy as possible under the circumstances – and the use of the word “clients” is deliberate here.

Social scientists have been studying how people act and interact in groups for many years. My late father-in-law, Dr Percy Black, z”l, was a distinguished social psychologist who worked as a consultant to industry for decades as well as being a highly regarded university professor and author.³⁰ He introduced me to his field in the late 1980s; I realized how valuable the insights of this academic field could be for IA and presented a paper on the topic in September 1993 at the *16th National Computer Security Conference* sponsored by NIST.³¹ That contribution won the *Outstanding Paper Award* at the Conference and was updated as a chapter in the *Computer Security Handbook* editions.³²

The following sections summarize key points about social psychology in the context of managing TS groups; however, readers interested in details and academic references need merely consult any university text on social psychology. An updated version of the original paper is in [Chapter 13](#) of this textbook.



FIGURE 12.24
Angry caller.

SOCIAL COGNITION: FORMING JUDGEMENTS ABOUT ISSUES

How people explain their own and others’ behavior can influence how they interact and how they interpret communications. In TS, staff members’ perhaps unconscious models explaining callers’ behavior can influence their judgment and their interactions with the clients.



FIGURE 12.25
Judgement.

SCHEMAS

All of us use models of reality (*schemas*) to make sense of what we experience. Schemas

- Organize knowledge about the world
- Influence perceptions
- Affect memory
- Are more subtle and complex for in-groups than for out-groups
- May lead to self-fulfilling prophecies

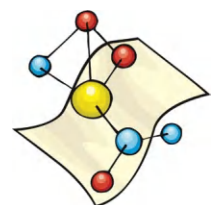


FIGURE 12.26
Schemas.

Problems can develop because of rigid schemas:

- Decision-making usually includes only a small subset of available information
- Early, negative, information weighted heavily
- Judgements are often based on inadequate samples
- The availability heuristic can lead to errors in judgment
- Language influences perception.

TS staff must be conscious of the dangers of allowing preconceptions to cloud their evaluation of reality. For example, a caller who made some egregious errors in a past call to the helpdesk may have such a bad reputation among the TS crew that anything the caller says thereafter, no matter how carefully observed and accurate, can be dismissed as unworthy of attention. The fact that, for example, such a caller may have been suffering from pneumonia or under the influence of a medication when the errors occurred may be unknown to the TS staff, but the damage is done because they are unaware of the dangers of such negative interpretations.

On the other extreme, a caller may be jovial, friendly, and fun to talk with, but those positive features of behavior and personality don't justify having the TS staff treat everything the caller says as gospel truth without the usual careful analysis and fact-checking. Prejudice can be positive, not just negative; in either case interpretations may be swayed by such interpretations.

WEINER'S CLASSIFICATION

Bernard Weiner's 1979 paper introduced a widely respected model for how human beings interpret other people's behavior.³³ The orthogonal factors are what stimulates the behavior (internal or external issues) and the predictability of the behavior (stable or unstable). The figure shows how different interpretations fall into the four classes of explanations.

In TS, we have to cope with all of the types of behavior and their causes. For example, Albert may call on Monday in a state of exhaustion and be hard to understand; on Tuesday, he may be in a great mood because he just got a date with a co-worker – and as a result is Mr Friendly and Competent. Similarly, Betty may be a terrible nuisance on a call on Wednesday because of her consistent refusal to read manuals; on Thursday she may have drunk an extra cup of coffee and finally exercised her intelligence effectively.

A number of errors of interpretation result from mistaken attributions and can interfere with the rational interpretation of information from TS clients and also difficulties for managers:

- Fundamental Attribution Error
 - Star Trek's Leonard Nimoy is really like the character he portrays (Mr Spock).
 - This caller must be stupid because he doesn't know what I already know.
- Actor-Observer Effect
 - What I do is a reasonable response to the situation but what you do is in your nature.
 - When I typed the wrong command in the error was due to a confusing user interface.
 - When the caller typed the wrong command it was because of something wrong with them.

	Stable	Unstable
Internal	Dispositions; traits; level of ability or intelligence	Effort; mood; physical state
External	Degree of task difficulty; env helps/hindrance	Good/bad luck; opportunity; transient situations

FIGURE 12.27 Weiner's grid.

- Salience
 - What stands out is perceived as most important even if it isn't.
 - This client is the only member of the accounting department who is an immigrant from Jonsonia, so therefore the problem she is reporting must be due to lack of understanding of English.
- Self-Serving Bias
 - If I succeed it's because of how good I am, but if I lose it's not my fault.
 - Billy-Bob has problems with his Internet connection because he's incompetent.
- Self-Handicapping
 - If I expect to fail I'll make sure there's a good excuse.
 - As a TS team member, any mistakes I make are due to overwork and stress of the job.
- Depressed People
 - If I lose it's because of how bad I am, but if I succeed it's not to my credit.
 - The reason I have so many unsolved cases from the Sales Department must be because I'm incompetent.
 - The reason I have so few unsolved cases from the Shipping Department must be pure luck.

TS managers should be on the lookout for warning signs of any of these errors of judgment and help the staff avoid falling into negative attitudes that interfere with service to the client base.

PREJUDICE

Some of the most dangerous schemas are based on preconceptions about people because of their membership in particular social groups, e.g., country of origin, "race," gender, religion, disability, sexual orientation, familial status, and so on.³⁴

The basis message is one that I enunciated to my students: don't make assumptions about people based on group membership; *get to know each person individually*.

Some of the key points to raise in training TS staff to avoid falling into traps of prejudice include the following:

- Stereotypes are simple models of others.
- Roots of prejudice are many.
- The authoritarian personality includes prejudice.
- Minimal-group research shows how easy it is to generate inter-group hostility and prejudice.
- Group competition exacerbates prejudice.
- Creating common goals and projects for hostile groups mitigates prejudice.
- Favorable depictions improve inter-group relations.

Such training improves the performance of the TS group because *no one* is treated negatively because of prejudice. In a larger sense, such training can be a contribution to the improvement of society as a whole when the participants apply their learning to their behavior in the wider world.

There are classic texts about prejudice that can provide detailed research and analysis for further study.^{35,36}



FIGURE 12.28
Resisting prejudice.

PERSONALITY TYPES

At HP worldwide in the early 1980s, every single employee in the company had to complete a fascinating course from *Wilson Learning*. At the time, it was called the *Social Styles Series* but today it's called *Building Relationship Versatility: Social Styles at Work*.³⁷

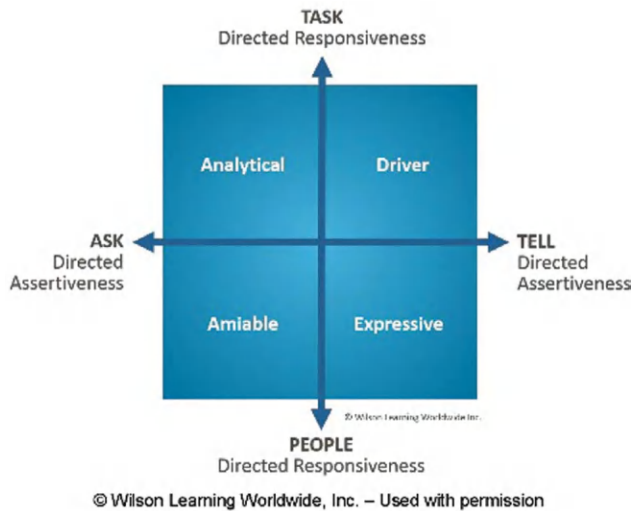


FIGURE 12.29 Wilson typology.

I think it was one of the most useful courses I have ever completed. The model helped all of us interact with fewer conflicts and greater understanding of the preferred styles of interaction of colleagues and clients. Our TS staff in the *Phone-In Consulting Service* (PICS) were able to interact more constructively with our clients because we were less likely to misinterpret the clients' preferred styles of interactions as forms of aggression or stupidity.

The main point of the course is that we must not dismiss or criticize others because their preferred social interactions differ from ours. Understanding preferences for social styles helps us avoid conflict and improve cooperation. The following sections summarize key points of each of the four main personality types in this typology.

DRIVER

- High assertion, low affect
- “You can have 7 minutes.”
- Time-sensitive, relatively unemotional, goal-directed
- “I enjoy the challenge.”
- Not interested in how people feel
- Not interested in how a problem was solved
- Concerned about results above all
- Dislikes being told what to do



FIGURE 12.30
Driver.

ANALYTICAL

- Low assertion, low affect
- “There are ... 4 reasons why...”
- Averse to deadlines, focused on fact-gathering
- “I learn so much here.”
- Not interested in how people feel
- Can lose track of global context by focusing on details
- Dislikes being told to stop research



FIGURE 12.31
Analytical.

AMIABLE

- Low assertion, high affect
- “How do you feel?”
- Focused on interpersonal relations
- “I love the people here.”
- Needs to establish a friendly basis for work
- Good conciliators
- Resents impersonality



FIGURE 12.32
Amiable.

EXPRESSIVE

- High assertion, high affect
- “Let’s get out there and win!”
- Focused on group achievement and acclaim
- “I enjoy being part of a winning team!”
- Excellent motivators
- Weak on details and follow-through



FIGURE 12.33
Expressive.

There’s a particular example I have used for years to illustrate the value of the *Wilson Learning* model. Around 1983, my TS team spent three 18-hour days working on a series of system failures of the HP3000 computer used in a large electronics factory. The failures were occurring apparently randomly throughout the day with fewer at night, when there was little activity in the factory. Our team of three system engineers (SEs) eventually found that the failures occurred predictably when electric forklifts traveled over a section of the floor where cables were connecting the HP3000 to some of the terminals. Turned out that these large battery-operated vehicles were generating induced voltage pulses that overloaded the HP3000 terminal interface. When we moved the cables to overhead conduits, the system failures stopped.

After the three days of work, I reported to the manager who had called us in for help. I had been told that he was a Driver in the Wilson typology, so I knew that he would appreciate a short-finned report. I walked into his office and said, “Problem is solved.” He asked, “Will it happen again?” I said, “Unlikely.” He said, “Thank you.” That was the end of the one-minute conversation following all that work. I was *not* offended: I knew that he was actually happy.

Sure enough, my boss received a letter from the client manager praising our team for our work and singling me out for my “professionalism.” I don’t think he would have been as pleased if I had bloviated lots of technical details he did not need.

INCORRECT AND DANGEROUS PERCEPTIONS

Misunderstanding others because we differ in social styles can lead to frustration. Without training and support, it’s easy for someone to misjudge colleagues or clients who have different preferences. Differences in personality style can even result in hostility.

As the figure indicates, people who are unaware of perfectly normal personality types can decide that people whose interpersonal styles are different on both of the Wilson Typology axes must be *bad*. Thus an Analytical may perceive an Expressive as a clown; the Expressive may see the Analytical as a robot. Similarly, a Driver may be irritated by an Amiable and see them as a wimp; the Amiable may be offended by the curtness of the Driver and see them as a dictator.

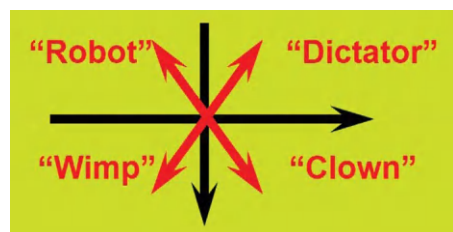


FIGURE 12.34 Errors of interpretation.

Once at HP, my colleague and friend Gilles and I – both *Analyticals* – were chatting over lunch when our friendly, bouncy colleague Sylvie (a wonderful *Expressive*) asked if she could join us. “Of course,” we both said. As soon as she had put her cafeteria tray down, we resumed our detailed discussion about the operating-system internals responsible for a particular type of system failure. She looked from one to the other of us, said, “You guys are incredibly boring” and flounced off in disgust. That was an example of a difference between an *Expressive* and two *Analyticals*. She hadn’t absorbed the principles of the Wilson Typology, but the two of us had, so we just chuckled instead of being offended.

CLIENT SUPPORT

There are clients who are frustrated, angry or just plain rude, and TS staff must be trained in how to handle themselves and their clients when conflicts arise. TS staff have to learn to be supportive coaches, not punitive critics.

HOW TO ENRAGE TS CLIENTS

There are some well-known responses from TS staff that can offend clients; here are some of the most time-to users I have run across in my 40 years of technical support followed by my comments in square brackets:

- “No one has ever complained about this before.” [So what? If the problem is real, we should thank the user for reporting it, not make veiled criticisms that imply that the problem can’t be real.]
- “I don’t have time for this now.” [*That’s a time-management problem for the TS team, not for the client. Take responsibility for getting the right person to take charge of the problem in real-time.*]
- “Why don’t you try calling ...?” [*Same comment as just above.*]
- “That’s not my problem.” [*Just plain rude as well as irresponsible.*]
- “Why don’t you reload the operating system and call me back if it happens again?” [*Significant risk and time-cost for the client; often the first line suggestion of the terminally incompetent technician.*]
- “Just format your hard disk and see if it happens again.” [*Even worse than the previous suggestion if it is just a casual suggestion to get the client off phone for now.*]
- “Don’t get mad at me – I just work here.” [*A professional will understand that there’s a difference between criticism directed at the organization or its procedures versus a direct ad hominem attack. The former should be taken seriously and passed on to people who can evaluate the seriousness of the criticism; the latter can be unacceptable and should be passed on to a manager who can explain the need for civility even under stress.*]

HANDLING IRATE CLIENTS

Tech support must handle irate clients well. Some of my instructions to my colleagues and employees in the TS teams I managed included:

- Support the client’s feelings.
- Take responsibility for getting a solution under way.
- Don’t take insults/abuse personally: stay cool.
- Continued abuse should be reported to operator’s supervisor immediately.
- Practice role-playing.



FIGURE 12.35
Coach.



FIGURE 12.36
Nasty TS person.



FIGURE 12.37
Enraged caller.

Research and practice show that experiencing a situation, even if only in role-playing, helps people handle the real thing more effectively. TS training should include sessions for practice in dealing with trouble. The outline of the exercises is as follows for each pair of team members:

- A team member takes role of a client calling the TS line.
- Another team member plays the role of the TS staffer answering the call.
- The exercise begins with a pleasant caller reporting a problem.
- The next phase of the exercise has the “caller” pretending to be slightly angry.
- The third phase works up to handling an angry caller.
- The final practice involves calming down a furious, out-of-control, abusive caller.

These exercises can be based on scripts, but it’s actually more fun and (in my experience) to encourage the staffers to use their own experiences in more spontaneous role-playing.

The pairs of TS staff switch roles when the set of exercises is complete. Not only is it more fun for each pair, but it also ensures that both members have practice in handling the problematic calls.

These exercises are particularly effective not only for helping raise awareness of the importance of avoiding unthinking, emotional responses but also for increasing the sense of teamwork within the TS group. They’re fun!

SYSTEMATIC RESPONSES

TS staff should be trained for *systematic problem-solving* for clients. For example, each team member should explicitly be told and should integrate the principle that they must take *responsibility* for getting the problem solved.

- Ask for details of problem.
- Write down what client says.
- Tell client when you will call back with a progress report.
- Call back on time.

If it takes longer than normal or than expected by the client to solve a technical problem, *call the client back with progress reports*. Regular contacts reassure the client that their problem is not being ignored. They also offer opportunities for additional questions and answers that may help solve the problem.

Clients can be highly and justifiably irritated when a problem has been solved but there’s a delay in notifying them. TS must routinely

- Call client back as soon as possible.
- Explain problem and solution using appropriate level of detail.
- Thank the client for having notified you of the problem.

WHAT IF THE PROBLEM STILL ISN’T SOLVED?

There must be a formal *problem-escalation procedure* when the first-level TS team has been unable to solve a problem *within the time-limit for that level of support*. In other words, the team must promptly bring a problem up to succeeding levels of expertise and resources. For example, the diagram below describes how technical problems can be escalated from the routine (normal) TS team upwards through four additional levels (the number of levels isn’t the point here).



FIGURE 12.38 Callback.



FIGURE 12.39 Escalation.

Not all problems can be solved with a single call and response. The helpdesk team must follow clearly defined procedures for handling problem that cannot be solved in the first interaction. Some key principles include the following:

- Keep support tickets open until the problem is solved to the *user's* explicit satisfaction.
- Define a second-level support team with advanced knowledge and extensive experience to handle difficult calls about specific systems.
- Define limits based on problem priority for how long the first- and second-level teams can allow a ticket to remain open.
- Ensure that the helpdesk team has all requisite information for getting support from an appropriate vendor or other external source.
- Check online user communities for extra help and insight when coping with difficult problems.
- Ensure that the helpdesk team members know the *vendor* escalation schedule for unsolved problems.
- Monitor the tickets to ensure proper escalation by vendor support.
- Keep the helpdesk's upper management informed at every step of *critical* issues (not user lack of training or user errors).
- In extreme cases, arrange meetings of high-placed executives with vendor executives of similar levels.
- If the vendor cannot or will not resolve the technical issue, consider openly contacting the vendor's competition to increase pressure for resolution.
- Involve corporate legal staff as last resort if the vendor is in breach of contract for quality of support.
- Provide full information to vendor support team.
- Document problem resolution in detail.

What is important is that there be a defined time limit for allowing a problem to remain unsolved; at that point the problem is sent to the next level. Every level must have its own defined time limit.

- In this example for software support, the initial team member transfers responsibility to the second-level team of specialists – perhaps TS staff with more years of experience in a particular subset of the products under support.
- After a defined time limit, the problem moves to the Senior staff – perhaps people with decades of experience.
- If necessary, they can then send the problem to the labs where specialists manage the software month by month, preparing updates or patches as they cope with problems reported from the field.
- As a last resort, the author(s) of the program code may have to get involved in analyzing and solving the problem if it's clear that it resides in design or coding errors.

This approach was used at HP when I was working there; it worked well – we had excellent industry reviews and happy customers!

MAKE USERS PART OF THE TECH SUPPORT TEAM

The only reason that there's a TS team – as distinct from a network/computer management team – in an organization is that the IT systems exist for the *users*: colleagues in the organization and external customers. It's important that all the TS staff perceive users as *us* not *them*; everyone in the team, and especially managers, should be referring to the users as *customers* even if they are in fact colleagues. In a sense, the users of the TS services pay the

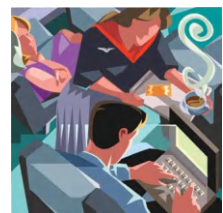


FIGURE 12.40
Users.

salaries of the staff. It's critically important for everyone in the team to prevent abusive language about these customers. "That idiot in Accounting..." or "The nuisance in Facilities..." are unacceptable descriptions for long term success of the TS group.

The other side of the relationship is to train users to think about tech support as *us* not *them*. I recommend that there be regular meetings of the TS group with various user departments so that users can voice their needs easily. The TS crew can learn from the questions and comments that might not otherwise arise. The TS team might be able to arrange visits by users to the TS center, perhaps with guided tours showing the users the facilities and the equipment as part of the effort to increase warm relations. Certainly, TS management should enforce unfailing politeness toward users, but also user managers would do well to ensure that their employees maintain courtesy when calling for help.

One helpful technique to build and maintain solidarity between TS and their users is to have periodic recognition of users who were quick to report important failures. Such awards can be publicized in a large organization's internal news and with posters; in smaller organizations, the publicity may simply be word of mouth and email.

KNOW YOUR USER COMMUNITY

The TS team will improve its *quality of service* (QoS) by learning as much as possible about their users. Priorities can differ; skills can differ; time-sensitivity can differ. The TS team should have profiles available with as much detail on the user community as possible to ensure the best QoS defined for each group of customers. QoS must vary to reflect the time-sensitivity and operational importance of each caller, e.g., in a hospital TS team, a call from staff experiencing technical problems with their blood-pressure monitors in the middle of a surgical operation must be considered top priority. A simultaneous call from the accounting department reporting that next month's billing isn't printing properly two weeks before their deadline cannot be considered top priority at that point.

What should the TS optimize for the different sectors of their customer base?

- Response time?
- Program development?
- Maintenance?
- Costs?
- Human relations?
- Client services?
- Problem avoidance?
- Learning new techniques for better work?

Determining priorities depends on thorough knowledge of the user community, e.g.,

- Where are the users in the organizational structure? Are they all in the same department, the same company, the same corporation, the same university, the same hospital – what?
- Are the users clerks? Managers? Executives? External customers?
- Do the users have technical knowledge? Are they data-entry clerks? Programmers? Network administrators? Emergency-response team members?
- Why do your users choose your service? Are they captive users who have no choice in where they get support or are they discretionary users who have alternatives?

To collect current data with which to answer these questions, the TS team must engage in thorough research to find the answers. Tools include:

- Questionnaires or surveys
- Group meetings



FIGURE 12.41

Get to know
your clients.

- Focus groups
- Individual interviews

Analysis of such information benefits from CAC and CATA, as described in previous sections of this text.

A 2021 study of HP's customer-satisfaction techniques has many details of the company's consistent efforts to maintain close relationships with its customers. The company worked with the Medallia services firm for real-time, multi-dimensional feedback from its customers:

HP brings together experience signals from three perspectives to guide product development and life-cycle management. First, business analyst teams use Medallia to gather data about customer emotion, captured through direct solicited customer feedback. For instance: Do they love a particular feature? Are there specific aspects of the product they'd like to see improved? Second, the team collects aggregated telemetry data for device usage and performance from customers who have opted in to share this information. These two data sources are then analyzed together and (when necessary) compared to the third data source: expected product experience as designed in the lab. Triangulating these data sources allows HP to find the true root cause for issues identified in the customer sentiment data. This analysis process is mostly manual for now, but HP is pursuing automation to help it scale....

HP uses Medallia to monitor experiences across the product lifecycle, with a goal of creating exceptional end-to-end experiences. Their approach incorporates other services and communications as an integral part of the product ownership experience: from awareness and consideration, purchase journeys, product setup, configuration, everyday product use, and getting support for questions or issues. ³⁸

TECHNICAL TRAINING

Everyone in TS must have basic knowledge of features of the systems they are supporting. There are many resources available, including some that are entirely online and others that involve in-place courses or travel to vendor locations. A variety of training tools help a TS team provide the best possible service to the customer community. Here are some ideas to help organize such training.



FIGURE 12.42 Training.

- Vendor courses
 - Operators benefit from product-specific courses
 - Managers need familiarity with vocabulary and concepts to work effectively with vendor TS
 - Crash-recovery courses centered on specific systems may be appropriate for larger shops
- Other external training
 - Product seminars from vendors are widely available
 - Trade-shows provide enormous opportunities for learning about current products as well as about competitive choices
 - Regional platform-specific user groups offer knowledge transfer among practitioners
 - Software-specific user groups & *Special Interest Groups* (SIGs) online offer a wealth not only of posted information but also opportunities for forming professional relations among experts
 - National/international meetings offer new information and novel perspectives
 - Industry trade associations can help TS members deepen their knowledge by sharing experiences and perspectives
 - Community-college courses are increasingly available online, obviating the need for attendance at specific locations
 - Universities also offer a wide range of continuing-education courses even without having to enroll in degree programs

- In-house training speeds the integration of new employees and widens the competence of established TS members
 - Local standards for specific tools such as Job Control Language (JCL), etc.
 - Special user-defined command catalogs for operations
 - Computer Assisted Instruction/Computer Based Training (CAI/CBT) packages
 - Seminars for/by staff
 - Distribution of readings for stimulation and discussion
- Training never stops
 - Integrate face-to-face training every day
 - Part of internal communications needed for good working environment
 - Training encourages personnel to share knowledge
 - Set aside fixed periods for peer-to-peer cross-training
 - Properly done, training enhances self-confidence
 - Discourage punitive responses to errors or questions
 - Admit ignorance cheerfully and naturally and find answers.

THE REDUNDANCY RULE

For effective operations even if certain key staff members are unavailable (think of the COVID-19 pandemic), it is essential that organization knowledge be distributed within the organization, not held by only one specific individual. My “redundancy rule” is that *no information shall be known to only one member of the team*. Information distribution prevents indispensability and allows the team to handle sick days, holidays, and periods of overload. The team can respond to peak demands without blowups. Effective information-sharing is also a solid basis for career advancement, motivating employees to learn by recognizing knowledge and talent through promotions.

Information sharing also provides different perspectives on problems; members may contribute insights based on their experience and on skills they have honed in different aspects of their work. The collegial atmosphere encourages team spirit and enhances self-respect.

BEWARE THE UNBRIDLED EGO

In teamwork, a destructive tendency is for some insecure members to compensate for their low self-image by becoming egoists.³⁹ Occasionally there are also narcissists who infiltrate our organizations and politics and wreak havoc.⁴⁰ It's difficult to cope with these behavioral problems, but even without psychiatric training, one can provide practical advice for such team members:

- Don't assume everyone else knows your thoughts
 - Write instructions down (giving and receiving) – records matter immediately and in the future
 - Repeat what you think are your assignments – quality control for communications
 - Avoid pronouns (it, he, she, they) in tech talk – be specific to avoid ambiguity
- Take criticisms as helpful
 - Everyone makes mistakes – don't feel that you are somehow a defective person
 - Don't think of analysis as an attack – work as a team member to improve process
 - Everyone can improve – aim for CPI



FIGURE 12.43
Redundant knowledge is good.



FIGURE 12.44
The narcissist.

- Total quality depends on team commitment
 - Analyze communications within the team – look for and improve miscommunication
 - Analyze problem definitions – make sure everyone shares the same concepts and terminology
 - Praise *teams* for successes even while recognizing *individuals* for outstanding performance.

WORKING WITH VENDOR SUPPORT

Having worked on TS for years in organizations that provided services to customers, I learned and articulated some straightforward principles for working effectively with service providers.

From the very start of the relationship between vendor and customer, the clients should establish basic principles for managers deciding on competing vendors and contracting with the chosen ones:

- *Avoid the bleeding edge*: organizations that depend on reliability of services for critical functions would do well to evaluate the experiences of similar clients with vendors who offer radically new services.
- *Don't buy on price alone*: evaluate reliability and QoS with existing customers of the candidate vendor.
- *Evaluate your sales contact from the candidate vendor*: be sure that different members of your own staff are receiving consistent information and professional behavior from the sales person.
- *Determine your own corporate liaison to the vendor*: assign a specific person in your organization to be the main contact with the vendor. Ideally, your candidate will have extensive experience in the specific service or product line of the vendor.
- *Specify all service commitments in the contract*: include response times, escalation procedures, and other aspects of QoS and specify possible consequences of violating those terms.
- *Do not tolerate illegal or unofficial deals*: no secret, verbal, private commitment are to be accepted. Indeed, any proposal for such covert operations should be grounds for refusing the contract and reporting the dishonest agent to their employer.
- *Never buy under pressure*: terms such as “this offer is valid for only the next week” should raise suspicions about the trustworthiness of the vendor.
- Have a named *scribe* write down minutes of all meetings with vendor staff and distribute those records to all participants of the meetings. Participants must be encouraged to send corrections to the scribe to update the minutes. The meeting organizer should always get agreement on specific dates and times for specific commitments from the vendor (and from employees of the client as well).

Some of the specific recommendations for support from software vendors are enumerated below.

VENDOR RESPONSIBILITIES

- *Source code must be in escrow*: there's a risk to the customer of having the vendor stop supporting a software product or insisting on upgrades that may not be acceptable to the client because of hardware limitations or interactions with other software products.
- *Phone-in consulting service*: there must be a helpdesk available for all the time during which the customer's systems are in production. For example, if a hospital runs its patient-registration system

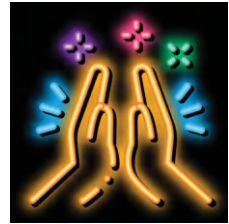


FIGURE 12.45
Collaboration.



FIGURE 12.46
Software vendors.

365/24, it would be unacceptable to contract with a software supplier whose helpdesk runs for only 12 hours a day on weekdays only.

- Online channels for support should include specific email addresses or websites for sending documentation to the vendor's helpdesk staff.

CLIENT RESPONSIBILITIES

- Every organization should identify a specific problem-manager for each problem or type of problem.
- It's important to characterize each problem with as much *relevant* detail as technically competent staff judge to be necessary to communicate to the vendor personnel.
- If a problem is not universal (that is, it appears and disappears depending on circumstances), TS staff should experiment with likely conditions to see they can report how they can isolate and reliably reproduce the problem with specific documented conditions.
- If there's online documentation available about problems in the vendor's systems, it is useful to search those resources *before* calling; if a solution is already online and works, one can save time compared with having to contact the vendor support services.



FIGURE 12.47
Problem-managers.

MULTI-VENDOR PROBLEMS

When technical problems seem to arise from the interactions of products from different vendors, there's a serious risk of paralysis. Finger-pointing may degenerate into deadlock as staff from the different suppliers try to excuse themselves from involvement. However, cooperation may be essential to identify and resolve the technical issues.

Once your own helpdesk team has established sound grounds for needing help from more than one vendor, it makes sense to arrange a meeting of vendor representatives with requisite technical knowledge to meet; virtual conferences are fine, since the physical locations of the personnel may be far apart, and travel would waste time as well as costing money. It's important to stop finger-pointing and avoidance of responsibility: make it clear that the issue is *not* fixing blame – the priority is getting the system working properly as soon as possible.

If there's continued hostility in the group, you may want to hire an external consultant with experience in handling conflicts involving multiple vendors.

Define operational tasks and deadlines cooperatively and make sure that those assignments and deadlines are clearly detailed in the meeting notes. Clarity about *who* is supposed to do *what* by *when* is essential when there are many people involved in the project.

Establish the time of the next taskforce meeting collectively to be sure everyone will be able to participate.

When the problem is resolved, ensure that the managers of all the participating organizations receive explicit thanks and praise for their employees. You can turn this experience into a positive force for your relationships with the suppliers as well as for your own employees.



FIGURE 12.48
Lots of contacts.

TEACHING AND TECH SUPPORT

TS staff must adapt to changes in the technology they support. New members of the TS team must come up to speed quickly to take on their new responsibilities. These needs mean that *teaching* becomes an integral part of any TS group. The following section distills well established principles for effective teaching.

I can imagine some readers being taken aback by pages of advice about teaching in a textbook about operations and security management. However, my field experience strongly supports the view that effective training (learning to do something specific) and education (broadening perspectives to increase creative thinking and improve problem solving) are important elements of management in any organization.

Effective learning is affected by variables in the

- Learner – e.g., background knowledge, language capabilities, attention-span, reasoning abilities, trauma, stress.
- Channel – e.g., in person, live online, recordings.
- Teacher – e.g., language competence, experience in field, experience in teaching.
- Message – e.g., positive, neutral or negative contexts for the new knowledge.
- Evaluation – e.g., person-to-person questions, written essays, short-essay exams, multiple-choice questions, fill-in-the-blank questions.



FIGURE 12.49

Teaching effectively.

LEARNER VARIABLES

Teachers have to consider how to work effectively with a range of students. For example, students' responsiveness may be affected by different degrees of prior knowledge and ability to grasp new concepts.

To adapt to different knowledge base, use the following approaches:

- *Define prerequisite knowledge, skills:* make sure that participants are aware of the assumptions underlying the teaching sessions or materials; provide supplementary readings to help participants be better prepared for their studies.
- *Ask each student for a short biography:* you can use your awareness of shared or unique experiences as tools for maintaining attention and encouraging participation.
- *Explore related areas of knowledge:* sometimes sharing participants' unique experiences can offer new perspectives that increase the value of the training sessions.
- *Identify strengths and weaknesses:* if possible, help participants improve basic knowledge and skills *before* plunging into new areas. Encourage those with applicable experience to share their perspectives for the benefit of the entire group.
- *Incorporate interests into examples:* knowing about the participants' backgrounds supports efforts to elicit their participation in the course.

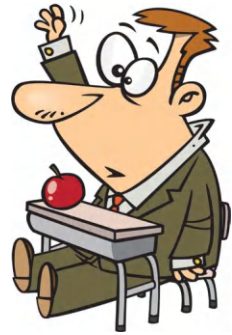


FIGURE 12.50

Learners.

Intelligence is less important than frequently assumed: people can vary in their speed of thought without seriously interfering with their ability to integrate new knowledge. Even in extreme cases, it may be possible to support learning-disabled people to achieve adequate levels of competence. Some ideas:

- *Effective study methods can help:* ensure that participants are aware of the well-established SQ3R (Survey, Question, Read, Recite, Review) technique for better learning.⁴¹
- *Encourage questions and discussion:* praise participants for raising questions in live classes or in online discussions. Questions indicate *thought*. Similarly, encourage contributions to in-class or online discussion threads by awarding points toward students' grades.

- *Praise interventions, ideas, and contributions*: make a fuss about novel ideas and helpful actions.
- *Offer assistance outside class*: students must feel confident that their requests for help will be treated seriously and supportively.

Alertness is another factor to consider.

- *Sleep deprivation is harmful to learning*: to be aware of students' schedules. For example, in the military academy where I taught for 20 years, military students who had been in physical training since 05:00 were sometimes sleepy in the 08:00 applied-statistics classes. It would have been counter-productive (and just plain rude) to treat them with anything but kindness.
- *Provide frequent breaks*: a four-hour unbroken live learning session doesn't make sense. Break at *least* every hour and encourage students to get up, move about, have refreshments and chat with each other. In online training, break the units up in a similar fashion.
- *Respond immediately to inattention*: in live classes, ask a question to any participant who seems to be off-focus (e.g., reading their phone in their lap).
- *Discourage heavy lunches*: live-training session planners should plan lunches that don't put participants to sleep. For example, serving students massive pieces of dead animals complete with rinds of fat may cause afternoon sleepiness in participants.⁴²
- *Forbid alcohol consumption during training*: alcohol interferes with the prefrontal cortex (locus of reasoning) and the hippocampus (essential for effective learning).⁴³
- *Use humor and the unexpected*: I *never* criticized *any* student for being drowsy in class; instead, I would switch accent to make them laugh – and wake up. Students so enjoyed the novelty that they would often say, "More accents, sir."

Another actor is motivation. Why are people in your training course?

- *Beware forced participation*: work to convince participants of the utility of the material. I always explained in classes how particular knowledge or techniques would be useful in practice. Many students have told me over the decades how they valued the practical applications of the knowledge they acquired in my classes.
- "What would you like to be able to do after this course that you can't do now?" An *operational* focus on learning ties the efforts to the real world. Telling students that the knowledge "is good for them" is inadequate. Be specific.
- *Address the benefits of mastery*: point out concrete applications of the subject matter. For example, when I addressed the value of frequency analysis using the log-likelihood ratio in my applied-statistics classes, I told the students about how, in 1971 at the age of 21 while finishing my MSc, I told a world-famous scientist that he had been using the wrong technique (*ANOVA*, or analysis of variance) to compare frequency distributions in his data. I used my portable programmable calculator to re-analyze data in one of his recently published articles and showed him that instead of a probability of the null hypothesis $p=0.04$, his data actually had a probability of lack of effect of $p = 10^{-6}$. He accepted me as a doctoral student and granted me four years of waived tuition and a stipend as a teaching and research assistant of \$11K/year –about \$72K in 2021 dollars.⁴⁴
- *Share your experiences in the real world*: Provide real-world examples whenever possible to motivate students to learn. For example, in my operating-system classes, I told my students about the performance analysis where solving the problem prevented loss of \$9.5M in today's currency.

CHANNEL VARIABLES

The way courses are structured and delivered affect learning.

How much time should we be planning for training?

- Allow for at least ~3 minutes/slide on average
- Plan for at most ~1 hour of work between breaks
- Schedule at most ~7 hour/day of work
- If possible, spread the training over more than one day or session for better assimilation and application.



FIGURE 12.51 Channel variables.

What are some of the environmental factors that help participants learn better?

- Keep the room relatively cool
- Use bright lights in the training center if possible
- Provide comfortable chairs but not heavily cushioned
- Make sure the desks or tables are appropriate for students to place portable computers and notepads
- Structure your electronic training materials with room for notes by the instructors *and* available for students to add their own notes
- Provide a variety of multimedia resources such as reference articles and videos to encourage further study and stimulation.

Visibility, audibility, and clarity of the presentations affect learning.

- *Don't be a robot*: change your position as lecturer to stand, move, or sit as you interact
- *Speak clearly at all times*: emphasize keywords and never mumble
- Presentation should vary in speed (within limits) to reduce the likelihood of putting participants to sleep
- *Overinflect for emphasis*: when lecturing live or in recordings, avoid monotonic drones. Use exaggerated inflections to emphasize specific points. As I told my students over the years, they should not assume from my teaching inflections that I would say to my wife, "Good MORNING, dear. Did you SLEEP well?" But when lecturing, I might say, "The SIX fundamental properties of the information that we PROTECT are summarized in the PARKERIAN HEXAD."

Encourage high interactivity to keep students alert and involved.

- Ask questions frequently: encourage open responses.
- Challenge individuals when possible.
- Turn discussions to include personal experiences of the participants.
- Use digressions constructively: return to the applicability of stories or discussions.
- Use examples from students' experiences whenever possible.
- Remember individual students' interests and bring examples to light for them.

TEACHER VARIABLES

An effective teacher is determined to help students learn.

- *Commitment to student achievement*: teaching must *never* be about power or ego.
- *Encourage questions and challenges*: QUESTION AUTHORITY is one of my long-time mottos.
- *Beware feelings of power and superiority*: seek psychological counseling if necessary.
- *Admit mistakes immediately and clearly*: everyone makes mistakes and openly correcting them is a lesson for the students.
- *Unforgivable to humiliate students*: anyone deliberately embarrassing a learner should be fired.
- *Every lesson is a chance for teacher to learn*: student questions can help us *think*.



FIGURE 12.52
Teachers.

Empathy and imagination support learning:

- Remember what it was like being a beginner, help students learn concepts and terminology by defining them before going into more advanced details.
- Identify basic knowledge and skills and help learners acquire them, if necessary, before continuing a more advanced course.
- Ensure that basics are thoroughly mastered before plunging into advanced topics. Provide placement quizzes if necessary and supply resources for improvement.
- If necessary, take longer than planned at start – adapt the schedule to the nature of the class members.
- Encourage meetings after class if necessary – be available for help.

Patience is essential:

- *Find alternative ways of explaining ideas/skills*: not every student will respond to the first attempt to clarify more complex material.
 - Use analogies – tie the new material to lived experience.
 - Practical examples always help.
 - War stories can be informative as well as entertaining.
- When a question is completely out of place for a specific session, defer answer but assure the student that you will respond.
 - Later in lecture if suitable.
 - At break or after class.
- Respect students for wanting to understand.

Subject knowledge:

- It is difficult or impossible to teach without mastering the subject.
- Ideally, the instructor should create their own materials to supplement available materials.
- Available resources can supplement the instructor's knowledge.
 - Textbooks
 - Articles
 - Colleagues
 - Online DBs
- Anytime that an instructor does *not* know an answer is when they should say, "I don't know; let's find out!"

Background information:

- *Read widely in related areas:* it's to your students' benefit for you to be able to introduce interesting side-topics to maintain their interest.
- *Bring in analogies from other areas of experience:* examples of similar issues can help students grasp new concepts.
- *Use personal life-experiences when suitable:* keep interest up.
- *Talk about feelings as well as ideas:* avoid being a boring robot.
- *Express values openly:* get students to think (and possibly disagree, which is stimulating).

Ethical standards:

- *Work for the students' good:* teaching is not a profession for selfish egomaniacs who need to compensate for deep-seated feelings of inadequacy by bullying their students and abusing power.
- *Revise materials as appropriate:* stay up to date.
- *Provide value for money:* one way or another, students are paying for their time and effort.
- *Work fully all the hours for which you are contracted.*
- *Take students' other commitments into account:* for example, if a student has family issues, work with them to help make up for missing classes or poor grades (if there are grades).
- *Make it possible to achieve maximum grades:* provide supplementary materials to support learning and give students complete lists review questions so there are no surprises in exams.
- *Beware of emotional entanglements with students:* do *not* have romantic affairs with students! The power imbalance makes any such involvement completely unethical and potentially deeply hurtful to the victims.

MESSAGE VARIABLES

Organization of the course supports effective learning:

- Design the course top-down
 - Provide an overview at the start to help students grasp the major areas of concern.
 - Sketch out areas of concern, desired skills.
 - Fill in details step by step.
- Provide signposts explaining upcoming sections.
- Start each section with restatement of why it matters.
- Emphasize mastery of basic knowledge.
- Point to more advanced topics.
- Provide cross-references.

Content must be up-to-date and relevant:

- Use good-quality textbooks if available
- Review current literature and provide links
 - journals
 - magazines
 - Web sites
- Look for guest lecturers with field experience – much easier now that online virtual meetings are easy



FIGURE 12.53

Plan your message.

- *Arrange site-visits if possible:* e.g., in the sections on physical and facilities security in my IA courses, I would take my students on a tour of our own university buildings and of a local hospital, where they could see unlocked electric-power panels (opportunities for system shutdowns), strangers wandering the halls (no sign-in stations in the hospital), unlocked doors everywhere, unprotected network equipment in public spaces, glass windows in the IT rooms, and unprotected valves for the water systems.

Review questions help students check their knowledge and eliminate nasty surprises:

- Helpful for review purposes – improve learning by eliminating surprises.
- Include passive and active knowledge:
 - *Passive:* “Which of the following is the component which levitates the flammiger?”
 - *Active:* “How would you levitate a flammiger?”
- Provide practice in problem-solving, e.g.,
 - “A user tells you that....; how would you respond?”
 - “The screen display shows....; what would your next step be?”

EVALUATION

Evaluating the degree of learning not necessarily part of industry or internal courses but can be helpful to students to encourage more thorough learning, particularly if initial results are poor.



FIGURE 12.54 Results.

- Evaluation is a difficult issue for many teachers
 - Some organizations think they can evaluate general intelligence or overall learning ability
 - At minimum, teachers should insist on evaluating acquired skills
- Daily quizzes helpful for review
- Select exam questions exclusively from review questions
- Use a high standard of mastery:
 - E.g., 80% for PASS
 - Low scores generally indicate that the student or course has failed
- Provide extra *make-up* exams
 - Schedule review period before make-up exam; e.g., my courses had a two-week gap between the deadlines for original quizzes and make-up quizzes
 - Higher of the two grades counts; e.g., if original quiz score was 75% but the make-up quiz score was 85%, the 85% score was used in the course-grade calculations
 - Replacement exams should be harder than the originals
 - My courses usually included make-up exams with 50% more questions in half the time of the original
 - E.g., original quiz had 20 questions in 40 minutes but make-up quizzes had 30 questions in 30 minutes

NOTES

- 1 Kabay (1997).
- 2 Twin (2020).
- 3 Rist (2021).
- 4 Kabay (2021).
- 5 U.S. Department of Commerce (n/a).
- 6 U.S. National Institute of Science and Technology (2021).

- 7 Redscan (2021).
- 8 Security Magazine (2021).
- 9 U.S. Federal Bureau of Investigation (2018).
- 10 Carnegie Mellon University (2021).
- 11 U.S. National Institute of Science and Technology (2021).
- 12 Carnegie Mellon University (2021).
- 13 Carnegie Mellon University (2021).
- 14 Carnegie Mellon University (2021).
- 15 Carnegie Mellon University (2021).
- 16 Carnegie Mellon University (2021).
- 17 Carnegie Mellon University (2021).
- 18 CVE Program (2021).
- 19 Meunier (1991).
- 20 SANS (2023).
- 21 SANS (2023).
- 22 SANS (2023).
- 23 Neumann (2023).
- 24 Neumann (2023).
- 25 Neumann (2023).
- 26 Schneier (2023).
- 27 Schneier (2023).
- 28 Herold (2023).
- 29 Herold (2023).
- 30 Stowe Today (2017).
- 31 U.S. Department of Commerce – National Institute of Standards and Technology (1993).
- 32 Kabay, Robertson, Akella, and Lang (2014).
- 33 Weiner (1979).
- 34 U.S. Department of Justice (n/a).
- 35 Allport (1979).
- 36 Adorno (2019).
- 37 Wilson Learning (2021).
- 38 Medallia (2021).
- 39 Bryner (2008).
- 40 Brazier (2020).
- 41 Kabay (2006).
- 42 Glassman (2016).
- 43 Mira et al. (2020).
- 44 CoinNews Media Group LLC (2021).

WORKS CITED

- Adorno, T. E.-B. (2019). *The Authoritarian Personality* (Illustrated Edition ed.). Verso. Retrieved September 4, 2023, from <https://www.amazon.com/Authoritarian-Personality-Theodor-Adorno/dp/1788731646>
- Allport, G. (1979). *The Nature of Prejudice: 25th Anniversary Edition* (25th Anniversary ed.). Basic Books. Retrieved September 4, 2023, from <https://www.amazon.com/Nature-Prejudice-25th-Anniversary/dp/0201001799>
- Brazier, Y. (2020, September 29). *All About Narcissistic Personality Disorder*. Retrieved October 16, 2021, from Medical News Today: <https://www.medicalnewstoday.com/articles/9741>
- Bryner, J. (2008, April 27). *The Fragility of Self-Esteem*. Retrieved October 16, 2021 <https://www.livescience.com/2495-fragility-esteem.html>
- Carnegie Mellon University. (2021). *CERT History*. Retrieved August 13, 2021, from CMU SEI: <https://www.sei.cmu.edu/about/divisions/cert/index.cfm#history>
- Carnegie Mellon University. (2021). *Cybersecurity Center Development*. Retrieved August 13, 2021, from CMU Software Engineering Institute: <https://www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm>
- Carnegie Mellon University. (2021). *SEI Blog | CERT/CC Vulnerabilities*. Retrieved August 13, 2021, from CMU Software Engineering Institute: <https://insights.sei.cmu.edu/blog/topics/certcc/>

- Carnegie Mellon University. (2021). *SEI Blog | Insider Threat*. Retrieved August 13, 2021, from CMU Software Engineering Institute: <https://insights.sei.cmu.edu/blog/topics/insider-threat/>
- Carnegie Mellon University. (2021). *SEI Digital Library*. Retrieved August 13, 2021, from CMU Software Engineering Institute: <https://resources.sei.cmu.edu/library/>
- Carnegie Mellon University. (2021). *SEI Podcast Series*. Retrieved August 13, 2021, from CMU Software Engineering Institute: <https://www.sei.cmu.edu/publications/podcasts/index.cfm>
- Carnegie Mellon University. (2021). *Vulnerability Notes Database*. Retrieved August 13, 2021, from CMU SEI CERT/CC: <https://www.kb.cert.org/vuls/>
- CoinNews Media Group LLC. (2021). Retrieved from US Inflation Calculator: <https://www.usinflationcalculator.com/>
- CVE Program. (2021, September 28). *Terminology: A Glossary of Terms Used by the CVE Program*. Retrieved October 12, 2021, from MITRE.ORG | About: <https://cve.mitre.org/about/terminology.html>
- Glassman, E. (2016, September 1). *Eating for Daily Alertness at Work*. Retrieved from The Times of Israel | The Blogs: <https://blogs.timesofisrael.com/eating-for-daily-alertness-at-work/>
- Herold, R. (2023). *Online Learning*. Retrieved September 15, 2023, from Privacy & Security Brainiacs | Training: <https://privacysecuritybrainiacs.com/training/>
- Herold, R. (2023). *Privacy & Security Brainiacs*. Retrieved September 15, 2023 <https://privacysecuritybrainiacs.com/>
- Kabay, M. E. (1997, February 15). *The Art of Technical Support*. Retrieved October 12, 2021, from M. E. Kabay | Courses: <http://www.mekabay.com/courses/academic/jac/TSP/index.htm>
- Kabay, M. E. (2006, August 28). *SQ3R: Active Learning for Everyone*. Retrieved from M. E. Kabay: <http://www.mekabay.com/methodology/sq3r.pdf>
- Kabay, M. E. (2021, October 23). *Statistics in Business, Finance, Management and Information Technology: A Layered Introduction with Excel*. Retrieved October 23, 2021, from M. E. Kabay | Courses | Academic | Norwich | QM213: <http://www.mekabay.com/courses/academic/norwich/qm213/index.htm>
- Kabay, M. E., Robertson, B., Akella, M., & Lang, D. T. (2014). *Using Social Psychology to Implement Security Policies*. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.). Hoboken, NJ, USA: John Wiley & Sons, Inc. Retrieved October 13, 2021, from <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Medallia. (2021, July 02). *How HP Engineers Amazing Experience Through Real-Time Customer Feedback and Telemetry*. Retrieved September 15, 2023, from Medallia | Resource: <https://www.medallia.com/resource/how-hp-engineers-amazing-experience-through-real-time-customer-feedback-and-telemetry/>
- Meunier, P. (1991, August 24). *Re: CD MODIFICATION: DEFINITION version 2 - Interim Decision 8/30*. Retrieved October 12, 2021, from MITRE | Data | Board | Archives | 1999-08: <https://cve.mitre.org/data/board/archives/1999-08/msg00114.html>
- Mira, R. G., Lira, M., Tapia-Rojas, C., Rebolledo, D. L., Quintalla, R. A., & Cerpa, W. (2020, January 24). Effect of Alcohol on Hippocampal-Dependent Plasticity and Behavior: Role of Glutamatergic Synaptic Transmission. *Frontiers of Behavioral Neuroscience*, 13, 1–15. <https://doi.org/10.3389/fnbeh.2019.00288>
- Neumann, P. G. (2023). *SRI International Computer Science Laboratory*. Retrieved September 15, 2023, from CSL SRI | Neumann: <https://www.csl.sri.com/~neumann/>
- Neumann, P. G. (2023, September 13). *The Risks Digest*. Retrieved September 15, 2023, from CATLESS | RISKS: <http://catless.ncl.ac.uk/risks/>
- Neumann, P. G. (2023, September 13). *The Risks Digest, Volume 33 Issue 84*. Retrieved September 15, 2023, from The Risks Digest: <http://catless.ncl.ac.uk/Risks/33/84>
- Redscan. (2021, February 17). *Redscan analysis of NIST NVD Reveals Record Number of Critical and High Severity Vulnerabilities in 2020*. Retrieved August 12, 2021, from REDSCAN: <https://www.redscan.com/news/nist-nvd-analysis/>
- Rist, O. (2021, October 29). *The Best Help Desk Software for 2021*. Retrieved November 9, 2021, from PC Magazine: <https://www.pcmag.com/picks/the-best-help-desk-software>
- SANS. (2023, 11 10). *Newsbites*. Retrieved November 14, 2023, from SANS | Newsletters: <https://www.sans.org/newsletters/newsbites/>
- SANS. (2023, 11 09). *OUCH! Newsletters*. Retrieved November 14, 2023, from SANS | Newsletters: <https://www.sans.org/newsletters/ouch/>
- SANS. (2023, 11 01). *SANS @RISK*. Retrieved November 14, 2023, from SANS | Newsletters: <https://www.sans.org/newsletters/at-risk/>
- Schneier, B. (2023, September 15). *About Bruce Schneier*. Retrieved September 15, 2023, from Schneier on Security | About Me: <https://www.schneier.com/blog/about/>

- Schneier, B. (2023, September 15). *Crypto-Gram Newsletter*. Retrieved September 15, 2023, from Schneier on Security | Crypto-Gram: <https://www.schneier.com/crypto-gram/>
- Security Magazine. (2021, February 15). *Record Number of Critical and High Severity Vulnerabilities Were Logged to the NIST NVD in 2020*. Retrieved August 12, 2021, from Security Magazine: <https://www.securitymagazine.com/articles/94602-record-number-of-critical-and-high-severity-vulnerabilities-were-logged-to-the-nist-nvd-in-2020>
- Stowe Today. (2017, November 2). *Concert Will Honor Memory of Percy Black*. Retrieved October 13, 2021, from Stowe Today | Music: https://www.vtcng.com/stowetoday/music/concert-will-honor-memory-of-percy-black/article_e3674838-bfef-11e7-a61f-lbfd9ac8cc0c.html
- Twin, A. (2020, August 24). *There Ain't No Such Thing as a Free Lunch (TANSTAAFL)*. Retrieved November 7, 2021, from Investopedia | Business | Business Essentials: <https://www.investopedia.com/terms/t/tanstaafl.asp>
- U.S. Department of Commerce. *National Institute of Standards and Technology*. Retrieved August 12, 2021, from NIST: <https://www.nist.gov/https://www.nist.gov/>
- U.S. Department of Commerce – National Institute of Standards and Technology. (1993, September 20). *Proceedings of the 16th National Computer Security Conference*. Retrieved October 13, 2021, from NIST | Information Technology Laboratory: <https://csrc.nist.gov/publications/detail/conference-paper/1993/09/20/proceedings-16th-national-computer-security-conference-1993>
- U.S. Department of Justice. *We Uphold the Civil Rights of All People in the United States*. Retrieved October 13, 2021, from US DOJ | Civil Rights Division: <https://civilrights.justice.gov/>
- U.S. Federal Bureau of Investigation. (2018, November 2). *The Morris Worm: 30 Years Since First Major Attack on the Internet*. Retrieved August 13, 2021, from FBI NEWS: <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>
- U.S. National Institute of Science and Technology. (2021, August 5). *National Vulnerability Database*. Retrieved August 12, 2021, from NIST Information Technology Laboratory: <https://nvd.nist.gov/>
- Weiner, B. (1979, February). A theory of motivation for some classroom experiences. *Journal of Educational Psychology*, 71(1), 3–25. <https://doi.org/10.1037/0022-0663.71.1.3>
- Wilson Learning. (2021). *Building Relationship Versatility: Social Styles at Work*. Retrieved October 13, 2021, from Wilson Learning | Products: <https://global.wilsonlearning.com/products/brv/>

13 Security-Policy Style

Why does style matter in policy documents?

Style is defined in dictionaries as “a way of writing or performing: the way in which something is written or performed, as distinct from its content.” Style includes the wording and tone, organization, presentation, and even maintenance of the policies. Style influences the reception and effectiveness of policies.

One of the major areas of my work and operations management has been the development and refinement of information-security policies. Over the years, I have seen cases in which well-designed policies have been implemented effectively in part because of the style of presentation.

Unfortunately, I have seen (and corrected) many cases in which the security policies were so poorly written that they offended and insulted the employees. The bad style included patronizing tone, grammar and spelling mistakes, and incomprehensible text.

This chapter reviews issues affecting policy effectiveness, including:

- Integrating well-known principles of social psychology into security management.
- Changing how employees (and customers and everyone else) see information security.
- Systematic approaches to developing effective security policies.
- Ways of communicating security policies for best results.

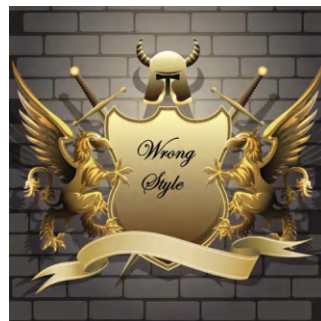


FIGURE 13.1 Style matters.

THE ZEN OF NETWORK SECURITY?

Information management is based on the availability of data throughout the enterprise. Data communications therefore make up a significant part of the investment in IT. It follows that network security is at the heart of information-system security, which is a growing component of operational budgets.¹ Network managers therefore have to work closely with colleagues in framing and implementing information-security policies. Their contribution to the information-security team is essential for success.

Your mission in devising network security policies is to ensure that network components support the basic principles of information security: to protect information from unauthorized or accidental modification, destruction, and disclosure and to ensure proper authentication, timely availability, and usability of those data.

The task is complicated by human and organizational resistance. Technology alone doesn't work. In changing human behavior, substance is not enough. Style makes the difference.

Security is always described as being everyone's business. Actually, security *interferes* with everyone's business. As a network manager, you have worked hard to make your networks user-friendly. You've done everything you can to make life easier for users; you've provided network access routines with a graphical user interface, client-server systems with hot-links between local spreadsheets and corporate DBs, and a gateway to the Internet for your engineering users.



FIGURE 13.2
Master of security.

So why is there anything different about securing your networks? Superficially, you might think that network security simply involves defining access controls, applying encryption, and providing people with hand-held password generators. What's so hard about that?

What's hard is that security policies offend deep-seated ways of seeing ourselves. We form close-knit work groups in which people *trust* each other. We don't lock our desks when we leave them for a few minutes; why should we obey the network security policy that dictates locking our keyboards? We lend people our car keys in an emergency; why should it be such a big deal if we lend them our access codes and passwords in an emergency?

Network users have to change the way they *think* about information. To implement security policies and procedures without focusing on attitudes and beliefs is to ensure non-compliance. If you impose security restrictions without convincing the users that they *need* to protect the networks, you will get lip-service and nothing more.

Every password written on a *Post-It*TM note under the keyboard or stored in an insecure file on a personal phone is proof that security policies are meaningless unless users believe in them. At one of my training sessions on security policy, an executive commented, "I feel as if I've gotten religion!" He wasn't far off the truth. As you try to develop and implement your network security strategy, you will cross boundaries within your organization. If you try to *impose* more stringent security procedures for network use, you will be perceived as making people's jobs harder – and they don't even work for you. In many cases, you will be resisted with the comment, "Network security? That's *your* problem, not mine."

The only approach that works is to co-opt your colleagues. *Convince* your users that network security is in their own interest. *Involve* them in developing security policies. You depend on them to implement the procedures you work out collectively. Make sure that users recognize that they *own* their security procedures, and you'll have *partners* instead of opponents.

PSYCHO-SOCIAL FACTORS IN INFOSEC POLICY

All of us have commiserated with colleagues about the difficulty of getting people to pay attention to security policies to comply with what seems like good common sense. We shake our heads in disbelief as we recount tales of employees who hold the door open for their work mates, thereby rendering million-dollar card-access systems useless.

One problem is that although information-systems security and network-management personnel have a wide variety of backgrounds, many of us lack any formal training in social psychology. Indeed, I was apparently the first security professional to present a systematic view of how social psychology plays a role in effective security management; my paper on "Social Psychology and INFOSEC" received the *Outstanding Paper Award* at the 16th *National Computer Security Conference* organized by the NIST *Computer Systems Laboratory* (CSL) and the *National Computer Security Center* (NCSC) of the *National Security Agency* (NSA) in September 1993 in Baltimore, MD.² The following material is based on that paper.

Security policies and procedures affect not only what people do but also how they see themselves, their colleagues, and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. The established principles of human social behavior have much to teach us in our attempts to improve corporate and institutional information security.

Information-security specialists concur that security depends on people more than on technology. Another commonplace is that employees are a far greater threat to information security than outsiders.



FIGURE 13.3
Psychology helps
INFOSEC.

It follows from these observations that improving security depends on changing beliefs, attitudes, and behavior, both of individuals and of groups. Social psychology can help us understand how best to work with human predilections and predispositions to achieve our goals of improving security:

- Research on social cognition looks at how people form impressions about reality (knowing these principles, we can better teach our colleagues and clients about effective security).
- Work on attitude formation and beliefs helps us present information effectively and so convince employees and others to cooperate in improving security.
- Scientists studying persuasion and attitude change have learned how best to change people's minds about unpopular views such as those of the security community.
- Studies of factors enhancing prosocial behavior provide insights on how to foster an environment where corporate information is willingly protected.
- Knowledge of the phenomena underlying conformity, compliance, and obedience can help us enhance security by encouraging compliance and by protecting staff against social pressure to breach security.
- Group-psychology research provides warnings about group pathology and hints for working better with groups in establishing and maintaining information security in the face of ingrained resistance.

RATIONALITY IS NOT ENOUGH

Information-security policies sometimes seem to evoke strong emotions among our colleagues. People can get very angry about what they perceive as interference with their way of getting their work done. Sometimes people subvert information security by systematically getting around the rules; for instance, on one security evaluation of the IT department at a company in the 1980s, I noticed a soft-drink delivery man opening the door into a secured area by using the keypad. Startled, I turned to the manager I was interviewing and asked if he had seen this flagrant breach of security; he replied, "Oh yeah, no problem. We got tired of opening the door for him every week, so we gave him the combination-code to the lock."

Psychologists use the word *schema* to summarize the complex picture of reality upon which we base our judgments.³ That manager's schema included a trustworthy soft-drink delivery man; an information-security specialist's schema in the same circumstances included all the potentially untrustworthy friends of that soft-drink delivery man.

Schemas are self-consistent views of reality. They help us pay attention to what we expect to be important and to ignore irrelevant data. They also help us organize our behavior. For example, our schema for relations at the office *includes* polite greetings, civil discussions, written communications, and businesslike clothes. The schema *excludes* obscene shrieks, abusive verbal attacks, spray-painted graffiti on the walls, and colleagues at work dressed in swimsuits. It is the schema that lets people tell what is inappropriate in a given situation.

Unfortunately, security policies and procedures conflict with most people's schemas. Office workers' schemas can include sharing office supplies (*Lend me your stapler, please?*), trusting their team members to share information (*Take a look at these figures, Sally*), and letting their papers stay openly visible when they have to leave their desk.

Alas, sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving workstations logged on without protection are gross breaches of a different schema. Think about access controls: normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for them; when we see a visitor, we smile politely (who knows, it may be a customer). In contrast, access-control policies require that we



FIGURE 13.4

User irritated by incomprehensible security rules.

refuse to let even a well-liked colleague piggyback their way through an access-card system; security policies insist that unbadged strangers be challenged (politely) or reported to security personnel. Common sense tells us that when the CEO of the company wants something, we do it; yet the information security dictates that we should try to train computer-room operators to forbid entry to anyone without documented authorization including the CEO.⁴

If we persist in assuming that we can influence our colleagues to change their perception of information security simply by informing, cajoling, nagging, or browbeating them, we will continue to fail.

Information security must be integrated into the corporate culture; such a change needs to use all of the techniques that social psychology can teach us.

WRITING DOWN PASSWORDS: IRRATIONALITY IN PRACTICE

I have long argued that passwords are a terrible way of authenticating identity, particularly when untrained users make up their own without supervision.

- Many well-meaning but unaware people choose really stupid, easy-to-guess passwords such as *123456*, the names of people important to them (or favorite sports teams, or the product whose billboard is visible from their office window, the names of objects on their desk), or even (gasp) “password” or “p455w0rd.”⁵
- Good passwords increase the keyspace not only by being longer but also by using upper- and lowercase letters, numbers, and special characters – resulting in monstrosities such as “j3q(K8bX_*5” – and let’s not even _think_ about using “O” and “0” in the character set;
- Some users generate their passwords using funny rules such as using particular letters from the words in phrases (e.g., using the third letter of each word in “Mary had a little lamb; its fleece was white as snow” produces “rdatmsesiso”) – and then they forget the rules.
- People sometimes use numerical increments to get around rules preventing password reuse (e.g., *fisu3nema*, *fisu4nema*, *fisu5nema*...) thus compromising their *next* password as soon as the *current* password is discovered.
- Users often use exactly the same password for everything (their private Web email, their corporate professional email, their DVD-club login, their talking-slug club – everything) with the result that any single password compromise is a potentially complete security compromise.
- Making passwords hard to guess forces many people to write them down, often on *paper*.
- Physically-recorded passwords get stored in the same places network security auditors have always found them: in desk drawers, under keyboards, under chair seats, in files labeled “C:\passwords.txt” and even in plain view on the back (or front!) of video screens (that actually happened at a university where the ADMIN password was taped on each of the screens in a computer lab).
- When people *do* pick hard-to-guess passwords and *don’t* record them securely, they often call the helpdesk or security administrator to reset them because they *forget* them or forget how to access their password safes, causing a great deal of irritation and wasted time for everyone concerned.



FIGURE 13.5

Beware the naive users' password choices.

A study published by *Nucleus Research* in 2006 reported findings on user behavior concerning passwords. To no one’s surprise, based on a survey with 325 respondents, the researchers found that:

Unfortunately, more than one in three enterprise users keep a written record of their passwords – despite the clear security risks of doing so.

...Of the third of users that write down their passwords, one third of those do it on paper, such as a sticky note. Even more dangerous are the other two thirds: they keep their passwords as a text file on their laptop PC or mobile device, where it could be easily lost or stolen.

There was also no correlation between complexity, frequency, and quantity and how often users called the helpdesk with password-related issues.

- Seventy percent of enterprise users called the IT helpdesk once a year for help with a forgotten or missing password.
- 16 percent called two to three times a year.
- 9 percent called three to five times a year.
- 5 percent called more than five times a year for password help.⁶

POOR UNDERSTANDING OF RISK

A long-standing joke among statisticians is that gambling is a tax on people who don't understand probability theory. Unfortunately, many non-security people have about the same level of misunderstanding about the risks of poor security as they do about the likelihood of winning a lottery by buying a ticket at their gas station.

I think that these findings are consistent with social scientists' understanding of human perception of risk. Basically, human beings are terrible at evaluating risk; all kinds of factors interfere with rational appraisal of risk. For example, our judgment is affected by such factors as the salience (visibility, ease of being noticed) of the evidence.

A famous study examined people's willingness to undergo surgery or radiation. The researchers offered different groups two complementary ways of understanding the risks – by mortality rates versus survival rates.

For example, one group was informed that the survival rates at treatment were:

- 100% for radiation and 90% for surgery.
- One year after treatment survival rates were reported as 77% for radiation versus 68% for surgery.
- Survival rates five years after treatment were 22% for radiation versus 34% for surgery.

The other group was given exactly the same information, but it was framed as

- 0% mortality upon radiation treatment vs 10% mortality for surgery.
- 23% mortality one year after radiation versus 32% mortality one year after surgery.
- The five-year prognosis was 78% mortality for radiation versus 66% for surgery.

The results were striking: 44% of the patients informed of the risk via *mortality* rates said they'd take the radiation but only 18% of those who were told about *survival* rates chose radiation.⁷

On the face of it, the results don't make sense: why would anyone respond differently to the same risk statistics as a function solely of wording?

A *National Research Council* report suggests that people normally evaluate risk in a nonlinear fashion and that framing of problems exerts a profound effect on perception of risk:

Risk characterization is often conceived as a summary or translation of the results of technical analysis for the use of a decision maker. Seen in this light, a risk characterization may fail for two reasons: it



FIGURE 13.6

Security is risk management
not gambling.

may portray the scientific and technical information in a way that leads to an unwise decision, or it may provide scientific and technical information in a way that is not useful for the decision maker. Although such failures do occur, an often overlooked danger to risk decision making is a fundamental misconception about how risk characterization should relate to the overall process of comprehending and dealing with risk.

The scientists proposed seven key principles for improving risk assessment:

1. Risk characterization should be a decision-driven activity, directed toward informing choices and solving problems.
2. Coping with a risk situation requires a broad understanding of the relevant losses, harms, or consequences to the interested and affected parties.
3. Risk characterization is the outcome of an analytic-deliberative process. Its success depends critically on systematic analysis that is appropriate to the problem, responds to the needs of the interested and affected parties, and treats uncertainties of importance to the decision problem in a comprehensible way. Success also depends on deliberations that formulate the decision problem, guide analysis to improve decision participants' understanding, seek the meaning of analytic findings and uncertainties, and improve the ability of interested and affected parties to participate effectively in the risk decision process. The process must have an appropriately diverse participation or representation of the spectrum of interested and affected parties, of decision makers, and of specialists in risk analysis, at each step.
4. The analytic-deliberative process leading to a risk characterization should include early and explicit attention to problem formulation; representation of the spectrum of interested and affected parties at this early stage is imperative.
5. The analytic-deliberative process should be mutual and recursive. Analysis and deliberation are complementary and must be integrated throughout the process leading to risk characterization: deliberation frames analysis, analysis informs deliberation, and the process benefits from feedback between the two.
6. Those responsible for a risk characterization should begin by developing a provisional diagnosis of the decision situation so that they can better match the analytic-deliberative process leading to the characterization to the needs of the decision, particularly in terms of level and intensity of effort and representation of parties.
7. Each organization responsible for making risk decisions should work to build organizational capability to conform to the principles of sound risk characterization. At a minimum, it should pay attention to organizational changes and staff training efforts that might be required, to ways of improving practice by learning from experience, and to both costs and benefits in terms of the organization's mission and budget.⁸

PRACTICAL PSYCHOLOGY

- In every security course or awareness program, instructors and facilitators should explicitly address the question of corporate culture, expectations, and social schemata. Don't rely solely on intellectual discourse when addressing a question of complex perceptions and feelings.
- Address the feelings and perceptions of all participants as they learn about the counter-intuitive behaviors that improved security will demand. Encourage learners to think about how they might feel and respond in



FIGURE 13.7 Happier employees will be more cooperative about security.

various situations that can arise during the transition to a more secure environment. For example, ask participants to imagine.

- asking a colleague not to step through a secured entrance without passing through the access-control system with their own identity.
- telling their boss that they will not copy software without a license to do so.
- walking up to a visitor or employee who is not wearing an identity badge.
- Use simulations, videos, and role-playing exercises to bridge the gap between intellect and emotion.

FRAMING REALITY

How can we make the corporate culture more supportive of information security?

In a previous section, I explained that the *schema* is what social psychologists call the way people make sense of their social interactions. Information-security practitioners need to change our colleagues' schema.

Schemas influence what we perceive. For example, an employee refuses to take vacations, works late every night, is never late, and is never sick. A model employee? Perhaps, in one schema. From the security point of view, the employee's behavior is suspect. There have been cases where such people have actually been embezzlers unable to leave their employment: even a day away might result in discovery of their crimes. Saint or sinner? Our expectations determine what we see.

To change the schema so that people take information security seriously, we should provide participants in training and security awareness with real-life examples of computer crime and security breaches so that security policies make sense rather than seeming to be arbitrary.

Schemas influence what we remember. When information inconsistent with our preconceptions is mixed with details that fit our existing schemas, we selectively retain what fits and discard what conflicts. When we have been fed a diet of movies and television shows illustrating the premise that information is most at risk from brilliant hackers, why should we remember the truth that carelessness and incompetence by authorized users of IS cause far more harm than evil intentions and outsiders ever do?

Instructors should emphasize the many benefits of information security by showing how policies protect all employees against false accusations, prevent damage to the organization's reputation and profits, and even play a role in national security (especially where business touches the technical infrastructure on which we all depend).

Most important of all, teaching others about information security cannot be an occasional and haphazard affair. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues. In light of the complexity of social cognition, our usual attempts to implement security policies and procedures seem pathetically inept. A couple of hours of lectures followed by a video, a yearly ritual of signing a security policy that seems to have been written by Martians – these are not methods that will improve security. These are merely lip service to the *idea* of security.

According to research on counter-intuitive information,⁹ people's judgment is influenced by the manner in which information is presented. For example, even information contrary to established schemas can be assimilated if people have enough time to integrate the new knowledge into their world views. It follows that security policies should be introduced over a long time, not rushed into place.

An effective information-security program includes frequent reminders of security. To change the corporate culture, practitioners should use methods such as a security corner in the corporate publication, security bulletins detailing the latest computer crime or security breach that has hit the news, contests for identifying the problems in realistic scenarios, and write-in columns to handle

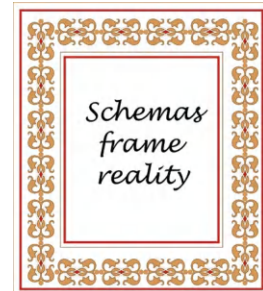


FIGURE 13.8
Change users' perceptions.

questions about policies. Information security has to become part of the framework of reality, not just an imposition from management.

GETTING OUR SECURITY POLICIES ACROSS

I have emphasized that the schema (the way people make sense of their social interactions) profoundly influences whether security policies will be integrated into the corporate culture.

What are some of the ways to change our colleagues' schemas so that they become more receptive to information-security policies?

Preliminary information may influence people's responses to information presented later. For example, merely exposing experimental subjects to a list of words such as *reckless* or *adventurous* affects their judgment of risk-taking behavior in a later test. It follows that when preparing to increase employee awareness of security issues, presenting case studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

Pre-existing schemas can be challenged by several counter-examples, each of which challenges a component of the schema. For example, prejudice about an ethnic group is more likely to be changed by contact with several people, each of whom contradicts a different aspect of the prejudiced schema. It follows that security-awareness programs should include many realistic examples of security requirements and breaches. In a counterexample, students in my college INFOSEC courses have commented on the unrealistic scenario in a training video they are shown: a series of disastrous security breaches occur in the same company. Based on the findings of cognitive social psychologists, the film would be more effective for training if the incidents were dramatized as occurring in different companies.

In practical terms, practitioners should stay current and update their materials. Case studies from the real-world help make awareness and training more effective.

Perceptions of risks and benefits are profoundly influenced by the wording in which situations and options are presented. It follows that practitioners should choose their language carefully during security-awareness campaigns. Instead of focusing on reducing failure rates (breaches of security), we should emphasize improvements in our success rate.

Judgements are easily distorted by the tendency to rely on personal anecdotes, small samples, easily available information, and faulty interpretation of statistical information. Basically, we humans are not rational processors of factual information. If security-awareness programs rely strictly on presentation of factual information about risks and proposed policies and procedures, they will run up against our stubborn refusal to act logically. Security program implementation must engage more than the rational mind. We must appeal to our colleagues' imagination and emotion as well. We must inspire a commitment to security rather than merely describing it.

BELIEFS AND ATTITUDES

Psychologists distinguish between beliefs and attitudes.¹⁰ "A belief ... refers to cognitive information that need not have an emotional component...." An attitude refers to "an evaluation or emotional response....". Thus, a person may believe that copying software without authorization is a felony while nonetheless having the attitude that it doesn't matter.

Beliefs can change when contradictory information is presented, but some research suggests that it can take up to a week before significant shifts are measurable. Other studies suggest that when



FIGURE 13.9 Present convincing examples.



FIGURE 13.10 Be aware of attitudes.

people hold contradictory beliefs, providing an opportunity to articulate and evaluate those beliefs may lead to changes that reduce inconsistency.

These findings imply that a new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only help the security practitioner, but they may actually help move the corporate culture in the right direction.

An attitude, in the classical definition, “is a learned evaluative response, directed at specific objects, which is relatively enduring and influences behavior in a generally motivating way.” The advertising industry spends over \$50B yearly to influence public attitudes in the hope that these attitudes will lead to changes in spending habits that is, in behavior.

Research on classical conditioning suggests that attitudes can be learned even because of simple word association. If we wish to move our colleagues toward a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies like “Sneakers” may do harm indirectly by associating pleasant, likeable people with techniques that are used for industrial espionage. When teaching security courses, we should avoid praising the criminals we describe in case studies.

One theory on how attitudes are learned suggests that rewards and punishments are important motivators. Studies show that even apparently minor encouragement can influence attitudes. A supervisor or instructor should praise any comments that are critical of computer crime or that support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

When enforcing security policies, too many organizations focus entirely on punishing those who break the rules. However, everything we know about modifying behavior teaches us to use reward rather than punishment. One of my students, a security officer in a large corporation, experimented with reward and punishment in implementing security policies. Employees were supposed to logoff their terminals when leaving the office; however, compliance rates were around 40 percent. In one department, she used the usual techniques: putting up nasty notes on terminals that were not logged off, reporting violators to their bosses and changing the passwords on delinquent accounts. In a different department, she simply identified those users who had indeed logged off their terminals and left a Hershey’s Chocolate Kiss on the keyboard. After one month, compliance rates in the department subject to punishment had climbed to around 50 percent. Compliance in the department getting chocolates had reached 80%.

CHANGING ATTITUDES TOWARD SECURITY

Just as the previous chapter includes guidance on various aspects of effective teaching, persuasion – changing someone’s attitudes – also depends on effective communication. The four areas of concern parallel those in teaching:

- *Audience variables:* at whom is the persuasion aimed?
- *Communicator variables:* who is trying to persuade?
- *Message variables:* what is being presented?
- *Channel variables:* by what means is the attempt taking place?

Audience Variables

As mentioned above, questionnaires and interviews may help cement a favorable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. As a teacher of information security, I find that I now feel much more

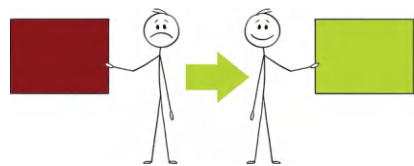


FIGURE 13.11 Change is possible!



FIGURE 13.12 Involve your audience.

strongly about computer crime and security than I did before I created my courses. We should encourage specific employees to take on public responsibility for information security within their work group. This role should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

Communicator Variables

Attractiveness, credibility, and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likeable people who understand the issues and sincerely believe in the policies they are advocating.



FIGURE 13.13

Choose good presenters.



FIGURE 13.14 Style matters in communication.

Message Variables

Fear can work to change attitudes only if judiciously applied. However, excessive emphasis on the terrible results of poor security is likely to backfire, with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counter arguments is more effective than one-sided diatribes. The *Software Publishers' Association* training video, *It's Just Not Worth the Risk*, uses this technique: it shows several members of a company arguing over copyright infringement and fairly presents the arguments of software thieves before demolishing them.¹¹

Modest repetition of a message can help generate a more positive response. Thus, security-awareness programs which include imaginative posters, mugs, special newsletters, audio and video tapes, and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination.

Channel Variables

The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. In modern organizations, most people assume that a meeting is the ideal way to communicate new information. However, the most effective medium for convincing someone to pay attention to any topic is face-to-face persuasion. Security training should include more than tapes and books; a teacher or leader can help generate enthusiasm for or at least reduce resistance to better security.

In addition, security educators should not introduce new ideas to decision makers in a meeting. There is too much danger of confounding responses to policy with non-policy matters rooted in relationships among the participants. For example, someone might oppose a new policy simply because another executive has supported it. A good way to introduce security policies is to have individual meetings with one executive at a time in which one explains the issues and proposals and asks for support.



FIGURE 13.15

Use several channels.

Psychologists testing cognitive response theory have studied many subtle aspects of persuasion. For example, experiments have shown that rhetorical questions (e.g., “Are we to accept invasions of our computer systems?”) are effective when the arguments are solid but counterproductive when arguments are weak.

Don’t use rhetorical questions unless you are absolutely certain that everybody will inevitably have the same answer – the one you are looking for.

In comparing the central route to persuasion (i.e., consideration of facts and logical arguments) with the peripheral (i.e., influences from logically unrelated factors such as physical attractiveness of a speaker), researchers find that the central route leads to more lasting attitudes and attitude changes.

ENCOURAGING INITIATIVE

Wouldn’t it be great if our colleagues actually helped us enforce security policies?

Studies of how and why people help other people have lessons for us as we work to encourage everyone in our organizations to do the right thing. Why do some people intervene to stop crimes? Why do others ignore crimes or watch passively? Two social psychologists, Bibb Latane and John M. Darley, devised a schema that describes the steps leading to prosocial behavior:

- People have to notice the emergency or the crime before they can act. Thus, security training has to include information on how to tell that someone may be engaging in computer crime.
- The situation has to be defined as an emergency something requiring action. Security training that provides facts about the effects of computer crime on society and solid information about the need for security within the organization can help employees recognize security violations as emergencies.
- We must take responsibility for acting. The *bystander effect* comes into play at this stage. The larger the number of people in a group confronted with an emergency, the slower the average response time. In the words of a standard psychology text, larger groups seem to lead “to a diffusion of responsibility whereby each person felt less personally responsible for dealing with the emergency.” Another possible factor is uncertainty about the social climate; people fear appearing foolish or overly emotional in the eyes of those present. We can address this component of the process by providing a corporate culture that rewards responsible behavior such as reporting security violations.
- Having taken responsibility for solving a problem, we must decide on action. Clearly written security policies and procedures will make it more likely that employees act to improve security. In contrast, contradictory policies, poorly documented procedures, and inconsistent support from management will interfere with the decision to act.¹²

People implicitly analyze *costs* of helping and of not helping when deciding whether to act pro-socially. The combination of factors most conducive to prosociality is low cost for helping and high cost for not helping.

Security procedures should make it easy to act in accordance with security policy, e.g., there should be a hot line for reporting security violations, anonymity should be respected if desired, and psychological counseling and follow-up should be available if people feel upset about their involvement. Conversely, failing to act responsibly should be a serious matter; personnel policies should document clear and meaningful sanctions for failing to act when a security violation is observed, e.g., inclusion of critical remarks in employment reviews and even dismissal.

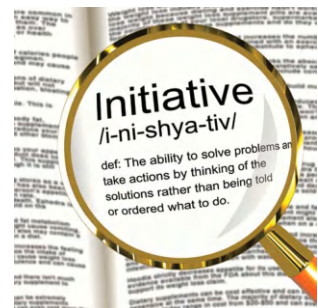


FIGURE 13.16
Reduce passivity.

One method that does *not* work well to increase prosocial behavior is *exhortation*. That is, merely lecturing people has little or no effect. Worse, the general level of stress and pressure to focus on narrow tasks can significantly reduce the likelihood that people will act on their moral and ethical principles.

Security is likely to flourish in an environment that provides sufficient time and support for employees to work professionally; offices where everyone responds to self-defined emergencies all the time will not likely pay attention to security violations.

Some findings from research confirm common sense. For example, *guilt* motivates people to act more prosocially. This effect works best when people are forced to assume responsibility. Thus, enforcing standards of security using reprimands and sanctions can indeed increase the likelihood that employees will subsequently act more cooperatively.

In addition, *mood* affects susceptibility to prosocial pressures: bad moods make prosocial behavior less likely, whereas good moods increase prosociality. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.

Even cursory acquaintance with other people makes it more likely that we will help them; it thus makes sense for security supervisors to get to know the staff from whom they need support. Encouraging social activities in an office (lunch groups, occasional parties, charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

DIRTY WORDS: CONFORMITY, COMPLIANCE, AND OBEDIENCE

These days, many people react negatively to the words *conformity*, *compliance*, and *obedience*. Unfortunately, ignoring social phenomena will not help the security practitioner attain her goals. We have to understand how people work together in reinforcing security policies.

Turning a group into a *community* provides a framework in which social pressures can operate to improve our organization's information security. People respond to the opinions of others by (sometimes unconsciously) shifting their opinion toward the mode – the most popular opinion.

Security programs must aim to shift the normative values (the sense of what one should do) toward protecting confidentiality, control, integrity, authenticity, availability, and utility of data.¹³

As we have seen in public campaigns aimed at reducing drunk driving, it is possible to shift the mode. Twenty years ago, many people believed that driving while intoxicated was amusing; today a drunk driver is a social pariah. In much the same way, we must move toward making computer crime as distasteful as public drunkenness.

The trend toward conformity increases when people within the group like or admire each other. In addition, the social status of an individual within a group influences that individual's willingness to conform. High-status people (those liked by most people in the group) and low-status people (those disliked by the group) both tend to be more autonomous and less compliant than people liked by some and disliked by others. Therefore, the security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely at both ends of the popularity range. Contrariwise, if security practices are currently poor and we want allies in changing the norm, we should work with the outliers to resist the majority's anti-security bias.

According to social psychologists, the norm of reciprocity holds that we should return favors in social relations.¹⁴ Even a small, unexpected, or unsolicited (and even unwanted) present increases the likelihood that we will respond to requests. For example, members of various religious cults



FIGURE 13.17 Make security a community effort.

often hand out flowers or books at airports, knowing that the norm of reciprocity will increase the frequency and amounts of donations from basically uninterested passersby.

A security-awareness program that includes small gifts such as an attractive mug labeled “SECURITY IS EVERYONE’S BUSINESS” or an inexpensive but useful booklet summarizing security policies can help get people involved in security.

In our field, we can personally ask an employee to set a good example by blanking their screen and locking their terminal when they leave their desk. Later, once they have begun their process of redefinition of themselves (“I am a person who cares about computer security”), we can ask them for something more intense, such as participating in security training for others (e.g., asking each colleague to blank their screen and lock their terminal). In this way, we gradually change the corporate culture so that a majority of people feel personally committed to protecting information assets.

BRINGING SECURITY HOME

A reader asked me why I consistently suggest that tidbits about personal security be included in corporate newsletters about information security. Why should the enterprise be concerned about telling employees how to protect their families against, say, *Nigerian advance-fee (“4-1-9”) fraud*?¹⁵ What does that have to do with corporate liability?

The benefit of including useful information about security that can help employees and their families comes from the psychological phenomenon called *internalization*.¹⁶ When we act in a particular way, we come to see ourselves in a new light: we integrate our behavior into a revised conception of ourselves. This phenomenon is thought to explain the success of the notorious *foot-in-the-door technique* used by salespeople and social activists: get the customer or potential volunteer to agree to a small purchase or action and there’s a better chance that they’ll agree to a larger purchase or action later.

For example, when political activists are looking for places to put up a prominent sign in a new neighborhood, they don’t just baldly go up to any old house and ask, “May we put up this big sign on your lawn?” No, they start small. They’ll canvas the block and ask people, “Do you support < whatever the issue is >? You do? Great! Could you display this little postcard-sized sign in your window? You WILL? Oh, that’s wonderful! Thank you!!”

Naturally, a week later, the little sign marks those houses that should be visited again. This time, the request can be for permission to, say, put up a sign two feet square on a wooden stick at the edge of the lawn. The week after that, some of the people with lawn signs may agree to join a demonstration or put up a really big sign or whatever the next phase of the plan is.

Why does this technique work?

According to some psychologists, agreeing to the modest request sets up a change in self-perception: “Oh, I guess I must be more interested in this than I thought.” Then when the next request arrives, the person seems to think something like, “Well, I suppose I really am interested in this after all – sure, go ahead.” Changing behavior, a little makes it more likely that you can change behavior a lot.

Some employees who act to protect their families against information-security threats may come to see themselves as security people; they internalize security as part of their own interests and value system. So when you ask them to cooperate at work on a security project, they may respond better than if they’ve never done anything security-related. You’ve converted some neutral bystanders into interested participants. Considering how inexpensive it is to include a paragraph about a useful security tip in a corporate newsletter that will be published anyway, the cost of the program is tiny compared to the potential benefits.



FIGURE 13.18 Learning about personal security improves commitment.

Besides, can you really argue against protecting children and families against bad cyberstuff? No, go ahead: put those little tidbits about *safe hex* into your newsletters and let your employees bring security home.

Don't worry – you'll get it back.

SUGGESTIONS FOR IMPROVING SECURITY EDUCATION

The preceding sections have looked at the major findings of social psychology that, in my experience, help us improve information-security programs. Herewith, a few reminders of key points and suggestions for practical application. I hope that these ideas will stimulate readers to think about social psychology as they work to implement security policies.

1. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues.
2. Security policies should be introduced over a long time, not rushed into place.
3. Presenting case studies is likely to have a beneficial effect on participants' readiness to examine security requirements.
4. Security-awareness programs should include many realistic examples of security requirements and breaches.
5. We must inspire a commitment to security rather than merely describing it.
6. Emphasize improvements rather than reduction of failure.
7. A new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers.
8. Do not portray computer crime using positive images and words.
9. Praise any comments that are critical of computer crime or that support the established security policies.
10. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.
11. Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training.
12. Frightening consequences should be coupled immediately with effective and achievable security measures.
13. Presenting objections to a proposal and offering counter arguments is more effective than one-sided diatribes.
14. Security-awareness programs should include repeated novel reminders of security issues.
15. In addition to recordings and books, rely on a charismatic teacher or leader to help generate enthusiasm for better security.
16. Encourage specific employees to take on public responsibility for information security within their work group.
17. Rotate the security role periodically.
18. Security training should include information on how to tell that someone may be engaging in computer crime.
19. Build a corporate culture that rewards responsible behavior such as reporting security violations.
20. Develop clearly written security policies and procedures.
21. Security procedures should make it easy to act in accordance with security policy.
22. Failing to act in accordance with security policies and procedures should be a serious matter.



FIGURE 13.19
Better security education.

23. Enforcing standards of security can increase the likelihood that employees will subsequently act more cooperatively.
24. A working environment in which employees are respected is more conducive to good security than one that devalues and abuses them.
25. Security supervisors should get to know the staff from whom they need support.
26. Encourage social activities in the office.
27. Pay special attention to social outliers during instruction programs.
28. Monitor compliance more closely in both ends of the popularity range.
29. Work with the outliers to resist the herd's anti-security bias.
30. Include small gifts in your security-awareness program.
31. Start improving security a little at a time and work up to more intrusive procedures.
32. Before discussing security at a meeting, have one on one discussions with the participants.
33. Remain impartial and encourage open debate in security meetings.
34. Meet again after a consensus has been built and play devil's advocate.

POLICY DEVELOPMENT

Figuring out what needs to be done in *developing* security policies has several phases:

- *Preliminary evaluation*: what needs to be protected?
- *Management sensitization*: get support for systematic research within the organization.
- *Needs analysis*: involve every sector of the organization to determine needs.
- *Policies and procedures*: use existing frameworks.
- *Implementation*: explain and convince colleagues to cooperate.
- *Maintenance*: keep up with changes & keep personnel involved.



FIGURE 13.20 Policy must evolve.

PHASE 1: PRELIMINARY EVALUATION

Before you can do anything else, you have to know what needs to be protected. Nobody keeps firewood in the safe and financial securities in the garden shed. A preliminary inventory will help you convince upper management that the enterprise needs to develop a corporate information-security policy that reflects the risks your needs. Within that policy, your preliminary analysis will alert management to areas that need immediate attention.

The preliminary evaluation should be quick and inexpensive. Think in terms of days of work by a few people. You don't want to waste your time in expensive detail work before you get approval and support from your upper management.

As a network manager, you have clear ideas about what your networks are designed for. You know how they ought to be used. However, your users are the best source of insight into the ways your networks are *really* used.

Work closely with your *Human Resources* (HR) staff in developing the research instruments: they know (or should know) the key managers you should contact in each department. You'll need to get the managers on your side to be able to interview their staff. Provide a White Paper to everyone in the organization that lays out your reasons for asking for their time and energy.

Some of the HR people are likely to have the professional skills and experience required to provide accurate and cost-effective evaluations of beliefs, attitudes, and behavior affecting security. They may be able to help you construct unbiased questionnaires, organize focus groups, and help during interviews.

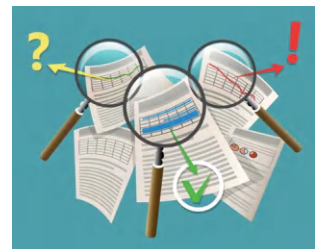


FIGURE 13.21
Get the big picture.

If you and your HR staff are not confident about this preliminary data collection, you should hire a consultant with proven expertise in collecting and analyzing social attitudes. Discuss such a study with a firm specializing in security audits and organizational analysis. If you don't know where to start looking, you can contact local universities and colleges and ask for the management-studies group (school, faculty, department or institute).

The following key issues should be part of your preliminary study, as they will be in more detail in subsequent phases.

- *Sensitive systems*: what shouldn't be universal knowledge? Imagine that you have an enterprise-wide electronic mail system. No one has ever asked you to put any particularly tight security on email. You think of it as mostly administrative stuff. But suppose you talk with your sales department staff. You learn that they send detailed reports on their prospects to their manager through your email. The prospect reports would be worth a fortune to your competition.
- *Critical systems*: what cannot be wrong without catastrophic effects? As part of your preliminary investigation, you chat with the users in your engineering department. They supply the new drawings required to respond to changes in major government contracts. They tell you the entire shop floor depends on these drawings.
- *Exposure*: how bad could things get if sensitive data were disclosed or critical data were wrong or unavailable? For example, if a competitor were to see the prospect reports you discussed with the sales staff, they could underbid you and win your business. Suddenly a whole new security dimension opens up in your thinking about the security of email. Similarly, you ask the engineering staff what would happen if any of their drawings were to be modified or damaged during transmission over the unsecured LAN. They explain that if someone were to alter dimensions or tolerances in any way, an entire production run could be ruined. Costs could run in the millions of dollars and lead to punitive damages for failing to meet specifications. Too many errors and you could be out of business. Suddenly it's clear that the integrity of those bits flowing through your network is worth a lot of protection.
- *Physical security*: what measures are in place already to safeguard equipment and people? I once found a network server in the wardrobe down where visitors put their muddy boots. No, because last year, you built a new enclosure for your LAN servers and gateways. OK, did anyone tell the security guards to check that room now that it has half a million dollars worth of data communications gear in it?
- *Access-control systems*: how are you currently ensuring that material and data are available only to those people who have legitimate reasons to get at them? Think about the unauthorized disclosure of the information moving through your data channels. Where could a dishonest employee or consultant tap into your channels? Where could outsiders gain entry to your networks? When was the last time you changed your modem telephone numbers? How heavily are the modems used? What kinds of information get transferred? How confidential are those data? There was a case some years ago in which an oil exploration company kept losing a series of bids for drilling rights. This was an odd problem; they made a point of using the best available geological data and financial cost estimates when setting their bids. In fact, they were highly competitive because of their use of modern technology – their financial estimates were transmitted to head office by modem. Over time, the company grew suspicious of the small margins by which they kept losing. Investigators found the reason for the run of bad luck: the modem transmissions showing how much to bid for those rights had been intercepted by wire-tappers for the competition.
- *Management and employee security awareness*: what do your colleagues believe about network security, how do they feel about the situation, and what do they actually do to protect corporate information? The best security apparatus on the planet can be defeated by uncooperative users. Knowing what they think (rightly and wrongly) will give you a heads-up warning on where your biggest challenges lie.

Throughout the preliminary evaluation, keep notes that will help you estimate the time required to put together an effective security policy and specific procedures.

- How many people will have to be interviewed once you get approval for the detail work.
- How many networks will you have to examine?
- How many networks application systems are there to analyze? Keep track of how long it's taking you to complete your initial interviews.
- Estimate how long it will take to interview everyone – then add a fudge factor for the unexpected (I habitually make my best guess and multiply by two, but you surely have your own experience to draw on).
- Keep a running tally of approximate costs for salary of your own staff during the preliminary analysis and use that tally to project the cost of a full-scale analysis.

PHASE 2: MANAGEMENT SENSITIZATION

Support from upper management is essential for further progress. Your goal in this phase is to get official support for an organization-wide audit and policy-formulation project. Some key points:

- In conjunction with the rest of the information-security project team, plan on a meeting that lasts no more than one or two hours.
- Start the meeting with a short statement about the crucial role of information in your organization's business.
- Use professional aids such as a management-oriented training video to sensitize the managers to the consequences of poor information security.
- After the video film, present your findings from the preliminary evaluation.
- Define an information-security working group to protect corporate information resources by
 - Setting priorities
 - Determining an action plan
 - Defining a timetable and milestones
 - Formulating policies and procedures
- Name the people you want to see on your working group.
- In your part of the presentation, emphasize the value of protecting networks.
- Provide estimates of the time involved and the costs of consulting services and software.



FIGURE 13.22 Generate management support.

You can end the briefing by offering the managers background reading¹⁷ about security. Some of them may be intrigued by this field; they more they learn, the more they will support your security efforts.

PHASE 3: NEEDS ANALYSIS

The information-security working group should include representatives from every sector of your organization. As you investigate your networks' security requirements, you need their experience and perspective to decide which areas to protect most strongly. More important, their involvement is a concrete expression of your concern for a fundamental attitude change in the corporate culture. Henceforth, security will be an *integral* part of the corporate culture.



FIGURE 13.23 Define specific needs.

For example, in a manufacturing firm, you'd include managers and staff from the factory floor, the unions, engineering, equipment maintenance, shipping and receiving, facilities management (including those responsible for physical security), administrative support, sales, marketing, accounting, personnel, the legal department and IT. Each of these members of the working group will help you improve your network security.

If your organization is very large, you may have to set up subcommittees to deal with specific sectors. Each subcommittee evaluates to what degree the systems and networks are vulnerable to breaches of security. For example, one group could focus on local and campus communications, another on wide-area enterprise networks, and a third on electronic data interchange with clients and suppliers.

Risk-analysis software is also available from several sources.¹⁸ These programs, in different degrees of detail and sophistication, ask users questions about their operations and estimate degrees of risk. The more advanced, and more expensive, programs use artificial intelligence (expert systems) to provide more precise probabilities of specific dangers. NIST published the *Guide for Selecting Automated Risk Analysis Tools* (NIST Publication #500-174) in 1989. Although the document has been officially retired. It is still available from NIST and still useful.¹⁹

PHASE 4: POLICIES AND PROCEDURES

When you have built a solid floor of understanding of your information-security needs, you're ready to construct the policies and procedures that meet your needs. Don't re-invent such policies from scratch; use existing policy frameworks as your scaffolding. Charles Cresson Wood, a respected authority in the security field, has recently published his 14th revision of *Information Security Policies Made Easy*.²⁰

It contains more than 1600 specific policies in written and electronic form; they cover everything one needs in establishing detailed, current information-security policies and procedures. Not only does Wood provide concrete examples of policies, he adds editorial explanations that clarify their intent. According to Wood, these policies are based on the best ideas from his decades of security-consulting practice with over 80 organizations. This excellent compendium will save you months of work.

When I provide consulting services to help clients develop their security policies, my contract explicitly stipulates that the client must buy a license for this extraordinarily useful resource (and I assure them that I have no financial interest in the purchase). In my view, working on security policies without using this resource is irresponsible.

Drafts of the proposed policies should be circulated among a team of representatives from each sector of the organization. These people must have volunteered to help; dragooning someone into reviewing policies is a waste of time. Pay attention to the questions, opinions, and especially complaints about the draft policies; every one of these responses must be treated seriously and respectfully.

Don't be impatient: you should expect to circulate *several* drafts of the proposed policies until there are an insignificant number of objections.

PHASE 5: IMPLEMENTATION

Once you've defined your policies, you're about halfway to your goal. The hardest part is ahead of you: explaining the need for security and the value of your new policies to all your fellow employees (or clients). Even if they agree intellectually, there's a good chance that their ingrained social habits will override your new rules for at least months and possibly years. Your task is to overcome these negative habits.



FIGURE 13.24 Instantiate needs in policies and procedures.



FIGURE 13.25 Moving from theory to reality.

Security policies and procedures require management support and sanctions. Begin your transformation of corporate culture at the top. Organize a half-day executive briefing session. In the section on network security, you can present your contributions to enterprise security.

- *Network security*: protection against eavesdropping and tampering.
- *Access controls*: password assignment, composition, lifetime, and confidentiality.
- *Encryption*: features, dangers, provision for emergencies.
- *Backup policies* for mainframes, networks, and workstations.
- *Security agreements*: summaries of the policies and procedures to be read and signed annually.

Your next target is the technical-support group, who will be the people who help explain your security policies to users. In a one-day training session, you cover:

- Everything you covered in the executive briefing
- Operating-system security provisions
- Security-software features
- Changes in operations to comply with new procedures

Lower-level staff need a half-day session that answers the following questions in terms that apply directly to their own work:

- Why should I care about information security?
- What are my obligations as an employee?
- How do I protect the PC I'm responsible for against viruses?
- How do I back up my data?
- How do I manage my passwords?
- What must I do if I see someone violating our security policies?

The class ends with the signature of the security agreement. Every employee should also read and sign the *annual* security agreement. There should be a simple online quiz to test employees' grasp of the security procedures; a high level (e.g., 80%) in this quiz should be required for acceptable performance. Failure to achieve the required level of competence in the quiz should result in additional training (preferably using additional materials such as videos, readings, and lectures) until the requisite level of competence is reached. Be sure to randomize the questions so that no one can easily cheat by using the answers to numbered questions in a previous exam.

These rigorous practices ensure that no one can argue that the organization's commitment to security is a superficial charade.

PHASE 6: MAINTENANCE AND ADAPTATION

Now that you've started the process of integrating a concern for network security into every aspect of your organization's work, you have to keep the issue fresh. Successful security-awareness programs²¹ can include amusing and creative posters, interesting videos, occasional seminars on stimulating security topics such as recent frauds or computer crimes and regular newsletters with up-to-date information.²²

There can be no fixed, static policy document that covers all eventualities. The information-security field changes constantly, and so must policies. Information security is a

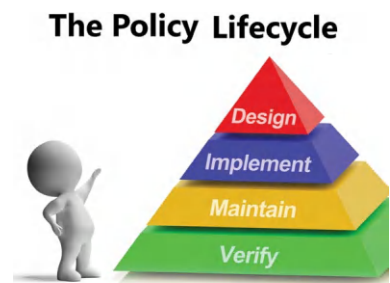


FIGURE 13.26 Policy cannot be static.

process much like total quality management: for success, both require a thoroughgoing integration into corporate culture.

Above all, some named individuals must see *maintaining security policies* as an *explicit part of their job descriptions*. Hoping that someone will spontaneously maintain security policies is like hoping that someone will spontaneously maintain financial records. However, security policies should represent the best efforts of people from throughout the organization, not the arbitrary dictates of just one person.

I strongly recommend that every organization commit to *Continuous Process Improvement* (CPI). For security policies, it should be easy for employees to suggest improvements in any aspect of policies. A committee that includes representatives from throughout the organization should meet periodically to consider those suggestions and update the policies as appropriate. The proposed changes should be circulated as draft for input; such exposure can contribute to a legitimate sense of policy ownership for employees. Major changes should be announced by upper management with an emphasis on explanations of those changes.

An *information-protection working group* can meet regularly – quarterly is a good frequency to try – to review all or part of the policies. Employees can be encouraged to suggest improvements in policies or to propose new policies. The working group can identify key areas of greatest change and work on those first, leaving minor policy changes to subcommittees. Members of the working group should discuss ideas with their colleagues from throughout the enterprise, not just with each other. Every effort should contribute to increasing the legitimate sense of involvement in security policy by all employees, including managers and executives.

Drafts of the new versions can be circulated to the people principally affected by changes so that their responses can improve the new edition. Truly respectful enquiry will result in a greater sense of ownership of the policies by employees, although few of them will rejoice in the new policies. Some employees will see new security policies merely as a mild irritant, while others may view them as a tremendous obstacle to productivity, and a general nuisance.

Ideally, major changes in policy should be described and explained in several ways. For example, a letter or email (digitally signed, one hopes) from the President, Chair of the Board of Directors, Chief Officers (CEO, CIO, CFO), or the CISO can announce important changes in policy and the reasons for the changes. A brief article in the organization's internal newsletter, or a spot on the intranet, can also provide channels for communicating the policy decisions to everyone involved.

WRITING THE POLICIES

Security policies should be written with clear indications that all employees are expected to conform to them. Language should be definite and unambiguous, e.g., "All employees must ..." or "No employees shall...." Some policies require people to do something – these are *prescriptive*; e.g., "Employees must follow the password procedures defined by the Information-Protection Group at all times." Other policies prohibit certain actions – these are *proscriptive*; e.g., "No employee shall make, order or install illegal copies of proprietary software under any circumstances."

Each policy should be short. Simple declarative sentences are best; writers should avoid long compound sentences with multiple clauses. Details of implementation are appropriate for standards and procedures, not for policies. Policies can refer users to the appropriate documents for implementation details, e.g., "Passwords shall be changed on a schedule defined in the *Security Procedures* from the *Information-Protection Group*."

Few people like to be ordered about with arbitrary rules. Trying to impose what appear to be senseless injunctions can generate a tide of rebellion among employees. It is far better to provide explanations of why policies make sense for the particular enterprise; however, such explanations can make the policies tedious to read for more experienced users. A solution is to provide *optional*



FIGURE 13.27
Clarity is crucial.

explanations – ideally, using hypertext. Readers can click on links for more details as they read the electronic documents. A less useful approach is to summarize policies in one part of the document and then to provide an extensive expansion of all the policies in a separate section or a separate document.

ORGANIZING AND PRESENTING THE POLICIES

Security involves a multitude of details; how one organizes these details depends on the purpose of the policy document. The most common format puts policies in a sequence that corresponds to some reasonable model of how people perceive security. For example, employees can look at security as a series of rings with a rough correspondence to the physical world.

Under this model, one might have a policy document with a table of contents that looks like this:

- Principles
- Organizational Reporting Structure
- Physical Security
 - Servers
 - Workstations
 - Portable computers
- Hiring, Management, and Firing
- Data Protection
 - Classifying information
 - Data access controls
 - Encryption
 - Countering industrial espionage
 - Communications Security
- Perimeter controls
 - Web usage and content filtering
 - Email usage and privacy
 - Telephone and fax usage
- Software
 - Authorized products only
 - Proprietary (purchased) software
 - Development standards
 - Quality assurance and testing
- Operating Systems
 - Access controls
 - Logging
- Technical Support
 - Service-level agreements
 - Helpdesk functions

The complete set of policies may be comprehensive, concise, and well written, but they will still likely be a daunting document, especially for nontechnical staff. To avoid distressing employees with huge tomes of incomprehensible materials, it makes sense to create special-purpose documents focusing on the security needs of particular groups. For example, it is pointless to provide the secretarial pool with policies defining internal firewall policies; it's also a waste of time to inflict details of separation of duty in accounting functions on the janitorial staff.

Organized!

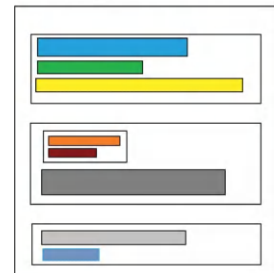


FIGURE 13.28

Organize the documents.

Policies should thus be made available in multiple formats. The topical organization presents policies in a sequence corresponding to an overall conception of security goals. For example, one can create different versions of the security policies to meet the interests and responsibilities of different sectors. One could have versions with different foci for different areas – perhaps starting at the external perimeter (physical security issues such as facilities protection, employee I&A for physical access, and loss-prevention policies) and working inwards to different functions.

One could usefully have guides like these:

- *General Guide for Protecting Corporate Information Assets*
- *Guide for Users of Portable Computers*
- *A Manager's Guide to Security Policies*
- *Human Resources and Security*
- *Network Administration Security Policies*
- *Programmer's Guide to Security and Quality Assurance*
- *The Operator's Security Responsibilities*
- *Security and the Helpdesk.*

Each of these files can present just enough information to be useful and interesting to the readers without overwhelming them with *irrelevant* detail. Each can make reference to the full policy document.

All the policies documents should be structured hierarchically, i.e., they should start with a general description and present increasing detail at lower levels.

PRESENTING THE POLICIES

Decades ago, most of the organizations I worked with used paper documents for their policies. Typically, employees would receive huge loose-leaf binders for the policies; some organizations also used short paper documents for specific purposes and even reference cards, summary sheets, stickers, and posters to communicate their policies. Updating this material was a nightmare: one would often see an employee's security binder topped with stacks of unopened envelopes containing quarterly updates that employees were supposed to manually insert into their binders to replace outmoded policies and include new ones. There's nothing wrong with providing cute, clever reminder cards or attractive posters reminding people of security policies as part of a security awareness campaign; however, expecting employees to maintain paper versions of policies that most see as secondary to their work is unrealistic.

When administrators at my university tried to get me to fill out paper forms, I digitized them, converted them to fillable PDF files, and sent them the completed forms as well as the blank ones with the comment that if these were not acceptable, I would send them the information in Sumerian cuneiform on clay tablets via mule train.

Policies are not inherently interesting. Large volumes full of policies quickly become shelfware. On the other hand, short paper documents are familiar to people; they can be carried around or placed at hand for easy reference anywhere. Reference cards, summary sheets, stickers, and posters are some of the printed media that can be useful in security awareness, training, and education programs. Printed text, like its electronic versions, provides the opportunity for typeface and color to be used in clarifying and emphasizing specific ideas. However, printed copies of policies share a universal disadvantage: they are difficult to update.



FIGURE 13.29 Outdated formats.

Updating dozens, hundreds, or thousands of individual copies of policy documents can be such a headache that organizations simply reprint the entire document rather than struggle with updates. Updates on individual sheets require the cooperation of every user to insert the new sheets and remove the old ones; experience teaches that many people simply defer such a task, sometimes indefinitely, and that others have an apparently limited understanding of the sequential nature of page numbers. Badly updated policy guides may be worse than none at all, especially from a legal standpoint. If an employee violates a new policy but available manuals fail to reflect that new policy, it may be difficult to justify dismissal for wrongdoing.

In today's world of near-universal access to computers in the work environment, electronic documentation of policies has enormous advantages from an administrative standpoint: all access to the policies can be controlled centrally, at least in theory. Making the current version of the policies and subsets of the policies available for reference on a server obviates the problem of updating countless independent copies. However, it is true that employees determined to defy authority can make their own copies of such files on most systems, leading to the electronic parallel to the normal situation when using paper: chaotic differences among copies of different age.

Centralized, unique electronic versions of policies are far more effective than any paper compilation can be. In addition, electronic policies offer hypertext, whether in HTML or XML, RTF and word-processor files, or PDFs and HELP files. Links allow users to find material quickly, reducing irritation and frustration when looking for specific policies. Having access to the single repository obviates the problems caused by individual storage of outdated materials. In addition, the most important function of hypertext for policy documents is to provide definitions of technical terms and explanations of the reasons for specific policies.

The most widely used hypertext format today is HTML. Its variant, XML, provides additional functionality for programmers, but from the user perspective the hyperlinks are the same. A simple click of the mouse in a Web browser can branch to a different section or page. More sophisticated programming allows the use of frames and, with JAVA or ActiveX, pop-up windows. Navigation buttons allow the user to move backward to a previous page or forward to another page. Links can also be used to open new windows so that several pages are visible at once. All of these techniques allow the user to move freely through a text with full control over the degree of detail they wish to pursue.

RICH TEXT FORMAT AND PROPRIETARY WORD-PROCESSOR FILES

Some people prefer to use word-processor files for hypertext. As long as everyone uses the same word-processing software, this approach can work acceptably. For example, it is usually possible to insert a hyperlink to a section of a single document, to a location in a different file on disk, or to a page on the Web. Some word processors, such as *MS Word* allow one to insert pop-up comments; floating the cursor over highlighted text brings up a text box that can provide definitions and commentary.

t file on disk, or to a
t pop-up comments,
definitions and

grams can display a
it. The headings can be
on as well as a constant

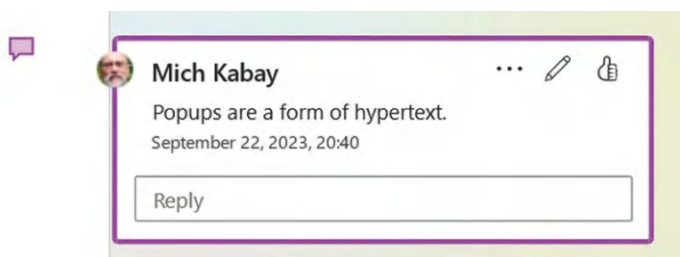


FIGURE 13.30 Popup in a WORD document.

In addition to explicit links, *MS Word* and other modern word-processing programs can display a table of headings that allows instant movement to any section of the document. The headings can be shown to the left of the document content, allowing quick access to any section as well as a constant overview of context.

One can also create an index by marking keywords in the text; the software then generates the complete list of references by page number.

PORTABLE DOCUMENT FORMAT

Adobe Acrobat's *portable document format* (PDF) provides all the hyperlinking that HTML offers, but it does so in a form that is universally readable, and that can be controlled more easily. The free *Acrobat Reader* (which allows printing and limited modifications to a file such as digital signatures and annotations) is available for multiple operating systems.²³

PDF documents can easily be locked, for example, so that no unauthorized changes can be made. In addition, unlike HTML and word-processor documents, PDF files can be constructed to provide near-perfect reproduction of their original appearance even if not all the fonts used by the author are present on the target computer system.²⁴



FIGURE 13.31 A different kind of acrobat.

ANNOUNCING CHANGES

Regardless of the medium through which one documents policies, it is critically important that *substantive* changes to the policies be announced clearly and in good time. Substantive changes are those that alter how people are to follow the rules; minor changes that don't alter the meaning of the policies don't have to be announced explicitly. For example

- The policy on passwords now requires approval by a new automated system that verifies that any proposed password conforms to complexity rules and is not the same as any of the previous passwords for that user. That's a substantive change.
- Someone misspelled the word "security" in a sentence, writing it as "securuity." That gets fixed without fanfare.



FIGURE 13.32 Announce changes clearly.

Communication of important changes can include:

- Verbal mention at meetings
- Email
- Notices on the appropriate pages of the appropriate web pages
- Lists of changes in each affected document
- Changes to existing training
- Addition of new training modules

For critical changes, users may be required to file confirmation that they have read, understood, and will comply with the changed policies.

NOTES

- 1 [Crawley \(2020\)](#).
- 2 [NIST Information Technology Laboratory \(1993\)](#).
- 3 [Cherry \(2019\)](#).
- 4 See “Access and Ego” section.
- 5 [Meyer \(2021\)](#).
- 6 [Nucleus Research \(2006\)](#).
- 7 [McNeil, Pauker, Sox and Tversky \(1982\)](#).
- 8 [NRC Committee on Risk Characterization \(1996\)](#).
- 9 *Framing Risk* section.
- 10 Quotations in this section are from [Lippa \(1990\)](#).
- 11 [Software Publishers Association \(1991\)](#).
- 12 [Latane and Darley \(1970\)](#).
- 13 See THE PARKERIAN HEXAD section of this text.
- 14 [Cherry \(2020\)](#).
- 15 U.S. Federal Bureau of Investigation
- 16 [Kelman \(1958\)](#).
- 17 [Kabay \(2021\)](#).
- 18 [N-Task \(2020\)](#).
- 19 [Gilbert \(1989\)](#).
- 20 [Wood \(2021\)](#).
- 21 [KnowBe4 \(2021\)](#).
- 22 [Herold \(2020\)](#).
- 23 [Adobe \(2021\)](#).
- 24 [Viahos \(2020\)](#).

WORKS CITED

- Adobe. (2021). *Adobe Acrobat Reader DC*. Retrieved November 9, 2021, from Adobe: <https://get.adobe.com/reader/>
- Cherry, K. (2019, September 23). *The Role of a Schema in Psychology*. Retrieved November 11, 2021, from Very Well Mind: <https://www.verywellmind.com/what-is-a-schema-2795873>
- Cherry, K. (2020, May 26). *What Is Reciprocity?* Retrieved December 17, 2021, from VeryWellMind | Theories | Social Psychology: <https://www.verywellmind.com/what-is-the-rule-of-reciprocity-2795891>
- Crawley, K. (2020, May 5). *Cybersecurity Budgets Explained: How Much Do Companies Spend on Cybersecurity?* Retrieved November 8, 2021, from AT&T Cybersecurity | Security Essentials: <https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget>
- Gilbert, I. E. (1989, October). *Guide for Selecting Automated Risk Analysis Tools*. Retrieved November 8, 2021, from NIST | Publications | Legacy | Special Publications: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-174.pdf>
- Herold, R. (2020). *Privacy Professor*. Retrieved November 8, 2021, from PrivacyGuidance: <https://www.privacyguidance.com/>
- Kabay, M. E. (2021, May 10). *Infosec Management*. Retrieved November 8, 2021 from M. E. Kabay: <http://www.mekabay.com/infosecmgmt/index.htm>
- Kelman, H. C. (1958). Compliance, identification, and internalization: Three processes of attitude change. *Journal of Conflict Resolution*, 2(1), 51–60. <https://doi.org/10.1177/002200275800200106>
- KnowBe4. (2021). *Human Error. Conquered*. Retrieved November 8, 2021, from KnowBe4: <https://info.knowbe4.com/asap-ga-video>
- Latane, B., & Darley, j. M. (1970). *The Unresponsive Bystander: Why Doesn't He Help?* (Vol. 1). Prentice Hall. Retrieved December 17, 2021, from <https://smile.amazon.com/Unresponsive-Bystander-Why-Doesnt-Help/dp/0139386130/>
- Lippa, R. A. (1990). *Introduction to Social Psychology* (Vol. 1). Belmont, CA, USA: Wadsworth Publishing Co. Inc. Retrieved November 11, 2021, from <https://smile.amazon.com/Introduction-Social-Psychology-Richard-Lippa/dp/0534982107>
- McNeil, B. J., Pauker, S. G., Sox, H. C., & Tversky, A. (1982, May 27). On the Elicitation of Preferences for Alternative Therapies. *New England Journal of Medicine*, 306, pp. 1259–1262. <https://doi.org/10.1056/NEJM198205273062103>

- Meyer, B. (2021, October 15). *Most Common Passwords: Latest 2021 Statistics*. Retrieved November 11, 2021, from Cybernews: <https://cybernews.com/best-password-managers/most-common-passwords/>
- NIST Information Technology Laboratory. (1993, September 20). *Proceedings of the 16th National Computer Security Conference*. Retrieved September 19, 2023, from NIST | Publications | 1993: <https://csrc.nist.gov/pubs/conference/1993/09/20/proceedings-16th-national-computer-security-confer/final>
- NRC Committee on Risk Characterization. (1996). *Understanding Risk: Informing Decisions in a Democratic Society* (Vol. 1). (P. C. Stern, & H. V. Fineberg, Eds.) Washington, DC: The National Academies Press. <https://doi.org/10.17226/5138>
- N-Task. (2020, April 11). *The 19 Best Risk Management Software of 2021*. Retrieved November 8, 2021, from nTaskManager: <https://www.ntaskmanager.com/blog/best-risk-management-software/>
- Nucleus Research. (2006, October 18). *Research Note G68: Benchmarking: The Sad Truth About Security*. Retrieved November 11, 2021, from Nucleus Research: <https://web.archive.org/web/20061114091231/http://www.nucleusresearch.com/research/g68.pdf>
- Software Publishers Association. (1991). *It's Just Not Worth the Risk*. Retrieved September 19, 2023, from Archive | Details: <https://archive.org/details/its-just-not-worth-the-risk>
- U.S. Federal Bureau of Investigation. (n/a, n/a n/a). *Nigerian Letter or "419" Fraud*. Retrieved November 9, 2021, from FBI | Scams and Safety | Common Scams and Crimes: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud>
- Viahos, J. (2020, September 13). *How to Embed Fonts in PDFs (and Why You Need to Do It)*. Retrieved December 14, 2021, from Printivity Insights | Design | Design Tips & Tutorials | Print Ready Files: <https://www.printivity.com/insights/2020/09/13/how-to-embed-fonts-in-pdfs/>
- Wood, C. C. (2021). *Information Security Policies Made Easy, 14th Edition*. Retrieved from Information Shield: <https://informationshield.com/products/information-security-policies-made-easy/>

14 Programming for Security

This chapter reviews well-established principles for writing secure code. Topics include

- Using databases (DBs) for good security
- Avoiding poorly designed file structures
- Planning for safe concurrent access
- Designing secure DBs
- Avoiding systemic problems in DB design

A reader of my *Network World Security Strategies* column wrote to me in 2001 with an interesting series of questions (shown in *italics* below):



FIGURE 14.1

Secure programming results.

- *I've been reading about security problems with the various OS components, both Windows and Linux, and the problems with security with applications software. Where is the best place to start implementing system security?*
 - It seems to me that security should be integrated into the requirements analysis, the design stage for software, the operating system security kernel, in corporate policy development and in human awareness, training and education programs.
- *Should security start with the computer programming languages themselves, or their support libraries?*
 - PASCAL uses strong typing and requires full definition of data structures, thus making it harder to access data and code outside the virtual machine defined for a given process. In contrast, C and C++ allow programmers to access any region of memory at any time the operating system permits it.
 - There are several sets of security utilities available for programmers.
- *With so many PCs linked via networks and the Internet, shouldn't all programs be coded with the assumption that the programs will be operating in an environment where they may very probably be subject to hostile attack?*
 - Yes, but the difficulty in testing for security is that there are so many possible ways to generate security holes in code. Buffer overflows, for example, are the most common form of security exploit, but clearly the programmers never thought to impose length restrictions on the input strings being handled by Web server software.
- *Do any current computer programming languages give programmers tools with which to implement security best practices in their code?*
 - All computer languages allow you to write code as well as you can smile. I think that strongly typed languages may offer better constraints on programmers, but the essential issue is that the programmers must continue to think about security as they design and implement code.
 - Java does include provisions for limiting access to resources outside the “sandbox” reserved for a process.
- *Is there any such thing as security best practices for computer programmers?*
 - There are recommendations on security related aspects of programming in most general information-security textbooks.
 - In addition to designing security into a system from the start, there are some obvious guidelines that can apply:

- Impose strong I&A for critical and sensitive systems in addition to the I&A available from the operating-system, ideally, use token-based or biometric authentication as part of the initialization phase of your application.
- Document your code thoroughly, including using data dictionaries for full definition of allowable input and output to functions and allowable range and type of values for all variables.
- Use local variables, not global variables, when storing sensitive data that should be used only within a specific routine, i.e., use the architecture of the process stack to limit inadvertent or unauthorized access to data in the stack.
- Re-initialize temporary storage immediately after the last legitimate use for the variable, thus making scavenging harder for malefactors.
- Limit functionality in a specific module to what is required for a specific job, e.g., don't use the same module for supervisory functions and also for routine functions carried out by clerical staff.
- Define views of data in DBs that conform to functional requirements and limit access to sensitive data, e.g., the view of data from a medical-records DB should exclude patient identifiers when the DB is being used for statistical aggregation by a worker in the finance department.
- Use strong encryption (NOT home-grown encryption) that has industry-standard routines to safeguard sensitive and critical data on disk. Locally developed, home-grown encryption is generally NOT as safe.
- Disallow access by programmers to production DBs.
- Randomize or otherwise mask sensitive data when generating test subsets from production data.
- Use test-coverage monitors to verify that all sections of source code are in fact exercised during quality assurance tests; investigate the functions of code that never gets executed.
- Integrate logging capability into all applications for debugging work, for data recovery after crashes in the middle of a transaction, and also for security purposes such as forensic analysis.
- Create log-file records that include a cryptographically sound message authentication code (MAC) that itself includes the MAC of the preceding record as input for the algorithm, this technique ensures that forging a log file or modifying it will be more difficult for a malefactor.
- Log all process initiations for a program and log process termination; include full details of who loaded the program or module.
- Log all modifications to records and optionally provide logging for read-access as well.
- Use record-level locking to prevent inadvertent overwriting of data on records that are accessed concurrently. Be sure to unlock a sequence of locks in the inverse order of the lock sequence to prevent deadlocks (thus if you lock resource A, B, and C in that order, unlock C, then B, then A).
- Sign your source code using digital signatures.
- Use checksums in production executables to make unauthorized modifications more difficult to conceal.¹

DATABASE MANAGEMENT AND SECURITY

DBs are ubiquitous and, like many pervasive infrastructure, sometimes we have to remind ourselves to consider their security implications. How often do most people think about the security implications of electrical systems, air-conditioning, data archives, and garbage? Security specialists do, yet I rarely meet security specialists who explicitly include DB-management systems in thinking about their organizations' security. That's ironic, because the huge data leakages of which we read constantly are almost always related to data from DBs.

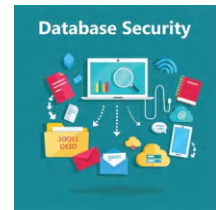


FIGURE 14.2

DB security matters.

We regularly hear about cyberattacks involving brute-forcing secure logins or exploiting software flaws, but there's a new segment of the cybercriminal economy that's growing fast: attackers who target companies that have unintentionally left data out in the open via misconfigured DBs.²

But why not just leave DBs to *DB Administrators* (DBAs)?

At one level, having at least a grasp of the principles of *DB management systems* (DBMS) security is as important to security professionals as having a grasp of programming principles or of telecommunications principles. We need to be able to speak a common language with our colleagues as we discuss IA.

At another level, understanding how DBs are designed and implemented speaks to our need as security professionals for a supportive relationship to our users, because data requirements and data relationships are at the heart of security requirements. As I'm sure you've heard many times, it's the rare organization where security is the driving force; we serve the strategic goals of the organization and that means we need to understand data requirements. On another level, there are security implications to how programs and data structures work; understanding how DBs work gives us insights into why the user interfaces work as they do and, even more important for security personnel, how systems can fail or be abused.

On a practical level, you may yourselves need to create a DB or participate in reviewing the security requirements for a DB and having a solid grasp of the principles will help you assimilate the details of any specific points you need to learn.

This section reviews principles of DBMS, security implications of DB structures and access methods for concurrency control, recovery strategies and effective DB resource management as essential components of good security and business continuity management. We start with a look at the state of data management in the 1960s and 1970s and how the development of the *relational database model* (RDBM) measurably improved IA.

CHAOTIC FILE STRUCTURES

The development of the *relational database management system* (RDBMS) was a tremendous boost to the security of data management in the 1960s and 1970s. The problems we faced then were deeply related to security.

The fundamental problem of data structures in the 1960s is that there was nothing to provide linkages among the data stored in files. If a programmer needed to use information in one file as a pointer to locate information in another file – for example, to look up an order number for customers so that they could locate the order details for a current order – everything had to be done in a specific program.

Keeping track of record numbers, doing comparisons between a search value and the values in records that were being read serially, defining the record structures for every file – these functions resided in each individual program. Make a mistake in writing one program and the results could ricochet through the entire system by corrupting values that would then be read by other programs.



FIGURE 14.3

Messy and insecure data.

There were no safeguards on what you could put into a file other than what a specific program written by specific programmer happened to include as a limitation. Did you want to change a restriction on the values in a particular field? Sure – go find every single program needing the change and then make all the changes, and then recompile all of those programs and hope you got it right.

Another problem was that in the absence of any theory for organizing data, it was very easy for programmers to duplicate data. For one thing, there might be more than one programmer on the system; so, it wasn't unexpected that, say, a customer record might be duplicated in files used by the accounting department for billing and by the order-processing department for inventory controls. The problem occurred when somebody needed to change the customer information – for example, if the customer got a new telephone number. Because there was no theoretical basis deciding how to store information relating one type of data to another, it was hard for programmers to figure out how to store related information. Should you store repeated information in a single record or in multiple records? For example, if you were storing data about orders, should you create a single record that looked like an order form or was there a better way? Should you replicate information to every record where it might be useful? For example, should you put contact information for a customer into every order header?

Documentation was always a mess: nothing in the file itself described the record structure; the only description was in the program data definitions – and many programmers had still not heard of in-line comments. Sometimes, programmers would scribble file definitions on pieces of paper; I personally remember seeing clipboards with file structures hung on nails on the wall in the programming area. File incompatibilities could develop very easily under such circumstances; different programmers could easily diverge in their file structures without knowing it. Even a single programmer might forget the details of a less-used file and find a program wreaking havoc by mistake by reading information and interpreting it wrongly or by trashing existing records with malformed data. When different programmers or a forgetful individual programmer stored the same data by different names in different files, their inconsistencies could lead to unexpected errors.

In a sense, the problems of data structures paralleled the early problems of controlling printers. Printing was fraught with tedious details: we had to get the right file structures, incorporate them into our data definitions within the programs, create the output record formats in detail – every single position, every punctuation mark, every separator – and even, in the older systems which had no printer drivers, take into account the specific attributes of the printers we were dealing with. At that time, some systems still had no spoolers (SPOOL meant *Shared/Simultaneous Peripheral Operation On Line*): a program controlled a given printer directly – if by mistake, another program started writing to a printer in use, you might actually get a mixture of data appearing in a jumbled mess on the printer.

RDBMSs were conceptually similar to the development of spoolers and printer drivers: they provided a standardized method for control of data in a way that eliminated the need for special coding within each program and they took care of the next problem faced by filesystems: concurrency, which is the topic of the next section.

CONCURRENCY AND CODD

Concurrency was a nightmare for early programmers.

If two programs access a single data file at the same time and both programs attempt to make changes to the same data, there is a real possibility that the second one to write into the file will destroy the changes made by the first one.

The classic *lost update* problem can be illustrated by this sequence of events:

1. Joe's process reads the inventory file and puts a copy of the Widget total in a memory buffer (variable): there are 25 Widgets.
2. Moments later, Shakheena's process also reads the same record and puts 25 Widgets into her buffer.

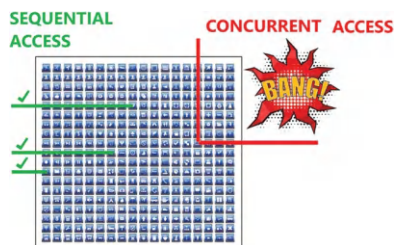


FIGURE 14.4

Must control concurrency.

3. Joe takes out 10 Widgets from his copy of the inventory total and writes out the inventory record to show that there are 15 Widgets left.
4. Shakheena takes out 5 Widgets from her copy of the original inventory total and writes out the inventory record to show that there are 20 Widgets left.

So how many Widgets are left in reality after Joe and Shakheena both withdraw their amounts from their copies of the original inventory total? Well, you can see that although Shakheena's overwriting of Joe's total seems to put 20 Widgets in inventory, actually there are only 10 left.

One approach was to *serialize* access to the files so that only one process could access the data file at a time; however, blocking access to the entire file was out of the question for multiuser systems where dozens or hundreds of users (that was a lot of people 50 years ago) were supposed to be accessing the same data collection at the same time. Serializing access to the entire file had unacceptable performance consequences.

Dr E. F. Codd³ was working for IBM in their San Jose research laboratory when he developed the RDBM that he published in 1970. He and fellow IBM scientist Christopher J. Date pursued the relational model and were instrumental in developing the *Structured Query Language* that we universally know as SQL, usually pronounced “sequel” and sometimes simply by the letters of its acronym.⁴

Codd defined a DB as “a self-describing collection of integrated records.” There are some pretty significant words in the definition before you. And it is a *model of a model*. We will look at each of these concepts in turn in subsequent sections of this text.

THE DEVELOPMENT OF DBMSS

You'll recall how much trouble unstructured collections of individual files can be; DBs are collections of files that include self-referential data. Data about the data are called *metadata*; they can be read and interpreted by the DBMS and thus used to communicate with the application programs accessing the data.⁵

The *data dictionary* contains some (not all) of the metadata and defines attributes of all the fields and records, including logical constraints on the data ranges and relationships among the data. Metadata include names, editing constraints such as allowable ranges, and relationships among records such as the number of records that share a common value (called a key). Because the metadata reside with the data instead of inside the compiled programs, maintaining programs becomes vastly simplified. In the same way, the metadata provided documentation about the DB, reducing the errors and inconsistencies that are inherent with manually maintained, replicated copies of system documentation.

Metadata extend integration by providing performance-enhancing indexes for common lookups; DBs can even store default formatting such as number of visible decimal places in displaying a field, for output such as displays or paper reports.

The curious phrase “a DB is a model of a model” expresses the notion that DBs do not have to be what is called *isomorphic* with reality; that is the structure of the DB is an abstraction from reality. Indeed, it is a *second-order* abstraction in the sense that DB designers represent *their* view of what they understand from interviewing *users*. Naturally, the users are expressing *their* perspective on reality. The implication is that a DB design should never be viewed as rigidly fixed for all eternity; it is an *instantiation* of one *interpretation* of a *view* of reality.

Another comment is something that I have been teaching for decades: *the availability of the tool determines perceptions of what is possible*. One of the most striking experiences I ever had as a consultant occurred in the mid-1980s when I was just striking out on my own. I was helping a clothing factory in Montréal to optimize their DBs and the head of IT and I were walking through the offices one day when I stopped dead in my tracks. I pointed to an employee at a desk and asked the VP if we



FIGURE 14.5
DBMS controls
data structure
and access.

could go speak to him. “Hi,” I said, “whatcha doin’?” Well, said the employee, he was calculating subtotals based on a report. You see, it was precisely the sight of someone using a calculator with a computer printout that got my curiosity going. “Have you done this before?” I asked. “Sure,” he said, “every month for the last three years.” “Did you ever ask anybody to put the subtotals into the report for you?” He stared at the VP and me in astonishment and said, “They can DO that?” And this is why I am telling you this story. It seems that nobody had ever walked around finding out what the employees needed or telling them what was possible.

From a security standpoint, the risk of errors resulting from any manual process should raise hackles; that the manual process was being repeated month after month for years was an appalling potential source of data-integrity problems.

The lesson, even for security experts, is that we need to use the time-tested technique of MBWA: *management by walking around*.⁶ There is no substitute for contact with reality. All the reports in the world are just hearsay: go out and see for yourself what’s happening in your working environment.

DBMS COMPONENTS

A DBMS includes DBs and the tools for building, modifying, monitoring, securing, and repairing them. A DB contains *files* – sometimes people call them *tables* and in some systems they are called *relations* or *datasets* – each of which consists of *records* (also called *rows* or *tuples*) in which there are *fields* (also called *columns* or attributes). Designers establish *relationships* or *links* among tables to help locate data; these linkages among the tables help users navigate through the DB.

It’s the DB *application* that provides a particular way of accessing the DB; for example, a particular DB application might be an accounting program or a production-control program or a patient-records program. DB applications provide for our control over what constitutes acceptable data; for example, an inventory system can include provisions for defining reorder points to prevent exhaustion of parts supplies.

DB applications provide user interfaces so that employees can enter data quickly and correctly as well as locating data using interactive queries or stored procedures. Applications normally include capabilities for creating new reports as well as for generating predefined reports.

The DBMS also includes a DB application with general capabilities often called a *query* program. Users with little or no programming experience can use the query program to work on subsets of their data to answer specific questions, for calculations and to generate reasonably sophisticated reports with features like sorting, subtotals, headers, and even graphs. Unfortunately, query programs run by DBAs may also bypass normal security restrictions, resulting in security problems if they tamper with the self-consistent data of the DB.

Access by an application program to the data flows through an *application-program interface* (API) which in turn depends on the internals of the DBMS to interpret metadata from the data dictionary. The metadata translate requests for functional definitions of the data such as the name of a patient into pointers to records and descriptors of the specific parts of the records that correspond to the needed data.

The relational model has a number of strict requirements. The most important is that every single record must be unique. That means in practice that we are going to have to name an attribute of the information that is naturally unique or alternatively, to impose one that we can force to be unique. We call the unique identifier of the record the *key*.

Keys make an enormous difference to the structure and performance of DBs. Keys can consist of a single field or of several fields that are concatenated to form a *compound key*. Keys can be used to create a special set of pointers called an *index* (plural *indexes* or *indices*) that can greatly speed access to records. For example, if *patient_ID* is a key for treatment records, then one could have the DB almost instantly retrieve the records of treatments for a specific patient without having to read



FIGURE 14.6
Know your tools.

all of the patient records to find the right ones. The *patient_ID* key allows the DBMS to use random access (direct I/O) with a specific record number instead of serial access (serial I/O).

Defining appropriate keys is critically important in designing DBs. The choice of keys depends very much on the kinds of questions that users typically ask; one of the concerns is that keys add to the overhead of the DB – both in terms of requiring extra storage space for the pointers (some define a chain of values with the same key and others point to the start or end of the chain) and in imposing a performance cost whenever we add or delete records (because we have to modify pointers to keep the chain descriptors correct).

Choosing the right keys is at the heart of the DB designers' skillset. Just as an example, imagine an order-entry system in which the only key to the order dataset were mistakenly defined as *customer_ID*; it would be impossible to have more than one order in the dataset per customer – a ridiculous constraint.

Continuing our imaginary order-entry system example, suppose an amateur DB designer decided to include full customer information (name, address, telephone number) in the same record as the order number and the date of an order (what we call an order-header, which corresponds to the top of an order form). Suppose a very large customer had 3,000 orders in the DB – are we to accept that there should be 3,000 copies of the same information stored uselessly in the order-header file? Ridiculous. We prevent these problems in the process called *normalization*, which is the subject of the next articles in this series.

DATA ANOMALIES AND NORMALIZATION

Before Dr E. F. Codd and his colleagues formalized the reasoning for deciding how to group data into records (relations, rows, tuples), programmers were always running into problems that qualify as security issues: they would discover that users were causing their files or primitive DBs to lose critically important data.

Suppose we naïvely defined an inventory record that put all the details about items in a store into a single record; how would we keep track of the items in our store if we deleted the last record that includes the item information? How do we store information about an item that nobody has bought yet? Why are we storing copies of the information about the same items and the same people?

The *deletion anomaly* results from badly normalized data structures. For example, erroneous record layouts can mix information about fundamentally different entities. There's no good reason to store details about a doctor other than the doctor's unique identifier in the record pertaining to a patient. There's no good reason to store information about a car other than the unique identifier of the car in the same record as price information about types of repairs. These non-normalized data structures don't make sense even if we don't know much about DBs.

A dataset that mixes detailed information about a part with radically different information about where the parts are stored causes a real headache. We need to separate the information about the parts from the information about how many there are and where they are kept. What we can do is to keep a record that links a specific part number to a specific bin number and lists how many of that part are in that bin. Now that is a normalized design and it easily handles information about parts that are out of stock, bins that are empty, and parts that are in more than one bin.

Problems can occur in a poorly structured DB when we delete records. For example, consider a library DB in which we delete the record with information about the publisher when there are many books that point to that publisher. You can see that removing the only record that tells us the name, address, telephone number, and so on for the publisher could be very harmful for the library and would make the book records that point to the nonexistent publisher record meaningless (e.g., they might have the number 2345 which used to point to Taylor & Francis which now wouldn't mean anything at all).

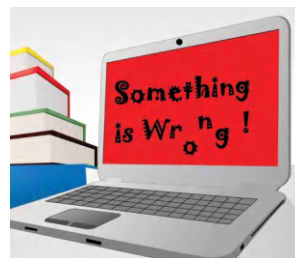


FIGURE 14.7 DB errors can be disastrous.

DBs have strict rules which make it impossible to cause this kind of havoc; we call these rules *referential integrity constraints*. Other examples include not being able to add a record that duplicates a unique key value in a dataset or not being allowed to add a record that points to a nonexistent key. As an example of the latter, an order-entry system would prevent an operator from adding an order for a client that does not yet exist in the DB. First you add the client record, then you can add the order placed by that client.

You are (perhaps unconsciously) familiar with such constraints simply from having bought things on the Web, where it is perfectly normal for us all to fill out an identification form about ourselves *before* we can place our order containing the items we want to buy. The next time, however, if we allow the vendor to keep our information, we can just identify ourselves and fill out the details of the new order.

These DBMS rules improve security by reducing violations of confidentiality, control, integrity, authenticity, availability, and utility. Surprise!⁷

NOTES

- 1 Nichols, Kabay, and Braithwaite, *Writing Secure Code* (2014).
- 2 Bressers (2021).
- 3 History Computer (2021).
- 4 Target (2017).
- 5 Incidentally, I happen to continue using words with “data” as plurals because of my early years of learning Latin, but almost no one else does anymore. You can be perfectly correct nowadays saying “data is” or “metadata is.”
- 6 Belyh, *Management by Walking Around (MBWA) – The Essential Guide* (2021).
- 7 Readers may find my course materials on *Database Management* helpful: see the PowerPoint lectures at < https://www.mekabay.com/courses/academic/norwich/cs240/cs240_lectures/index.htm >.

WORKS CITED

- Belyh, A. (2021). *Management by Walking Around (MBWA) – The Essential Guide*. Retrieved November 11, 2021, from Cleverism: <https://www.cleverism.com/management-by-walking-around-mbwa/>
- Bressers, J. (2021, February 17). *Accidental Database Breaches Are on the Rise – How Can Your Company Avoid Becoming the Next Headline?* Retrieved November 11, 2021, from Security Magazine: <https://www.securitymagazine.com/articles/94622-accidental-database-breaches-are-on-the-rise-how-can-your-company-avoid-becoming-the-next-headline>
- History Computer. (2021, January 4). *Edgar Codd – Complete Biography, History, and Inventions*. Retrieved November 11, 2021, from History Computer: <https://history-computer.com/edgar-codd-complete-biography/>
- Nichols, L. E., Kabay, M. E., & Braithwaite, T. (2014). *Writing Secure Code*. In *Computer Security Handbook* (6th ed., Vol. 1); John Wiley & Sons, Inc. Retrieved November 10, 2021, from <http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/>
- Target, S. (2017, December 29). *Important Papers: Codd and the Relational Model*. Retrieved November 11, 2021, from Two-Bit History: <https://twobithistory.org/2017/12/29/codd-relational-model.html>

15 INFOWAR

Throughout history, technology has provided both weapon and target. When warriors mounted horses, their steeds were at once a threat to opponents and vulnerable to attack. A single horseman could dominate a battlefield of foot soldiers, but to stop the horseman, the enemy had only to stop the horse. And to imperil a nation of horsemen, the enemy had only to poison the herds' water supply.

The defining technology since the late 20th century is the computer. Computers are pervasive, necessary, and vulnerable to attack. Increasingly, they are linked in networks spanning both corporate and national boundaries. They are on work desks, in briefcases, and in people's pockets and handbags. But although connectivity opens possibilities for electronic commerce, it also opens opportunities for electronic crime, espionage, and outright warfare.

Attacks on data confidentiality and possession, and on the integrity, authenticity, availability, and utility of those data can cause untold damage. No one is immune: individuals, corporations, government departments and agencies, nations and supranational bodies like the United Nations and NATO are all vulnerable. We need to erect legal, organizational, and cultural defenses against information warfare at all these levels. IT managers, in particular, must familiarize themselves with the threat and begin to put in place systems that will minimize their organizations vulnerability to electronic warfare.

This chapter reviews

- Winn Schwartau's pioneering definitions of the levels of INFOWAR
- Specific cases of INFOWAR

SCHWARTAU'S THREE LEVELS OF INFOWAR

In his pioneering book, *Information Warfare: Chaos on the Electronic Superhighway*¹, security expert Winn Schwartau defines three levels of *information warfare* (INFOWAR) focusing on the *targets* of the attacks:

- Interpersonal
- Inter-corporate
- International

There are countless resources for tracking cyberattacks; for example, using search string < *latest hacking news* > for the GOOGLE search engine produced 96 million hits in November 2021. A few of the excellent sources include:

- *RISKS Digest: Forum on Risks to the Public in Computers and Related Systems*²
- *WIRED* using < hacked > as the search term³
- *BBC News*⁴
- *CNN*⁵
- *The Hacker News*,⁶ which has pages for Data Breaches, Cyber Attacks, Vulnerabilities, and Malware



FIGURE 15.1
Information: Target
and weapon.



FIGURE 15.2 Chaos
on the electronic
superhighway.

INTERPERSONAL ATTACKS

Interpersonal electronic warfare involves individuals who target other individual, corporate resources, and governmental resources. A constant stream of cases⁷ include impersonation and defamation in cyberspace (e.g., false attribution of damaging communications),⁸ appropriation of credit records for fraud and theft,⁹ harassment (e.g., death threats),¹⁰ and loss of privacy (e.g., theft of medical records).¹¹

In cases of fraud and theft, victims in the U.S. are in serious trouble once thieves obtain their Social Security Numbers (or equivalents in other countries) and credit records and order credit cards in the victim's name. Criminals can rack up hundreds or thousands of dollars of purchases and then default on the payments, leaving the original owner of the electronic identity to pick up the bill. Not only do the victims suffer the crime and bear the burden of the legal costs, but their credit ratings are ruined, sometimes for the rest of their lives. Victims may suffer severe emotional distress about this abuse.¹²

Scams such as the *advance-fee fraud*¹³ and the *refund and recovery scams*¹⁴ trick gullible victims into providing access to their financial accounts; some actually voluntarily authorize payments to the criminals, often blissfully unaware that it is out of the question for legitimate organizations to ask for gift cards as a form of payment.¹⁵

In other interpersonal information warfare cases, criminal hackers have harassed their victims by manipulating their phone services. On one occasion, the notorious *phone phreak* (as these hackers are called) Kevin Mitnick turned a victim's home telephone account into a coin-operated phone which demanded deposit of a quarter even though there was of course no coin slot.¹⁶

Criminals can also engage in *doxing*, which involves making private information such as addresses and phone numbers public. For example, some jurors, lawyers, and prosecutors involved in trials (Otten, 2023) have been doxed by supporters of accused criminals; the victims are then subject to threats of violence and even of murder.¹⁷



FIGURE 15.3 Attacking individuals.

INTER-CORPORATE CYBERCONFLICTS

The *inter-corporate* category includes attacks on corporate resources by agents of other corporate entities.¹⁸ In one case that went through a U.S. court, a judge summarized the issues as follows:

Compulife Software, Inc., which has developed and markets a computerized mechanism for calculating, organizing, and comparing life-insurance quotes, alleges that one of its competitors lied and hacked its way into *Compulife's* system and stole its proprietary data.... At one point ... the defendants also employed a hacker named Natal, who, it is undisputed, took *Compulife's* data for use in the defendants' software.... [T]he defendants hired a hacker, Natal, to 'scrape' data from its server. *Scraping* is a technique for extracting large amounts of data from a website.

The hacker created a bot to collect a partial copy of *Compulife's* Transformative Database, extracting all the insurance-quote data pertaining to two zip codes—one in New York and another in Florida.... [T]he bot requested and saved all premium estimates for every possible combination of demographic data within those two zip codes, totaling more than 43 million quotes.¹⁹

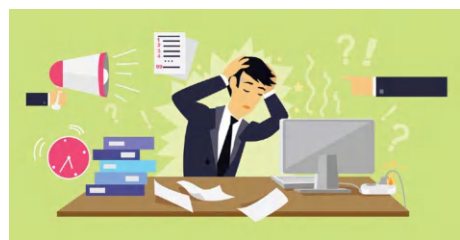


FIGURE 15.4 Cyber-headaches at work.

Ransomware attacks involve unauthorized encryption of data – including often corporate data – by criminals, usually in gangs. The criminals demand money for access to the decryption keys.²⁰ The best defenses against such attacks include:

- Maintaining up-to-date defenses through current patches to all software.
- High-quality anti-malware products.
- Frequent backups (e.g., daily) kept on storage media that are disconnected from the systems and networks.

INTERNATIONAL INFOWAR

Nation states in conflict have always focused on disabling critical infrastructure. For example, critical infrastructure in the Roman Empire included “the road system, agriculture and food stores, and the most beautiful, yet practical of them all, her aqueducts.”²¹ Methods of this form of conflict include not only classical disruption such as hacking, data destruction, DoS and DDoS, and *psychological operations* (PSYOPS) which often involve DISINFO.²²

The *Rand Corporation* carried out information-warfare exercises in 1995 which resulted in a report to the *IW Executive Board* of the U.S. Department of Defense.²³ The report included the following “seven defining features of strategic information warfare”:

- *Low entry cost*: Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.
- *Blurred traditional boundaries*: Traditional distinctions — public versus private interests, warlike versus criminal behavior — and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.
- *Expanded role for perception management*: New information-based techniques may substantially increase the power of deception and of image-manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives.
- *A new strategic intelligence challenge*: Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.
- *Formidable tactical warning and attack assessment problems*: There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents.
- *Difficulty of building and sustaining coalitions*: Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage.
- *Vulnerability of the U.S. homeland*: Information-based techniques render geographical distance irrelevant; targets in the continental U.S. are just as vulnerable as in-theater targets. Given the increased reliance of the U.S. economy and society on a high-performance networked information infrastructure, a new set of lucrative strategic targets presents itself to potential IW-armed opponents.



FIGURE 15.5 Global cyberconflicts.

RUSSIA

The Russian government waged a systematic DISINFO campaign in the U.S. 2016 election:

The operation was complex. What is publicly known now is perhaps most easily understood in two pieces, the subjects of separate federal indictments.

First, a billionaire Russian businessman and Putin associate allegedly assembled a network of troll factories; private Russian companies engaging a massive disinformation campaign. Their employees posed as Americans, created racially and politically divisive social media groups and pages, and developed fake news articles and commentary to build political animosity within the American public.

Second, the Russian military intelligence agency, known by its Russian acronym as the GRU, allegedly used coordinated hacking to target more than 500 people and institutions in the U.S. The Russian hackers downloaded potentially damaging information and released it to the public via WikiLeaks and under various aliases including “DCLeaks” and “Guccifer 2.0.”²⁴

The PSYOP involved extensive posting of professional-grade illustrations to support well-written postings in social-media accounts created using pseudonyms and pretending to be from U.S. residents along with regular blogs that attracted thousands of followers. The article cited above pointed out that:

These trolls were instructed to stir up racial tensions, stage “flash mobs²⁵” and organize activist campaigns – sometimes announcing events for opposing groups at the same times and locations.

A report submitted to the *U.S. Senate Intelligence Committee* in 2018 delved into the details of the Russian PSYOP and found that:

“What is clear is that all of the messaging clearly sought to benefit the Republican Party — and specifically Donald Trump,” the report says. “Trump is mentioned most in campaigns targeting conservatives and right-wing voters, where the messaging encouraged these groups to support his campaign. The main groups that could challenge Trump were then provided messaging that sought to confuse, distract and ultimately discourage members from voting.”

....

The Russians aimed particular energy at activating conservatives on issues such as gun rights and immigration, while sapping the political clout of left-leaning African American voters by undermining their faith in elections and spreading misleading information about how to vote. Many other groups — Latinos, Muslims, Christians, gay men and women, liberals, Southerners, veterans — got at least some attention from Russians operating thousands of social media accounts.²⁶

In the campaigns for the 2020 presidential election, the Russian *Internet Research Agency* (IRA) was found to be using Facebook and Twitter to spread disruptive conspiracy theories intended to cause further breakdown of U.S. society.²⁷

By May 2021, *Facebook* issued a report on DISINFO campaigns using its platform.

Facebook says it has uncovered disinformation campaigns in more than 50 countries since 2017, when it began the cat-and-mouse game of cracking down on political actors seeking to manipulate public debate on its platform. The report, which summarizes 150 disinformation operations the company says it has disrupted in that period, highlights how such coordinated efforts have become more sophisticated and costly to run in recent years — even as these operators struggle to influence large numbers of people as they once did.²⁸



FIGURE 15.6 Russian hacker.

Facebook reported that “it has uncovered disinformation campaigns in more than 50 countries since 2017.” In addition, the DISINFO/PSYOP campaigns have become more complex, with operatives blending into local journalism and political activism, particularly to support fascists in the United States and elsewhere.

JOINT CHIEFS: U.S. BEHIND ON INFOWAR CAPABILITIES

In November 2021, Lt. Gen. Dennis Crall, the Joint Staff’s CIO, discussed U.S. cyberwarfare capabilities at a conference for *Special Operations and Low Intensity Conflict*. A report described his presentation as follows:

The U.S. needs a better strategy and more advanced tools for information operations, Lt. Gen. Dennis Crall, the Joint Staff’s chief information officer, said Thursday.

The government has become slower and less confident in its approach, a reticence it can’t afford as artificial intelligence drastically increases the pace of messaging and information campaigns, said Crall, who is also the Joint Staff’s director for command, control, communications, computers, and cyber.

“The speed at which machines and AI won some of these information campaigns changes the game drastically for us. If we study, if we’re hesitant, if we don’t have good left and right lateral limits, if every operation requires a new set of permissions...We’re never going to compete.”

....

Currently, the U.S. government lacks a central organizer for influence campaigns. The State Department has a Global Engagement Center that can identify and respond to things like extremist messaging on social media, disinformation campaigns, etc., and can award grants to private and non-governmental organizations as well as academics, but it’s not positioned to engage with global audiences on broad topics like the desirability of democracy or authoritarian rule.

“I would look at irregular warfare, whether it be messaging or really any kind of warfare in the future, the speed game of...digital transformation, predictive analytics, machine learning, artificial intelligence, they are changing the game...and if we don’t match that speed, we will make it to the right answer and that the right answer will be completely irrelevant,” Crall said.²⁹

INDUSTRIAL ESPIONAGE

The U.S. *National Counterintelligence Center* (NACIC) which later became the *Office of the National Counterintelligence Executive* (ONCIX) reported annually to Congress from 1995 to 2008 about foreign economic collection and industrial espionage.³⁰

First of all,

Section 809 of the *Intelligence Authorization Act for Fiscal Year 1995* defined foreign industrial espionage as “industrial espionage conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private U.S. company and aimed at obtaining commercial secrets.”³¹

Throughout the period of reporting, there was little change in the list of targeted technologies; the 2004 report lists the following:

Information systems are a key target, with more than 40% of the PhDs employed in the field in 2001 (the most recent year of available data)



FIGURE 15.7 U.S. lagging in INFOWAR.



FIGURE 15.8 Spies among us.

being foreign-born (compared with 10% of all PhD scientists and engineers overall in the USA). Sensors, aeronautics, electronics, armaments and energetic materials are other industrial targets for espionage.

The 1996 report notably added biotechnology, information warfare, manufacturing processes, nuclear systems, space systems, telecommunications and weapons effects and countermeasures to the list of targets.

According to these reports, industrial espionage is carried out in many ways:

Traditional methods of espionage include classic agent recruitment, U.S. volunteers, surveillance, surreptitious entry (including bribery at hotels to allow access to guest and luggage rooms), specialized technical operations such as *communications intelligence* and *signals intelligence* (COMINT and SIGINT).

Additional methods include:

- Using foreign students studying in the United States,
- Foreign employees of U.S. firms and agencies,
- Debriefing foreign visitors to the United States on their return to their home country,
- Recruitment of immigrants,
- Ethnic targeting (suborning or threatening Americans with foreign family ties), and
- Elicitation during international conferences and trade fairs.

Agents have also exploited private-sector firms, joint ventures, mergers or acquisitions, and non-profit organizations as opportunities and fronts for espionage. Hiring competitors' employees, signing corporate technology agreements, sponsoring research projects in the United States and assigning foreign liaison officers to government-to-government research and development projects are additional valuable methods for covert data gathering.

Open-source intelligence (OSINT) methods include open or covert use of public DBs, hiring information brokers and assigning consultants to gather information for confidential research reports. In some cases, foreign interests have paid lobbyists to influence lawmakers and to facilitate extended contacts with high-placed officials with access to valuable information. Other OSINT channels listed in the 1996 report include bid proposals, energy policies, marketing plans, price structuring, proposed legislation, tax and monetary policies, and control regulations for technology transfer and munitions.

COINTEL PERSPECTIVE

A reader with a COINTEL background who wished to remain anonymous contributed the following comments for my *Network World Security Strategies* column in November 2010. The first-person pronoun refers to him.

Industrial and economic espionage are not the same in U.S. government parlance. Federal agencies define *industrial* espionage as economic espionage carried out by or for foreign intelligence service (FIS) personnel. If the economic espionage is carried out by non-state FIS personnel it is defined as corporate *economic* espionage. The statistics for each are recorded and correlated separately. Sometimes congressional or civilian agencies will issue deceptive reports where the economic espionage is listed as industrial espionage. Factually the figures are all for economic espionage but the figures for industrial espionage are usually classified because of the involvement of a FIS. The FBI treats both industrial and economic espionage the same, as criminal acts. Therefore gross under-reporting of all types of economic espionage is the norm.

In the national security organizations (e.g., DoD and CIA, but not the FBI), we do not care about criminal acts, we care about poaching on our turf and threats to national security. So involvement of



FIGURE 15.9
Counterintelligence.

a FIS in any manner will bring in national assets for counter-intelligence. Unfortunately, those assets and people were nearly wiped out (70% downsized) in President Clinton's administrations and it takes five to ten years to reconstruct those units by training new personnel to meet adequate levels of skill and experience.

From 1993 to 2005, four nations have dramatically increased their economic and industrial espionage against the USA: the People's Republic of China, Russia, France and Israel (ranked in order of magnitude by the number of agents and the number of incidents). Israel and France are by far the more brazen, audacious and successful, especially given their smaller pools of manpower.

Here's an example of brazen: Back in 1992 at the Paris Airshow the Russians for the very first time brought out for show their frontline Mig-29's and Su-28 fighter jets along with advanced air-to-air missiles (AA-10 Archer and Alamo). Both Russian aircraft manufacturers were there for foreign sales opportunities. The AA-10 (also known as the Russian AAMRAMski) had unique forward swept, trapezoidal, waffle patterned maneuvering fins. U.S. military groups were extremely interested in these missiles and their capabilities. The DoD (five different groups) and other civilian agency teams (all with technical Russian language speakers) were all there with expensive still and video cameras.

We asked the Russians to give us a show and tell; and they did. Wow! Up-close and even in the cockpits. We were ecstatic and content.

Just after we had left the secured Russian area (the roped-off area to keep the crowds 100 feet away from the aircraft for security), we videotaped three dispersed French INTEL groups approaching the Russian rope line through the crowd. One was composed of scantily clad and well endowed French ladies who proceeded to provocatively distract the young lonely armed Russian guards and older male flight officers. The other two groups jumped the rope line, and proceeded to physically tear one of the fins off the AA-10 missile still attached to the SU-28 wing pylon. Before the Russians could stop them they scattered and ran off through the crowd with their prize, one AA-10 missile fin.

We (USA) would never have done this. Too rude, crude and gauche. Besides we had gotten enough photographs with scales in the view to go build our own fins and wind tunnel test them.

The Russians protested and the French authorities denied all involvement.

Today several French missiles for sale have similar waffle patterned fins.

CHINA

The immense growth and development of the Chinese economy has been accompanied by a rising tide of industrial espionage and criminal hacking originating from the People's Republic of China (PRC). The *Annual Report to Congress on the Military Power of the People's Republic of China* from the U.S. Department of Defense has been issued every year since 2002. The description of the reports is as follows:

Section 1202 of the National Defense Authorization Act for Fiscal Year 2000, Public Law 106-65, as amended, provides that the Secretary of Defense shall submit a report "in both classified and unclassified form, on military and security developments involving the People's Republic of China. The report shall address the current and probable future course of military-technological development of the People's Liberation Army and the tenets and probable development of Chinese security strategy and military strategy, and of the military organizations and operational concepts supporting such development over the next 20 years. The report shall also address U.S.-China engagement and cooperation on security matters during the period covered by the report, including through U.S.-China military-to-military contacts, and the U.S. strategy for such engagement and cooperation in the future."³²

中国经济的巨大增长和发展伴随着来自中华人民共和国的工业间谍活动和黑客犯罪浪潮的兴起。

FIGURE 15.10
Chinese INFOWAR.

The 2021 report includes a description on page 64 about the *People's Liberation Army* (PLA) *Strategic Support Force* (SSF) and its information-warfare responsibilities:

- The PLA Strategic Support Force (SSF) is a theater command-level organization established to centralize the PLA's strategic space, cyber, electronic, information, communications, and psychological warfare missions and capabilities.
- The SSF's Network Systems Department is responsible for information warfare with a mission set that includes cyberwarfare, technical reconnaissance, electronic warfare, and psychological warfare.

....

As part of its efforts to restructure the PLA for modern warfare, the CMC [*Central Military Commission*] established the PLA SSF in 2015 to centralize the PLA's strategic space, cyber, electronic, and psychological warfare missions and capabilities. The SSF's creation highlights the PRC's understanding of the information domain as a strategic resource in modern warfare. Among the impetuses for the SSF's establishment was the PLA's apparent concern about the disparity between its cyber capabilities and those of the U.S., and the view of China's leaders that achieving information dominance and denying adversaries the use of the electromagnetic spectrum is necessary to seize and maintain the strategic initiative in a conflict. The SSF reports directly to the CMC and supports the entire PLA with its capabilities. The PRC's 2019 defense white paper described the SSF's modernization goals as "seeking to achieve big development strides in key areas and accelerate the integrated development of new-type combat forces, so as to build a strong and modernized strategic support force."

A striking report about Chinese-sponsored industrial espionage surfaced in 2005 when *TIME Magazine* published an interesting report by Nathan Thornburgh about an investigation code-named TITAN RAIN that began in late 2003.³³ As an ISSO for *Sandia National Laboratories* of the U.S. DoE, Shawn Carpenter noticed a flood of expert hacker activity focusing on data theft from a wide range of "the country's most sensitive military bases, defense contractors and aerospace companies." Carpenter discovered that "the attacks emanated from just three Chinese routers that acted as the first connection point from a local network to the Internet." Carpenter worked with U.S. Army and FBI investigators to learn more about the attacks and the attackers. According to Thornburgh, various analysts judge that "Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced." Thornburgh pointed out that systematic vulnerability scans by the Chinese IW specialists were massive in scope:

They hit hundreds of computers that night and morning alone, and a brief list of scanned systems gives an indication of the breadth of the attacks. At 10:23 p.m. pacific standard time (PST), they found vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona. At 1:19 am PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia. At 3:25 am, they hit the Naval Ocean Systems Center, a defense department installation in San Diego, California. At 4:46 am PST, they struck the U.S. Army Space and Strategic Defense installation in Huntsville, Alabama. As with prior attacks, the targeted networks were unclassified systems; the military's classified networks are not connected directly to the Internet. But even unclassified systems store sensitive information and provide logistics support throughout the armed forces. Government analysts say the attacks are ongoing, and increasing in frequency. But whether the Titan Rain hackers are gathering industrial information or simply testing their ability to infiltrate a rival nation's military systems, the U.S. government is taking the threat very seriously.

So was Carpenter treated as a hero by Sandia managers?

Well, no. He was fired for inappropriate and unauthorized use of DoE computer resources and information. However, he then "spent five months of his own time secretly tracking the Chinese cyberespionage ring Titan Rain and giving information about them to Army intelligence and the

FBI.”³⁴ In 2007, he won his lawsuit against Sandia National Laboratories for wrongful dismissal and was awarded \$4.7 million in damages.³⁵

BLOCKING IP TRAFFIC FROM SPECIFIC NATIONS

Scott Granneman wrote a thoughtful and stimulating commentary about Chinese hacker attacks in *The Register* in 2005.³⁶ He also mentioned the *Titan Rain* case, but he focused first on the experience of some personal friends of his who run Web-hosting services.

They both independently discovered that their systems were being swamped by a flood of peculiar requests originating in a wide range of sites in the PRC. He wrote,

Both of my friends thought about their situations, and both came to the same conclusion: block the entire IP ranges! Use WHOIS to look up the IP address’ range, then block ‘em with the server’s firewall. This quickly grew into a mammoth, seemingly neverending task, but it immediately began to pay off. Fishy Web server requests tapered off greatly, and while there are still a few every day, it’s now become a manageable problem. If things keep up at the same pace, sometime in the next few months they’re going to have blocked every IP in China.

Granneman asked whether his friends had told their clients about their new policy of blocking all packets originating in the .CN domain; they said no.

Granneman, to his credit, raised two ethical questions:

1. Should his friends have told the clients about the global block on Chinese access to their websites?
2. Is there something wrong with blocking all access to a website for all users in a national domain?

For the first question, I think that simple ethical rules dictate that his friends should indeed have informed their clients of the new policy. One rule in ethical decision making is to consider all the stakeholders affected by a decision, and their clients are potentially affected. Another is that openness characterizes appropriate actions; a desire for secrecy always raises questions about whether a course of action is ethical (it doesn’t mean that all secrecy is bad, just that it raises questions that should be answered).

However, for the second, I cannot conceive of how anyone could reasonably argue that the owners of a private website have any limits whatsoever on how they restrict access to their information. The Web is a method for voluntarily sharing documents (and now, much more) using standard protocols (http, html, and so on). Nothing in the technology removes the absolute right of the data owner to control how that information is shared. For example, if a copyright holder chooses to restrict access to published documents by requiring registration, that’s fine. If they require access controls using a userID and a password, that’s fine. If they require users to buy smart cards and log in using one-time passwords, that’s a real pain but it’s also fine. If they require users to have biometric equipment for retinal scans, brain-wave measurements and a signature in blood giving away rights to the user’s house, that may be crazy but it’s also perfectly legal provided (U.S.) laws on public accommodation³⁷ don’t kick in. The worse the restrictions, the fewer the users, but *no one* has an absolute, unlimited right to access *any* document on a privately owned site on the Web.

So if a private Web-site owner wants to block all packets originating from the PRC, there is absolutely nothing morally or legally wrong with such a decision.

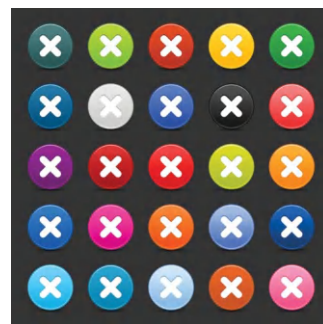


FIGURE 15.11 Filtering traffic selectively.

Personally, I have blocked all email with country domains from which large amounts of spam originate; if someone in those countries wants to communicate with me, they can write me a letter. Illegal? No. Immoral? No. Unethical? No.

MY email. MY website. Don't bother me if I don't like you, your ISP or your country!

RESPONDING TO CHINESE INDUSTRIAL SPAM

When I have time to spare, I respond to Chinese spam from industrial companies that I find in my trash folder with the following macro message translated into Chinese (note that I take advantage of cultural values by emphasizing that the senders are embarrassing themselves and their country):



FIGURE 15.12 Making fun of spammers.

I'm sorry to inform you that you have been the victim of criminal fraud.

The unsolicited commercial email (UCE or "spam") that someone sent out on your company's behalf was NOT sent to the selected addresses that they claimed they would use. For example, your spam mentions industrial goods but was sent to randomly collected addresses, including mine – and I am a retired university professor specializing in operations management and information security and can have absolutely no value to you as a customer. In addition, if you are sending offers of industrial goods to my .EDU address, you should know that all .EDU addresses are for educational institutions, and thus completely useless to you.

You have been cheated and made to look like idiots.

I strongly recommend that you demand full details of the email distribution list that the criminals who defrauded your company used in their fraudulent scheme. They took your money under false pretenses.

Given that you live in the People's Republic of China, where there is no effective rule of law, I recommend that you deal with the criminals personally. Stuffing several hundred paper copies of their fraudulent email – email that disgraces you and your company before the world – up their noses or other body orifices would be a highly appropriate punishment. You can also just illegally beat them severely, as that is a common technique used by your own police forces on anyone disliked by people in power. If they complain to the police, you can always bribe an officer or two to look the other way or to beat them some more.

It would also be nice if you could spread the word to your colleagues in business in China so that fewer of you could make total fools of yourselves in the eyes of millions of unwilling recipients of your useless, pointless, stupid junk mail.

I sincerely wish you every success in stopping these criminals from further embarrassment and humiliation before your entire family, community and nation.

Don't bother responding: your email address is blocked. In fact, ALL email from .cn addresses goes straight to the trash folder.

BLOCKING PORN

In mid-2023, I started receiving pornographic spam from HOTMAIL addresses. I dutifully reported every one of hundreds of messages that included mostly pictures of women's breasts (!?! coupled with invitations to become friends because... wait for it ... the "senders" found me interesting <LOL>. After a few weeks I checked my address list, found no one with HOTMAIL addresses and simply blocked *all* email from *any* HOTMAIL address. Some months later (it took that long), the porn flood from HOTMAIL slowed significantly. Whew!

NOTES

- 1 Schwartau, Information Warfare: Chaos on the Electronic Superhighway (1994).
- 2 ACM Committee on Computers and Public Policy (2021).
- 3 WIRED (2021).
- 4 British Broadcasting Corporation (2021).
- 5 CNN Business (2021).
- 6 TheHackerNews (2021).
- 7 U.S. Internet Crime Complaint Center IC3 (2021).
- 8 Beal (2014).
- 9 U.S. Federal Trade Commission (2021).
- 10 So and Szep (2021).
- 11 Steger (2019).
- 12 Modic and Anderson (2015).
- 13 U.S. Federal Bureau of Investigation.
- 14 U.S. Federal Trade Commission (2021).
- 15 U.S. Federal Trade Commission (2021).
- 16 Takahashi (2011).
- 17 Otten (2023).
- 18 Christos (2020).
- 19 Sussman (2020).
- 20 U.S. Cybersecurity & Infrastructure Security Agency (2023).
- 21 Assante (2009).
- 22 Kabay, Weekly Resources | DISINFO (2021).
- 23 Molander, Riddile, and Wilson (1996).
- 24 Summers (2018).
- 25 National Center for Families Learning (2021).
- 26 Timberg and Romm (2018).
- 27 Frenkel and Barnes (2020).
- 28 Dwoskin (2021).
- 29 Tucker (2021).
- 30 U.S. National Counterintelligence Executive (2011).
- 31 U. S. National Counterintelligence Center (1995).
- 32 U.S. Department of Defense (2021).
- 33 Thornburgh, The Invasion of the Chinese Cyberspies: An exclusive look at how the hackers called TITAN RAIN are stealing U.S. secrets (2005).
- 34 Thornburgh, The Invasion of the Chinese Cyberspies: An exclusive look at how the hackers called TITAN RAIN are stealing U.S. secrets (2005).
- 35 Thornburgh, A Security Analyst Wins Big in Court (2007).
- 36 Granneman (2005).
- 37 FindLaw (2018).

WORKS CITED

- ACM Committee on Computers and Public Policy. (2021, November 6). *The Risks Digest* (P. G. Neumann, Ed.). Retrieved November 12, 2021, from RISKS: <https://catless.ncl.ac.uk/risks/>
- Assante, N. J. (2009, January 5). *Infrastructure Protection in the Ancient World*. Retrieved November 15, 2021, from Proceedings of the 42nd Hawaii International Conference on System Sciences: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.401.7316>
- Beal, A. (2014, December 12). *How to Handle a Defamatory Attack to Your Online Reputation*. Retrieved November 12, 2021, from Andy Beal: <https://www.andybeal.com/how-to-handle-a-defamatory-attack-to-your-online-reputation/>
- British Broadcasting Corporation. (2021, October 18). *Computer Hacking*. Retrieved November 12, 2021, from BBC NEWS | Topics | Computer hacking: <https://www.bbc.com/news/topics/c347w30eq7xt/computer-hacking>
- Christos, K. R. (2020, December 5). *Big Business Hired Hackers to Destroy Competition: Is Your SMB At Risk?* Retrieved November 15, 2021, from LinkedIn: https://www.linkedin.com/pulse/big-business-hired-hackers-destroy-competition-your-smb-kim-christos?trk=public_profile_article_view

- CNN Business. (2021, November 11). *HACKING*. Retrieved November 12, 2021, from CNN | Specials | Tech: <https://www.cnn.com/specials/tech/hacking>
- Dwoskin, E. (2021, May 26). *Russia Is Still the Biggest Player in Disinformation, Facebook Says*. Retrieved November 16, 2021, from The Washington Post | Technology: <https://www.washingtonpost.com/technology/2021/05/26/facebook-disinformation-russia-report/>
- FindLaw. (2018, April 23). *Public Accommodations and Equal Rights*. Retrieved November 15, 2021, from FindLaw | Learn About the Law | Civil Rights | Civil Rights Overview: <https://www.findlaw.com/civilrights/civil-rights-overview/public-accommodations-equal-rights.html>
- Frenkel, S., & Barnes, J. E. (2020, September 1). *Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say*. Retrieved November 16, 2021, from The New York Times: <https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html>
- Granneman, S. (2005, August 31). *On Blocking Chinese IP Addresses: The Great Firewall of China*. Retrieved November 15, 2021, from The Register: https://www.theregister.com/2005/08/31/blocking_chinese_ip_addresses/
- Kabay, M. E. (2021, February 5). *Weekly Resources | DISINFO*. Retrieved November 16, 2021, from M. E. Kabay | Courses | Politics of Cyberspace: http://www.mekabay.com/courses/academic/norwich/cs407/cs407_resources/cs407_links_files/sheet015.htm#RANGE!A1
- Modic, D., & Anderson, R. (2015, September). It's all over but the crying: the emotional and financial impact of internet fraud. *IEEE Security & Privacy*, 13, 99–103. <https://doi.org/10.1109/MSP.2015.107>
- Molander, R. C., Riddile, A., & Wilson, P. A. (1996, March 29). *Strategic Information Warfare: A New Face of War*. <https://doi.org/10.7249/MR661>
- National Center for Families Learning. (2021). *What Is a Flash Mob?* Retrieved December 19, 2021, from Wonderopolis: <https://wonderopolis.org/wonder/what-is-a-flash-mob>
- Otten, T. (2023, August 17). “We Will Kill You”: Trump Supporters Threaten Judge, Jurors Amid Indictments. Retrieved September 24, 2023, from The New Republic: <https://newrepublic.com/post/175032/trump-supporters-threaten-judge-jurors-amid-indictments>
- Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway* (Vol. 1). Independently Published. Retrieved November 11, 2021, from <https://smile.amazon.com/Information-Warfare-Chaos-Superhighway/dp/B08QRYXNWR>
- So, L., & Szep, J. (2021, November 9). *Reuters Unmasks Trump Supporters Who Terrified U.S. Election Officials*. Retrieved November 12, 2021, from Reuters | Campaign of Fear: <https://www.reuters.com/investigates/special-report/usa-election-threats/>
- Steger, A. (2019, October 30). *What Happens to Stolen Healthcare Data?* Retrieved November 12, 2021, from HealthTech | Security: <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>
- Summers, T. (2018, July 27). *How the Russian Government Used Disinformation and Cyber Warfare in 2016 Election - An Ethical Hacker Explains*. Retrieved November 16, 2021, from The Conversation: <https://theconversation.com/how-the-russian-government-used-disinformation-and-cyber-warfare-in-2016-election-an-ethical-hacker-explains-99989>
- Sussman, B. (2020, May 28). *Company Hires Hacker for Corporate Espionage*. Retrieved November 15, 2021, from SecureWorld: <https://www.secureworld.io/industry-news/company-hires-a-hacker-for-corporate-espionage>
- Takahashi, D. (2011, October 21). *The “World’s Most Wanted Hacker,” Kevin Mitnick, Has Gone Straight (Interview)*. Retrieved November 12, 2021, from VentureBeat: <https://venturebeat.com/2011/10/21/interview-with-the-former-worlds-most-wanted-hacker-kevin-mitnick/2/>
- TheHackerNews. (2021, November 12). *Home*. Retrieved February 28, 2024 from TheHackerNews: <https://thehackernews.com/>
- Thornburgh, N. (2005, August 25). *The Invasion of the Chinese Cyberspies: An Exclusive Look at How the Hackers Called TITAN RAIN Are Stealing U.S. Secrets*. Retrieved November 15, 2021, from TIME Magazine: <http://content.time.com/time/nation/article/0,8599,1098371,00.html>
- Thornburgh, N. (2005, August 29). *The Invasion of the Chinese Cyberspies: An Exclusive Look at How the Hackers Called TITAN RAIN Are Stealing U.S. Secrets*. Retrieved November 15, 2021, from TIME Magazine: <http://content.time.com/time/subscriber/article/0,33009,1098961,00.html>
- Thornburgh, N. (2007, February 14). *A Security Analyst Wins Big in Court*. Retrieved November 15, 2021, from TIME Magazine: <http://content.time.com/time/nation/article/0,8599,1589735,00.html>
- Timberg, C., & Romm, T. (2018, December 17). *New Report on Russian Disinformation, Prepared for the Senate, Shows the Operation’s Scale and Sweep*. Retrieved November 16, 2021, from Washington Post: <https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/>

- Tucker, P. (2021, November 14). *Joint Chiefs' Information Officer: US Is Behind on Information Warfare, AI Can Help*. Retrieved November 16, 2021, from American Military News: <https://americanmilitarynews.com/2021/11/joint-chiefs-information-officer-us-is-behind-on-information-warfare-ai-can-help/>
- U. S. National Counterintelligence Center. (1995). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1995*. Retrieved November 15, 2021, from Homeland Security Digital Library: <https://www.hsdl.org/?abstract&did=463217>
- U.S. Cybersecurity & Infrastructure Security Agency. (2023). *Stop Ransomware*. Retrieved September 24, 2023, from CISA: <https://www.cisa.gov/stopransomware>
- U.S. Department of Defense. (2021, November 3). *Military and Security Developments Involving the People's Republic of China 2021*. Retrieved November 15, 2021, from U.S. DoD Search | China: <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>
- U.S. Federal Bureau of Investigation. *Advance Fee Schemes*. Retrieved November 12, 2021, from FBI | Scams and Safety: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/advance-fee-schemes>
- U.S. Federal Trade Commission. (2021, May). *Gift Card Scams*. Retrieved December 19, 2021, from FTC | Consumer Information: <https://www.consumer.ftc.gov/articles/gift-card-scams>
- U.S. Federal Trade Commission. (2021, May). *Refund and Recovery Scams*. Retrieved November 12, 2021, from FTC | Money & Credit | Resolving Consumer Problems: <https://www.consumer.ftc.gov/articles/refund-and-recovery-scams>
- U.S. Federal Trade Commission. (2021, Mar). *What to Know About Identity Theft*. Retrieved November 12, 2021, from FTC | Privacy, Identify & Online Security | Identity Theft: <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft>
- U.S. Internet Crime Complaint Center IC3. (2021, November 4). *News Releases | Frequently Asked Questions | Annual Report*. Retrieved March 1, 2024 from [ic3.gov](https://www.ic3.gov/): <https://www.ic3.gov/>
- U.S. National Counterintelligence Executive. (2011, November 3). *Annual Reports to Congress on Foreign Economic Collection and Industrial Espionage*. Retrieved November 15, 2021, from Homeland Security Digital Library: <https://www.hsdl.org/?lists&id=1980>
- WIRED. (2021, November 12). *Hacked*. Retrieved November 12, 2021, from WIRED | Search: "hacked": <https://www.wired.com/search/?q=hacked&page=1&sort=score>

16 Cyberlaw Issues

In my experience, relatively few information-security practitioners have a grasp of the legal environment in which they work. Exceptions include *Certified Information System Security Professionals* (CISSPs), who must demonstrate and maintain their knowledge of laws pertaining to computer crime, privacy, and other information-security matters. This section reviews some critical aspects of the most important laws governing cyberspace crime in the United States and includes a brief summary of European privacy laws.

As always, it's legally important to state clearly that I am not a lawyer, and this is not legal advice. For legal advice, consult an attorney licensed to practice in your jurisdiction and qualified in the specific area of the law concerned.

This chapter reviews

- Basic cyberlaws in the United States and the European Union
- Employee privacy rights
- Defamation
- Intellectual property
- Spam
- Vulnerability exposure
- Virus-writing in academic courses



FIGURE 16.1 Laws matter for INFOSEC.

CYBERLAW STATUTES IN THE UNITED STATES

The earliest laws criminalizing particular unlawful behavior involving computers and networks were legislated in the United States. The *Computer Fraud and Abuse Act of 1986* (18 USC §1030(a)) specifically protects “government-interest” computers, including federal, state, county and municipal systems; financial and medical institutions; and computers used by contractors supplying such institutions. However, it also includes *any* unauthorized access to any computer that uses any security measures.

The Act prohibits the use of “a program, information, code or command” with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.¹

Another law governing interstate electronic communications has been used in prosecutions of computer crimes: 18 USC §1343, dealing with *wire fraud*. Wire fraud requires the following elements:

- A scheme to defraud by means of false pretenses.
- Knowing and willful participation with intent to defraud.
- The use of interstate wire communications in furtherance of the scheme.²



FIGURE 16.2 Learn about applicable statutes.

The *Electronic Communications Privacy Act of 1986* (18 USC §1367 and others), generally known as the ECPA, assigns fines and prison sentences for anyone convicted of unauthorized interception and disclosure of electronic communications such as phone calls through land lines or mobile systems and email.³ In addition, the ECPA specifically prohibits making use of an unlawfully overheard electronic communication if the interceptor knows that the message was unlawfully obtained. On the other hand, *providers* of electronic messaging systems, including employers, are permitted to intercept messages on their *own* systems in the course of their normal operations; naturally, they are authorized to transmit messages to other communications providers as part of the normal course of transmission to the ultimate recipient. The ECPA also prohibits access to stored messages, not just those in transit. *U.S. Code* Chapter 41 also criminalizes the use of interstate communications for

- § 871. Threats against President and successors to the Presidency
- § 872. Extortion by officers or employees of the U.S.
- § 873. Blackmail
- § 874. Kickbacks from public works employees
- § 875. Interstate communications
- § 876. Mailing threatening communications
- § 877. Mailing threatening communications from foreign country
- § 878. Threats and extortion against foreign officials, official guests, or internationally protected persons
- § 879. Threats against former Presidents and certain other persons
- § 880. Receiving the proceeds of extortion⁴

Another form of prohibited speech is everything associated with child pornography: making, sending, publishing, or storing images of children engaged in sexually explicit conduct (18 USC §2251-2252) or trickery to fool victims into accessing pornography on the Web:

- § 2251. Sexual exploitation of children
- § 2251A. Selling or buying of children
- § 2252. Certain activities relating to material involving the sexual exploitation of minors
- § 2252A. Certain activities relating to material constituting or containing child pornography
- § 2252B. Misleading domain names on the Internet
- § 2252C. Misleading words or digital images on the Internet⁵

The *Communications Decency Act of 1996* (47 USC §223) or CDA was a highly controversial statute prohibiting anyone using interstate or communications from transmitting obscene or indecent materials when they know that the recipient is under 18 years of age – regardless of who initiated the communications. In June 1997, in a stinging rebuke to proponents of censorship, the U.S. Supreme Court issued its ruling on the CDA, finding that it violated First Amendment protection of free speech. The unanimous opinion stated that the effort to protect children from sexually explicit material went too far because it also would keep such material from adults who have a right to see it.⁶

In addition to federal laws, the United States has a tapestry of state laws applying to computer crimes. States differ widely in the availability of computer-crime laws and in their definitions and penalties. State laws address:

- Unauthorized access
- Computer trespass
- Hacking
- Viruses
- Spyware

- Ransomware
- Other malware
- Denial-of-service attacks
- Other forms of computer extortion
- Phishing⁷

EUROPEAN GDPR

The members of the European Union agreed on sweeping regulations protecting privacy of residents:

In 2016, the EU adopted the *GDPR*,⁸ one of its greatest achievements in recent years. It replaces the 1995 *Data Protection Directive* which was adopted at a time when the internet was in its infancy.⁹

The law was fully implemented by May 2018.

The 99 *Articles* in 11 *Chapters* are breathtaking in the completeness of coverage of privacy issues. Some of the key *Articles* are:

- 9 Processing of special categories of personal data
- 10 Processing of personal data relating to criminal convictions and offences
- 12 Transparent information, communication, and modalities for the exercise of the rights of the data subject
- 13 Information to be provided where personal data are collected from the data subject
- 16 Right to rectification
- 17 Right to erasure (“right to be forgotten”)
- 25 Data protection by design and by default
- 30 Records of processing activities
- 32 Security of processing
- 33 Notification of a personal data breach to the supervisory authority
- 34 Communication of a personal data breach to the data subject
- 37 Designation of the data protection officer

It’s important for organizations doing business in the European Union *even if they are not based there* to understand that these laws apply even to non-resident organizations.¹⁰

WORLD WILD WEB

Cyberspace crime poses a jurisdictional problem because the perpetrator of a crime can reside in one country, act through computers and networks in several other countries, and cause harm to computer systems in yet other countries. Trying to investigate and prosecute crimes that are carried out in milliseconds when international cooperation can take days and weeks means that many computer crimes simply go unpunished.

The most irritating aspect of computer-crime investigations and prosecutions is the jurisdictional quagmire resulting from incomplete and inconsistent laws. In international



FIGURE 16.3 Europe catches up.



FIGURE 16.4 The Web has problems.

law, no one may legally be extradited from one country to face prosecution in another country unless both countries involved have *dual criminality*. That is, an offense must be similar in law and at the same level of criminality (misdemeanor, felony) before extradition can be considered by courts of law. Unfortunately, the paucity of laws even recognizing the existence of computer crimes interferes with capture, extradition and prosecution of criminals who live in one jurisdiction, use computers and networks in other jurisdictions, and harm victims all over the world.

A good example of the frustration felt by law enforcement officials and victims of computer crime occurred in the year 2000, when a world-wide infestation by the email-enabled worm *Love Bug* caused damage and lost productivity estimated in the hundreds of millions of dollars. The malware was sent using an email message with the subject line “Kindly check the attached love letter coming from me” and upon reading the message, victims infected their system and sent copies of the infected message to everyone on the victims’ email contact lists.

Panic ensued: Systems in banks and factories were infected. In the UK, Parliament shut down its email network for several hours to prevent infection. Even the Pentagon was reportedly affected.¹¹

The putative originator of the worm was a computer programming student in Manila, The Philippines. Even though the alleged perpetrator came close to admitting his responsibility for the infection – and was lionized by the local press – there were no applicable laws in The Philippines under which he could be prosecuted locally. As a result, he was never extradited to the United States for prosecution.¹²

A similar case occurred in 1996, when Julio Cesar Arditia was accused of unauthorized penetration of U.S. military and university systems. The 23-year-old Argentinian citizen could not be charged in his homeland for lack of cybercrime statutes there. Interestingly, he voluntarily came to the United States in 1998 to face his accusers. Under a plea-bargain, he was sentenced in May 1998 to three years’ probation and a \$5,000 fine.

The current state of law enforcement for cyberspace crimes resembles the early days in the Wild West of the United States. Let’s hope that more countries can bring their legal systems into the 21st century.

OPPORTUNISTIC COMPUTER TRESPASS

A reader recently wrote to me with a practical question:

I’m at a cyber cafe and see an IBM rep log into the IBM site using GoToMyPC. I see the login and password. It was there for public display.

Is it legal for me to login to that site, and download a customer list, and use this information?

Has IBM, and this employee, left the door open for me and, in doing, made this information public?

As I understand the laws and jurisprudence in the United States (and with the clear disclaimer that I am not a lawyer and this is not legal advice), using a system login without authorization is a violation of law(s). The CFAA applies to federal-interest computers (essentially any computer used by or for federal, states, county, or municipal government departments and agencies OR any vendors supplying services to those entities).

Additionally, the ECPA has no limitations on its applicability. It applies not only to unauthorized interception of private communications such as email messages during transmission but also to stored versions of such documents.

Neither the CFAA nor the ECPA makes an exception for unauthorized access using a stolen (or borrowed, or inadvertently seen) user ID and password. It’s irrelevant how easy it is to break into



FIGURE 16.5 Do not enter!.

a system: contrary to the widely posted beliefs of criminal hackers and their supporters, exploiting obvious vulnerabilities to make unauthorized use of a restricted system does not exculpate the intruder.

The parallel in the real world is that if someone drops the metal key for entering a secured area of a business office or to enter the front door of a home, the finder of the key has no legal right to use it to enter the premises and then to eat pastries, steal radios, or snuffle through private information or any other property in the poorly secured area. Similarly, just because a computer network is poorly secured, no one has a legal right to penetrate it – regardless of how they do so – and to access confidential information or to tamper with corporate systems.

Some legal scholars have argued strongly that *unless* there are strong security measures for a computer system that at least attempt to block access (e.g., I&A systems and data-access controls) then anyone should be free to access the unprotected systems at will.¹³ There *have* been occasional discussions in the courts about whether a system visible on the Internet that does *not* have any kind of warning about being restricted can be penetrated inadvertently without criminal penalty; to avoid such ambiguity, security policies should include an explicit warning equivalent to the NO TRESPASSING sign on a field in the countryside. Such a sign makes it illegal to walk on the land, regardless of whether the perimeter is protected by barbed wire, automatic machine guns, or landmines.

I hope you will forgive me for adding a personal note about ethical standards here. When I returned from a plane trip to Washington decades ago, I was walking out to the parking area when I noticed a parking stub on the floor. Upon picking it up to throw it in the waste basket (I just don't like litter), I noticed that it was time-stamped for a few hours before I landed.

(Before I go further, I hope you won't interpret my example as insufferable self-righteousness – I'm just trying to make a point.)

So as I was saying, I threw the ticket away. Now, why didn't I use the ticket to get out of paying for a whole day of parking in the garage? After all, the security system of the garage was clearly inadequate: it did not authenticate the authorized user of a particular ticket (for instance, by printing an image of the license plate of the car used when getting the ticket at the dispenser). I just plain *don't like* the idea of cheating the parking garage out of their fee. The fact that I *could* do so is irrelevant: being *able* to cheat someone doesn't make it right.

LEGAL IMPLICATIONS OF QUALITY-ASSURANCE FAILURES

I had an interesting experience years ago. A well-known magazine (the name is not necessary for my purposes, and I like not being sued) had been sending me dunning letters claiming that a gift subscription I gave a friend recently was about to expire. Here's the text of the letter I sent to the CIO of the publishing company:

RE: Computer error generates possible interstate postal fraud

Dear <name concealed>:

I bought a gift subscription for a friend in June 2002 and paid for a three-year subscription.

I have been receiving dunning letters from your subscription service since August, two months after I bought the subscription. All of them insist that the subscription will end "soon."

The computer program that sends out warnings about expiration of gift subscriptions has a serious error – it doesn't consider the actual expiry date. This error is likely an oversight; i.e., quality assurance has failed. However, it is also possible that someone has deliberately programmed the system to ignore the termination date in an effort to frighten gift donors into sending renewal fees years earlier than required.

```

F0 FE 14 04 1C 70 04 A0 00 00 EF 00 70 04 B2 C0 00 00 05
FB C0 50 D0 F7 00 00 BB EF E0 F0 D1 00 AE B0 04 50 00 EE
E2 B6 04 F0 00 FF 01 A0 00 F2 EE 50 E0 04 NC 0F 03 1C F2
03 01 EE 70 A0 B6 A2 E0 B5 20 04 FD 03 A0 B2 01 C2 C1 E0
E4 03 A2 20 0F C9 C4 00 C0 C2 0A E0 C0 A5 EE F0 20 EF 05
E0 C0 00 EF 00 F0 05 04 30 F4 EF 14 00 FF 01 A0 01 00 0F
14 00 E0 F0 50 E0 AE 0A B2 FB C0 00 A0 B6 A2 0F EF E3 F0
5F A0 F2 EE 03 B2 F2 A5 EE E2 B6 04 0F C9 C4 B0 C0 F2 EE
04 0F 20 04 C2 C4 E0 F7 01 03 D1 EE BB 70 AE 00 00 20 04
EC BE C7 06 A0 EF 05 B6 A2 E4 05 A2 30 00 E5 03 C0 C2 50
F7 00 B2 01 C2 C5 04 0F 03 A0 70 A0 B6 A2 0A B6 A2 E0 BB
00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 06 10 A5 0C A3 EE F0 20 BB EF C0 00 05 EF 0A C0 C2 C2
0F C3 A7 F0 EF E0 B1 AC 00 20 F0 70 00 EE C1 F4 00 F0 F0
BB 00 C4 B6 00 F2 0A B2 FB 03 1C F2 A5 E3 EF 03 B2 FB FB
00 EF A2 20 0F EE 70 A0 04 C0 0A B2 01 EF EC C4 F2 A5 EE
E0 F0 F2 B7 03 A6 E0 B1 0A B2 C1 02 00 04 C0 05 E0 FF B1
FF 01 E3 E0 B6 A2 E4 00 A5 EC EF 0A E0 BC 00 E0 C5 B6 A2
B6 A2 02 05 0F 03 00 5F F0 B1 D2 C4 B0 C0 A2 A0 0F 03
C9 04 C0 B6 01 C2 0F 03 B6 A5 EF C9 04 00 C4 0F 02 01 C2
C0 C2 50 0B EE F0 20 EF 02 10 B0 20 0F F0 E2 03 0F EE F0
00 F0 FE 04 F0 A0 00 00 E3 FE 00 C2 00 E3 F1 0F B6 01 A0

```

FIGURE 16.6 Design and coding errors may cause legal problems.

The message “In fact, they’ll soon receive their last issue” was in a letter purportedly signed by <name removed>, President and Publisher; I enclose that letter for your reference.

Given that the subscription in question ends in June 2005, the statement is false.

Sending misrepresentations designed to induce recipients to send you more money may constitute fraud. Using interstate postal mail to perpetrate fraud may constitute a violation of U.S. Federal Mail Fraud statutes. I urge you to correct this error at once.

[I am not a lawyer and this is not legal advice. For legal advice, consult an attorney qualified to help you in this matter.]

What struck me about this relatively minor problem is that a computer-programming error may have legal repercussions when it affects marketing or any other communications with clients. In this case, what I hoped was the simple omission of an expiration-date check allowed the computer system to send wholly inappropriate warnings that could have been interpreted by naïve recipients as pressure to renew gift subscriptions that wouldn’t actually need renewal for a long time. There’s nothing wrong with suggesting early renewal; however, stating or even implying that without the renewal, the subscription will end in the immediate future is clearly out of line.

Similar concerns about being legally required to comply with the terms of out-of-date advertising led to the recommendation to put expiration dates on all advertising likely to be circulated via email, and Google implanted a feature for automatic expiration of messages back in 2018.¹⁴ Concerns over fraudulent tampering with the content of such freely circulating email ads leads to the recommendation to use digital signatures to be able to repudiate forged versions of the original advertisements.

In conclusion, to avoid embarrassment and possible legal entanglements, everyone with responsibility for automated processes should be especially careful to apply proper quality assurance to any automatically generated mass communication involving prices or services.

ETHICAL DEBATE OVER COMPUTER TRESPASS

I engaged in a vigorous debate with a reader of my security column about the ethical issues surrounding unauthorized access to systems. The following is an edited version of my response to a series of questions and arguments he put up for discussion. The correspondent’s questions are in quotes and my responses are indented in italics.

“If I see an ID and password and use this am I breaking in?”

Yes.

“What did I break?”

Ethical principles and the law. And “breaking in” is a metaphor, not a literal description of physical damage, so your question about what you broke is surely disingenuous – that is to say, sophistry.

“Who is to say that this was not meant to be a public login ID.”

You are, by applying your own good sense and experience of how people make mistakes by failing to protect their systems. You don’t seriously expect anyone to believe that you truly think that a user ID and password left visible on a screen in a cyber-café constitute a public access ID?

“It was given to me in public.”

No it wasn’t, any more than a person who leaves her purse on a table in that cyber-café is giving it to you when you steal it.



FIGURE 16.7

Let’s be clear.

“If, at a public website, the company accidentally left their customer names and addresses in a file that I can access. Clearly, it was not their intention to give me access to these files; or was it? Have I broken the law by taking and using this customer base?”

Yes, you have appropriated information to which you have no legal or moral right. That the information is stored electronically is no more relevant than if it had been written on paper or graven in stone.

“What did I “break” into in these examples?”

Their security perimeter; you also broke ethical principles and the law.

“The door was left open and it was inviting. By not having proper security, did the company not authorize me to have access?”

No, it didn't. Making a mistake does not constitute permission.

“I think that we can use physical examples only so far in the cyberspace.”

Cyberspace is a metaphor too. There is no special privilege accorded behavior solely on the basis of medium of communication. That you are using electronic methods for accessing the information is no more relevant to the ethical and legal issues than if you claimed that you could legally eavesdrop on a conversation solely because it was in, say, German. Do you believe that we could convince anyone that “Germanspace” and “Frenchspace” have different rules from “Englishspace” bearing on the inappropriateness of listening in on conversation between human beings? Why should we view responsibility, courtesy, consideration and kindness as irrelevant solely because of the use of, say, the Internet? Do you feel that slander is wrong when it's spoken face-to-face but OK when it's communicated through a telephone? What other technological tools absolve the user from normal rules of civility? Is a driver who makes rude gestures at you any less rude because he's doing it from inside an automobile than if he did it on the sidewalk as you were walking past each other?

“In my opinion, if I as a company am sloppy, then I am responsible.”

You mean, surely, irresponsible. And yes, you are certainly responsible for the consequences of your failures. Why does that responsibility then remove responsibility from the criminal who attacks your system using the vulnerabilities you have left in place? What is he, then, a robot? A mere automaton, devoid of personal responsibility for his actions? Sounds very much like the rationalizations of those defective people who abuse their spouses or their children and then blame the victim for “provoking” their abuse. “Look what you made me do,” cries the abuser after smashing the victim's face. “It's your fault for making me mad.” Such refusal to accept responsibility is pathological; why should we not apply the same standard to abuse of other people's bad computer and network security?

“If via my sloppiness, my information security is violated, how can I blame the person who found themselves with access? I gave them this access via my sloppiness.”

No you didn't give them access. You made it easier for dishonest people to abuse the information that you inadvertently made accessible. You are to blame for incompetence and they are to blame for taking advantage of it. Responsibility is not a zero-sum game where it's impossible for people to have different kinds of responsibility for a bad event. If a driver is not wearing a seat belt when another car smashes them off the road because that driver is drunk, do you think that the unbelted person's stupidity – he's definitely partly responsible for the severity of his head trauma – absolves the drunk from responsibility for the consequences of his actions?

“On which party is the onus?”

There's not just one burden of responsibility. Data owners or data managers have a fiduciary responsibility to their stakeholders to protect confidential and critical data. That they can fail does not absolve those who abuse their weakness.

“The person who was supposed to take reasonable steps to protect their information or the person who showed up via the WWW and got access?”

Try your reasoning on “The person who was supposed to take reasonable steps to protect their family or the person who showed up via the front door and shot the family?” Are you seriously proposing that vulnerability of the victim exculpates the attacker?

“Your orientation is a moral one. Yes, we are our brothers’ keeper and should do as you so indicated. However, the law is quite different. It does not deal with moral issues. Instead, it has its own basis.”

Oh, but the law does consider moral principles. For example, in contract law, contracts may be voided if the judicial system concludes that the terms are unconscionable. Penalties are limited to prevent cruel and unusual punishment. Judgements about indecency and obscenity are based on notions of reasonable people and community values. Constitutional law in the USA is governed by interpretation and by discussions about the intent of the framers in writing specific articles. Were the law a question of absolute, binary logic, we would already have established robotic law courts in which there were no human factors taken into account at all. The law is an expression of a society's moral reasoning. It's not a mathematically precise weighing of responsibility in which one party in a conflict necessarily takes all the blame and the other none.

“My feeling is that the person who sets up a system that is open has done just that; they have opened up their system. They did that. They should not have done that. It's then an open system that is public.”

Nonsense. There is no more justification for claiming that a computer system that is poorly protected is therefore open to the public than to claim that your own house is open to the public when you forget to lock the door. Ore even worse, to claim that because you failed to install titanium-steel bars on your windows, the punk who breaks into your home by smashing the pathetically weak glass is not responsible for his actions.

Do you seriously propose to exculpate swindlers who prey on gullible people because the victims ought to have known better?

What's your attitude toward drug dealers who give narcotics to schoolkids? Surely the kids ought to have been taught better self-protective skills, right? Therefore the drug dealers have done nothing wrong, yes? They merely exploited a weakness in others and therefore bear no responsibility for their own actions.

Let me finish by telling you that if you truly believe that victims deserve all the blame and their victimizers none – if you actually believe what you have been writing instead of simply taking a debating position for the fun of it – then we have nothing further to say to each other on this topic.

EMPLOYEE PRIVACY RIGHTS

PRIVACY AT WORK¹⁵

Years ago I received an invitation to sign a petition:

Think the federal government threatens your privacy? It could be worse – you could work for them.

Federal agencies are increasingly monitoring their own employees using software that tracks keystrokes, takes screenshots, and even records Facebook and



FIGURE 16.8

How much privacy at work?.

Twitter activity! This threatens employees' abilities to express political opinions and to work freely without fear of censure.

These constitutional abuses came to light when scientists at the FDA, blowing the whistle on unethical drug review practices, found they were being spied on and intimidated. Now it's clear that other government agencies, including the TSA, extensively monitor their employees, down to their personal emails!

How can we expect to live in a free, private society if even federal employees are systematically monitored? Join us in demanding [an] end to federal employee spying.

PETITION TO THE FDA AND TSA: We all deserve the right to privacy, as is guaranteed in the Constitution. We demand that federal agencies adopt constitutional privacy practices and disclose to their employees the extent of monitoring.

I was surprised at the naiveté of this petition.

In my classes on cyberlaw and IA management, we discuss the absolute right of employers to monitor, control or restrict the use of the employers' resources by employees. In the United States, the *First Amendment* of the *Constitution* is often misunderstood to grant absolute freedom of speech; however, it does not. There are several categories of speech that have been excluded from *First-Amendment* protection (e.g., sedition, incitement to violence, defamation, and obscenity) but in any case, that constitutional provision applies to *governmental* restriction of speech in the public sphere. There are many instances where employers – or even customers negotiating contracts with consultants – are legally authorized and justified in demanding restrictions on speech related to the work being conducted for them.

Any employer in the United States may define explicit regulations or policies affecting what employees may do with employer-owned communications resources. Typical privacy agreements explicitly state that employees agree to have any communications carried out using employer facilities (telephones, computers, faxes) potentially be monitored or restricted. Non-disclosure agreements provide frameworks to restrict revelation of proprietary or otherwise confidential aspects of an organization's work. Security levels restrict communications among employees who have different degrees of access; access-control lists and other authorization schemes limit who may access which views of corporate data. Although there are restrictions on monitoring personal conversations on corporate telephones, it is also possible and legally acceptable to promulgate regulations barring such calls or explicitly letting employees know that all communications using employer-owned equipment may or will be monitored.

An essential component of legality for all such restrictions is that there be no possibility of an *expectation of privacy* when using corporate resources. Even company cars may be searched legally as long as the policies are clear (privately owned cars may not be searched by employers). The yearly signature of a privacy policy by all employees is one way of ensuring that no one has an unfounded expectation of privacy in the workplace when using corporate tools; on computer systems, a good policy is to post the privacy (or lack-of-privacy) provisions for email, Internet use, instant messaging, and application usage on the login screens for session and even on the start-up screens of applications.

On the other hand, if an employee makes a personal call on a personally owned mobile phone or personally owned computer that is not using corporate networks, normally those calls would be private according to the privacy policies of the organization. Note, however, that any use of the corporate Internet networks would instantly demolish any reasonable expectation of privacy if the policies made that clear.

For a summary of U.S. rulings about privacy at work, see the article "Privacy at Work: What Are Your Rights?"¹⁶ For a review of the European situation, see "European Court of Human Rights Expands Privacy Protections: *Copland v. United Kingdom*"¹⁷ and "Personal Privacy in the Workplace: An EU Perspective."¹⁸

In summary,

- *Prima facie*, before any other considerations, most employment contracts stipulate that all professional writings created in fulfilling your professional obligations as an employee are copyright by default by your employer.
 - In some cases, this claim of intellectual-property rights over your creations may even extend to materials produced outside of normal working hours IF you have signed a contract abdicating your claims to such rights.
 - All written, verbal and pictorial communications created using your employer's resources and during normal working hours are by default the property of your employer.
- By default, employees have absolutely no privacy rights over electronic documents created on their employer's computers or over email and other documents received on or sent from their employer's email system.
 - Thus if you receive personal mail on your employer's email system, you have potentially forfeited your privacy rights over such communications.
- Employer claims for total access to employee communications are subject to modification.
 - In particular, courts have ruled that employee privacy may result from "a reasonable expectation of privacy."
 - Such expectation is affected by explicit policies defining the degree or lack of privacy protection for employee communications.
- Organizations lacking explicit policies affirming the employer's rights to access employee communications are in a poorer position to assert that claimed right.
 - Conversely, when policies are explicit in removing employee privacy expectations, employees have a weaker claim to a reasonable expectation of privacy.
- Implementation of privacy policies.
 - Even if an organization does have policies, the degree to which they are enforced may affect how seriously a court will judge their seriousness.
 - For example, an employer that makes employees sign a renewal of their understanding that they have no privacy rights may have a much better defense against an employee's claim of breach of privacy than an employer that mentions the policy once at the initial contract signing and never thereafter.
- Custom and culture.
 - There have been court cases dealing with the privacy rights of employees over their personal phone conversations.
 - Few employers will ban such calls outright, and if policies make no mention of privacy issues, employees may easily develop an expectation of privacy about such personal use.
 - The great danger is that such expectations may gradually extend to such uses of employer resources as Web access and email.
 - Nonetheless, there are no restrictions on employers' rights to warn their employees that all communications may be monitored.

Thus, as I understand it, there are no inherent rights to privacy in the workplace in the United States. It is the obligation of the employer to make it clearly and frequently known to all employees just what the policies are about use of employer equipment, and it is the obligation of the employees to understand and follow the privacy guidelines if they intend to continue as employees.

FREE SPEECH AND CORPORATE POLICY

Privacy questions and free-speech arguments sometimes become part of the discussions of whether or organizations in the United States can or should attempt to limit *employee* self-expression in *public*.

I am specifically referring to written materials prepared outside working hours and posted without the use of corporate resources on publicly accessible sites such as a personal webpage, a blog, a social networking site (e.g., Facebook) or, for that matter, on the cork bulletin board at the local supermarket.

In the United States, an employer attempting to enforce a policy forbidding employees from identifying themselves as such in public commentary without explicit permission and prior approval of the content of their postings may encounter resistance based on a misunderstanding of law. “But you have no right to limit my speech,” says the outraged employee. “You are violating my rights under the Constitution of the U.S.!”

Well, not usually.

The angry employee is muddily thinking of the *First Amendment* of the *U.S. Constitution*, which reads in part, “Congress shall make no law ... abridging the freedom of speech, or of the press...”¹⁹

After calming the employee down to prevent possible violence, explain quietly that the First Amendment refers to government action, not to private contracts. An employment contract can and in your case, presumably does, limit public speech when the employee identifies herself as an employee. The range of possible prohibitions is wide:

Some state laws protect speech and expression, prohibit employees from participating in politics or becoming political candidates, prohibit employers from influencing employees’ votes, prohibit discrimination based on political affiliation of employees, among other laws.²⁰

Other forms of limitation of speech under contract can apply even for non-employees; for example, one can insert nondisclosure clauses into a contract for consulting.

In the 1990s, before the World Wide Web became such a normal part of our lives, I was the Wizop (that is, the Chief Moderator) of the *NCSA Security Forum* on *CompuServe*, which at that time was an important value-added network with thousands of moderated discussion groups. I promulgated policies that enforced professionalism and forbade profanity, libel, demeaning comments about individuals or groups and general incivility in our discussions. We had a dozen sysops (abbreviation for “system operators”) who monitored each of the 20 sections of the Forum and who would remove offensive messages at once. They would write to the correspondent and explain the rules (often by rewriting the offensive message without the offensive language or style), warning that repeat offenses would result in exclusion from the Forum.

Occasionally, we’d get a furious message protesting that it was illegal for us to restrict speech because of the First Amendment. At that point, I would trot out a macro to generate a response something like this:

Perhaps you misunderstand the application of the First Amendment. The CompuServe Security Forum is not a government agency: we are a privately-owned discussion group running on a privately-owned network. If we establish rules forbidding the use of the letter ‘e’ in any message on the Forum, we may not get much traffic but we will not be violating any laws. Comply with our rules of conduct or leave.

Even government agencies have the right to control public speech by their employees; an example is the *Uniform Code of Military Justice* which applies to members of the Armed Forces of the United States. Article 88 (*Contempt Toward Officials*) states that

Any commissioned officer who uses contemptuous words against the President, the Vice President, Congress, the Secretary of Defense, the Secretary of a military department, the Secretary of



FIGURE 16.9

How much can an employee say?

Transportation, or the Governor or legislature of any State, Territory, Commonwealth, or possession in which he is on duty or present shall be punished as a court-martial may direct.²¹

Unfortunately, case law shows that employers have extraordinary power to respond to employees' behavior even outside the workplace and working hours. Employers have successfully escaped legal consequences for firing employees for

- Having a bumper sticker of which they disapprove on an employee's personal car.
- Posting something they don't like on social media.
- Drinking alcohol (on their personal time).
- Skiing or other sports deemed too risky (and thus increasing insurance fees for the employer).
- Being obese (in the case of a teacher).²²

Worse, employees may have to sign away their rights to file legal complaints when agreeing to their employment contract:

Even in the few areas of employment where you do have legal rights, it can be nearly impossible to enforce them. Almost 20 percent of employers today require all employees to agree in advance not to go to court if the company violates their legal rights, and to take their dispute to a private arbitration system selected (and sometimes run) by the employer. If you don't agree, you don't get the job. Some of these programs are fair. But others are kangaroo courts in which employers may handpick the arbitrators and deny employees the right to have a lawyer, or whose rules don't require the arbitrator to follow the law.²³

DEFAMATION

Defamation is harmful false information directed at or about a specific person or persons; written defamation is *libel* and spoken defamation is *slander*:

Generally, defamation is a false and unprivileged statement of fact that is harmful to someone's reputation, and published "with fault," meaning as a result of negligence or malice....

The elements that must be proved to establish defamation are:

1. a publication to one other than the person defamed.
2. a false statement of fact.
3. that is understood as
 - a. being of and concerning the plaintiff; and
 - b. tending to harm the reputation of plaintiff.

If the plaintiff is a public figure, he or she must also prove actual malice....

Truth is an absolute defense to a defamation claim.²⁴

In recent years, a former president of the United States was sued for defamation because he claimed that E. Jean Carroll had lied about his raping her. He lost the case and was ordered to pay his victim \$5 million in damages.²⁵

After the accused made yet more defamatory comments about Ms Carroll, he immediately lost a second court proceeding and was ordered to pay to his victim an additional \$83 million.²⁶

Employees must agree not to post defamatory materials of any kind, but in particular *never* to post lies about competitors. Lying does not work well as a sales technique:

It's a sad truth in business that competitors sometimes spread lies about you. Unfortunately, I've had this experience first-hand and found it to be terribly frustrating. "Why would they do that? How can I get them to stop? What should I tell my prospect? This seems like it's going to hurt my sale. This must be a bad thing for me and my company". As hard as this might be to believe, this isn't a bad thing at all and in fact this can easily be used to help you.



FIGURE 16.10
Defamation can be expensive.

....

What is the competition trying to do here? Why would they spread lies?

There are two possible options here:

- They don't know the truth in the first place – This can get complicated though – for instance, is management intentionally misinforming the staff or is your company shrouded in secrecy, thus resulting in the misinformation being out there?
- They know they are lying but they just don't care – this is what I call “malicious intent” – Their motivations here are likely varied but at the end of the day they are intentionally spreading misinformation in an attempt to gain an advantage.

Now they both end up with the same result and while it is important to consider motivation, it doesn't really have any effect on the possible ways to handle this issue.²⁷

Readers can imagine the consequences of being sued for defamation by a competitor with facts at hand that demonstrate the problem unequivocally. One of the recent cases in which a company had to pay for spreading lies about a company was the defamation of Dominion Voting Systems by Fox News. The propaganda network settled with their victims by paying \$787,500,000 to avoid a trial.²⁸

TROLLS

Trolls are people who post annoying, insulting, off-topic, *ad hominem*, and defamatory comments in discussions on social media. Their postings are deliberately disruptive and increasing in number and intensity, particularly in the stressful times of the COVID-19 pandemic:

Someone posts something, and someone comments that instead of being constructive or contributing to the debate simply responds in a way that is anything but productive. Reasoning and level discourse only exacerbate the situation.

In the end a post is hijacked.

Sadly the current political climate, made worse by recent events and the ongoing pandemic, has these occurrences feel even worse....

“It would make sense that the pandemic is making trolling behavior worse and widespread,” explained Dr. Kent Bausman, a professor in the Online Sociology program at Maryville University....

“Social media as a platform, the research tells us, has made trolling behavior more pervasive and virulent,” said Kent.

“Considerable research shows how the online environment leads to a lack of inhibitions in posting behavior and adds to a sense of empowerment through the cloak of semi anonymity that comes with online posting,” Kent added. “When you combine these with the lack of accountability that often comes with one's online behavior, we have emboldened people to speak in a virtual public sphere in a manner they would not otherwise do in a physical public space.”²⁹

Some trolls are actually *bots*: programs written to pretend to be people but generating materials with a particular orientation – some including defamatory materials.³⁰

Well-established approaches to interfering with trolls are summarized by Julia McCoy in her excellent summary (citing her topics – more details in her article):

1. Don't feed the trolls
2. Be the boss! No trolls allowed
3. Add moderators to your roster



FIGURE 16.11

Trolls are nauseating.

4. If you can't ignore the trolls, call their B.S.
5. Kill them with kindness
6. Disarm them with humor
7. Have friends-only social profiles
8. Block, ban, or report trolls
9. Decompress before you reply
10. Stay professional³¹

In my view, it is absolutely required that the moderator(s) of any social-media site monitor *every single posting and comment* on *their* pages. I have maintained that policy personally for more than a decade on my *Facebook* page. Before accepting someone as a "Friend," I always check their own page to see if they are reasonable people (and not obvious troll material). If there's even the slightest doubt, I send them the following *Facebook Messenger* text:

Hi!

Welcome to my Facebook page!

Rules for participating in my Facebook page:

- I encourage well-written postings even when I disagree with their content; however, I do not tolerate postings that express bigotry such as racism, misogyny, homophobia, and other prejudices.
- Stick to the topic in discussions of a posting.
- Provide evidence where possible to support your position.
- Don't post disinformation (claims that aren't true such as anti-vaxxer propaganda or Trumpist lies).
- Don't use ad hominem attacks on other posters on the page when you disagree with them.
- Don't use obscenities and vulgarities.
- I delete offensive posts and send a warning about them to the writer.
- I block people who persist in violating the rules for MY page.

Have fun!

If someone posts an unacceptable response in a discussion, I remove their troll-post and send them the text above with a warning that if they violate my rules again, I will block them from commenting. Since only "Friends" can post responses on my page (although anyone can read the postings), this approach usually works. In my decade on *Facebook*, I've blocked only a handful of people. One particularly sad case was a friend and colleague I'd known for four decades who insisted on posting anti-vaxxer nonsense in serious discussions of epidemiology. I am still sorry to have lost her friendship but still maintain that blocking her comments was a responsible response.

So in conclusion, if you are running a corporate social-media site, be sure that your rules about postings are clear and that there are named employees or volunteers who are monitoring and controlling *everything* that is posted on *your* pages.

LEGAL RESPONSES TO DEFAMATION BY TROLLS

The fundamental problem for dealing with trolls is that they may not be unambiguously identified. Identification usually depends on the nature of the medium through which the abuse is transmitted. For example, email and social-media posts from many sources may not be traceable because the organizations allow unverified information in registering users:

Social media has become weaponized. And, while this weaponization poses serious threats to our country in the long term, the short term threat



FIGURE 16.12
Punishing trolls.

is to social media itself. Russia has poisoned the well, we know that now. And while the FBI and Justice Department play whack-a-mole on the back end of the spectrum finding and cleaning out false posts from these Russian social-ops teams and bots, it may be time for robust identity verification on the front end.

Social media is too powerful now to be anonymous.³²

On a personal level, the target of defamatory posts may report certain posts to law-enforcement agencies as cyberbullying – assuming that there is any way to identify the sources accurately.

Victims may also file civil lawsuits:

How you choose to respond depends on the nature of the trolling, the type of Internet site on which it occurs, and the level of threat presented.

While the scope of relevant criminal and civil laws is somewhat limited, there are some legal remedies that you can turn to if you are trolled.

- Criminal laws. Trolling is not a crime under federal law. But under the laws of many states, harassment, stalking, and/or bullying are illegal....
- Civil laws. When a troll uses false, disparaging language to attack a target, these acts may constitute online defamation. And, if the troll's attack is egregiously personal and offensive, the troll may be inflicting emotional distress on the victim. These are torts, and the victim may file a civil lawsuit against the troll for damages.³³

Facebook has recently been responding to increasing demands for control of unacceptable posts:

Facebook could reveal the identity of people who post defamatory material on its platform if asked by someone suing for defamation or by a court order.

The [Australian] federal government wants to do more to hold social media platforms accountable as publishers of the content on their platforms and is pursuing a two-track process: defamation law reform and the regulation of online abuse....

In the last quarter [July-September 2021], Facebook removed 31.5 million pieces of hate speech and 7.9 million pieces of bullying and harassment content it had found to breach its Community Standards.³⁴

Followers of a disgraced politician have been trolling judges and jurors with threats – some actually threatening murder. Some of the people involved in the trials have been *doxxed* with serious consequences for the victims:

The ... grand jurors who indicted Trump in Georgia were doxxed, meaning that their personal information was shared online. Georgia is one of the few states that publishes the names of jurors for the sake of transparency in criminal proceedings.

Internet users have shared the grand jurors names and addresses on far-right message boards and made violent threats against them. One user on the message board where the QAnon conspiracy theory began threatened to “follow these people home and photograph their faces.”

A user on another message board described the jurors' names as a “hit list.” Another user responded, “Godspeed anons, you have all the long range rifles in the world.”³⁵

INTELLECTUAL PROPERTY

A general definition of intellectual property is “creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.”³⁶

COPYRIGHT

Restricting Illegal Downloads

A reader asked about legal liability of managers in a corporation where users were downloading copyrighted music using peer-to-peer networks without permission of the copyright holders. She asked who would investigate such breaches of the law and whether presence of an acceptable-use policy (AUP) would affect the outcome of possible prosecutions.

As I understand the situation, failure to exercise due diligence in establishing, monitoring, and enforcing effective security policies governing acceptable use of copyrighted materials can lead to serious problems. Managers as well as employees may be accused of trafficking in stolen intellectual property and face lawsuits and fines. The doctrine of *vicarious liability* may result in legal proceedings against manager who should have known about the illegal activity. The doctrine of *contributory infringement* allows a manager to be charged if the supervisor actively controlled or tolerated the illegal copyright violations.³⁷

In this textbook, almost every image is licensed from ClipArt.com; some are my own creation and a few are used by explicit written permission of the copyright owners.



FIGURE 16.13

Uncontrolled downloads can lead to legal problems.

TRADEMARKS

As Happy as a Rock Star in a Pig Pen: Fair-Use Doctrine in a Video Game

Just how far does copyright extend? I ran across an astonishing case during my research for an intellectual-property yearly review for my graduate students that illuminate concepts of fair-use doctrine.

The owners (ESS Entertainment 2000) of the *Playpen Gentlemen's Club* in eastern Los Angeles objected to the inclusion of a strip club called the *Pig Pen* in the video game *Grand Theft Auto: San Andreas* owned and produced by *Rockstar Video*, which takes place in a cartoon version of Los Angeles called "Los Santos" that was composited by artists in Scotland from elements captured in photographs taken throughout the Los Angeles area. [I am not making this up.]

On April 22, 2005, ESS sued for trademark infringement and unfair competition under a number of statutes. The club owners argued that the video game's inclusion of a logo similar to that of their club would give the impression that they had authorized inclusion of *their* club in the game.

In response, Rockstar moved for summary judgment on all of ESS's claims, arguing that the affirmative defenses of nominative fair use and the First Amendment protected it against liability. It also argued that its use of ESS's intellectual property did not infringe ESS's trademark by creating a "likelihood of confusion."

The first trial resulted in a judgment in 2006 that the video-game makers were not culpable for trademark violations because their use even of similar names was protected by First Amendment law.³⁸ The plaintiffs appealed the judgment. Judge Diarmuid F. O'Scannlain of the *U.S. Court of Appeals for the Ninth Circuit* wrote the Court's opinion affirming the lower court's rejection of ESS' claims of trademark infringement and published it on November 5, 2008. The key elements of the Appeal Court's reasoning were as follows:

- In its defense, Rock Star argued that the nominative fair-use principle protected its use of a trademark. Nominative fair use occurs when someone uses a trademark to describe the trademarked product, not a competing product with a similar trademark. The original



FIGURE 16.14

Video game led to lawsuit.

In February 2005, *Louis Vuitton* won a lawsuit in Paris against Google in which the court ruled that

...Google's allowing competitors to run ads triggered by Louis Vuitton's trademark terms was counterfeiting, unfair competition and misleading advertising. The court has ordered Google to pay Louis Vuitton \$250,000 and stop displaying ads for Vuitton's competitors whenever users type in the company's name into the search engine.⁴²

In June 2008, the *Vuitton v. Google* case continued with news that Google attorneys had succeeded in gaining a hearing for an appeal before the *European Court of Justice* in Luxembourg.⁴³ The case ended in favor of Google, allowing it to continue selling ads that use other organizations' trademarks without permission. There was some pushback by legal scholars at the time:

Fiona McBride, trademark lawyer at Withers & Rogers, described the ECJ ruling about the origin of an ad as "perplexing". She said it seemed to be unnecessarily introducing "a requirement of element or doubt as to the origin of goods and services which is not relevant for determining the infringement of a registered trademark."

"This is a setback for brand owners and seriously limits the scope of their trade mark rights when it comes to challenging use of their trade marks in online advertising," added McBride. "Only rarely will the internet user be unable to ascertain the origin of the goods and services and it will therefore be easy for advertisers to circumvent the law and use third party trade marks as keywords. This means that advertisers can secure a commercial advantage by piggy-backing on the reputation of the trademarks."⁴⁴

Unfortunately, using other organizations' trademarks is conducive to fraud. One of the most egregious abuses is the use of the logo and name of the *U.S. Postal Service* (USPS) in advertising by Chinese criminals who create counterfeit U.S. *Forever* stamps. Advertisements from dozens of sources in China masquerade as U.S. firms but some of their *Domain Name System* (DNS) registrations show they are based in the PRC. An experienced stamp dealer commented,

There has been a large increase in shops selling USPS Forever stamps at up to 50% off face value. I've been a stamp dealer for over 50 years and know how to tell when a postage stamp is fake, not to mention when buyers think that current USPS Forever stamps that sell for so cheap could be genuine they are sorely mistaken. These fake stamps are being printed in China and shipped to the US and sold by wholesalers for as little as 10c per stamp and then these dealers can triple or quadruple the price and make a killing and still be selling them for 30% below the price at the post office.⁴⁵

I personally collected images of over 1,000 fraudulent stamp ads posted to Facebook between March and December 2023 and reported all the ads to Facebook without effect. I submitted a detailed report to the *United States Postal Inspection Service* (USPIS), the *USPS*, the *U.S. Department of Commerce*, the *FBI* and *Interpol* including all the screenshots. I also contacted several hosting companies that were allowing the criminals to have websites; none of those ever responded either.

PATENTS

Patents were established in the U.S. Constitution to support the progress of science and the useful arts. Patents (the word comes from Latin for “open”) provide a limited time (currently 20 years in the United States) for exclusive right to use writings and discoveries by the owner of the patent; after expiration of the patent, the techniques are available to everyone without interference.⁴⁶



FIGURE 16.16

Patents expire.

U.S. Patent Laws

The first *Patent Act* was passed in 1790; another in 1793; and an important revision (U.S. Code Title 35, abbreviated “35 USC”) was passed in 1952 with changes added in 1995.⁴⁷ Section 101 of the Patent Act (35 USC §101) stipulates that patents may be granted only for new, useful and non-obvious processes, machines, manufacturing techniques, composition of materials or improvements. “New” is defined in 35 USC §102, which explicitly excludes patents if the subject of the patents is:

- Previously known or used in the United States
- Patented or described in printed publication before filing
- In public use or for sale in the United States more than one year before filing
- Abandoned
- Not invented by the applicant
- Also invented by someone else at the same time
- Already patented by someone else

In addition, a patent may be rejected if it is obvious to a person with ordinary skill in the art concerned. In this context, “art” means science, technology, or technique. “Ordinary skill” is defined by the complex interplay of a hypothetical competent expert’s awareness of all pertinent prior art, the types of problems encountered, prior art solutions, the speed of technology change, and the educational level of such experts.

Patent Trolls

Patent trolls are companies that buy unused and overly broad patents and then threaten small companies with lawsuits unless they pay extortion fees to avoid being dragged into court – often in far-away jurisdictions – to fight these spurious claims. A study published by the *Boston University School of Law* found that patent trolls “...cost U.S. software and hardware companies U.S.\$29 billion in 2011....”⁴⁸ That estimate was confirmed by further research; one study found that “defending a troll case can easily cost more than \$4 million or more.”⁴⁹



FIGURE 16.17

Patent trolls are nasty bullies.

A company called *PanIP* was formed in March 2002 and began suing small companies for patent infringement within a month of its incorporation. The company tried to extort \$5,000 fees from dozens of victims to avoid being dragged into court. The patent-infringement claims broadly asserted that any organization using any “automated sales and service system” and an “automatic business and financial transaction-processing system” was infringing on its purchased patents. Observers noted that all online sales systems would presumably fall under these absurdly broad claims.

The owner of a small chocolate factory, *DeBrand Fine Chocolates*, was having none of it. He organized a group of small business owners to resist the extortion; by November 2002, he had 16 companies in the *PanIP Defense Group, Inc.*⁵⁰ Because of the organized resistance,

PanIP dropped its lawsuits in March 2004 and did not continue its extortionate campaign thereafter.⁵¹

A number of organizations now help to resist abuse by patent trolls. For example, the *Open Invention Network LinuxDefenders* project is focused on fighting “patent aggression.”⁵² Their approaches are listed as follows (quoting directly):

Prior Art Assistance

In many cases where one of our community members was the subject of patent infringement claims, Open Invention Network has leveraged our network of relationships to identify and share prior art for use against patent trolls or corporate patent aggressors. This helps OIN licensees at risk, or in litigation, to better defend against Linux-centric patent aggression.

Reducing Patent Application Claim Scope

Open Invention Network has been a leading user of third party pre-issuance submissions, which are prior art submissions to limit the claim scope, or secure outright rejection, of overly broad patent claims in patent applications which are focused on key technology areas relevant to Linux and adjacent open source technologies.

Encouraging Open Source Software Use of Inter Partes Review

“Inter Partes Review”, also known as an “IPR”, is a procedure for challenging the validity of an issued patent owned by a 3rd party. By challenging patents with IPRs, the Linux and broader Open Source community can help to eliminate them. Unified Patents — which OIN, IBM, Linux Foundation and Microsoft support through its Open Source Zone —has successfully invalidated several patents using IPRs.

Advocating Open Source Use of Defensive Publications

Defensive publications are documents that provide descriptions and artwork of an invention so that it enters the public domain and becomes prior art. The disclosure prevents other parties from obtaining a low-quality patent (or, a non-novel patent) on the same invention later. OIN encourages all Open Source community members to submit inventions as defensive publications for free at tdcommons.org.

Another organization for defending against patent trolls is the *License on Transfer (LOT) Network*. They describe their group as a

...community of 1700+ global industry leaders who have collaboratively immunized themselves against lawsuits from Patent Assertion Entities (PAEs, also known as “patent trolls”).⁵³

For more general information on defending companies against patent trolls, see an article by *Global Patent Solutions* from 2020, which has details expanding on each of the following recommendations:

1. Have an IP lawyer in your corner.
2. Follow due process in protecting your own intellectual property.
3. Join a group or organization that specializes in protecting against patent trolls.
4. Utilize other online resources.
5. Do your research.⁵⁴

The morals for today’s organizations:

1. Do your homework if you want a patent on novel technology.
2. Work with competent patent attorneys to do your filing right.
3. Do not give in to patent trolls.

LEGAL DIMENSIONS OF Spam

I've been watching with growing dismay as the number of unwanted and offensive messages has been rising in my email over the years. I'm not alone: reports as the original of this section was written were practically unanimous in suggesting a significant growth in the problem of unsolicited commercial email.⁵⁵ A shocking summary about the problem was maintained by statista.com, which published monthly graphs showing that 80%–90% of all email worldwide was spam.⁵⁶

Spammers have always been sneaky about their sleazy unwanted email, with tricky subject lines and forged headers a commonplace for years. However, my own observations, confirmed by industry reports, show even further depths of depravity among these horrible people.

One increasingly frequent dodge is to put random punctuation in the subject lines and even in the message text itself. I had to be careful in giving examples in my original article, because I didn't want my subscribers' antispam filters stopping the original message sent by email, so I left exact details to their imagination. Suffice it to say that, ah, *body-enhancing drugs* (none of which should be taken without medical supervision anyway and some of which make claims that are patently impossible – or at least, one hopes so – about specific bits) now have subject lines something like “\$PE.ND YOUR MON.E!Y ON USEL.ESS STUFF TO GET BIGG.ER.” As a result, my own antispam filter was failing to pick up some of these messages and I had to add additional details to my second-line filters. However, since the number of positions where one can put a variety of punctuation marks and other symbols is far larger than my patience, manual intervention is doomed. Luckily, antispam services are doing well in stripping excess punctuation out of the text when scanning for recognizable spam strings. Some mass-email services even provide good explanations of how to tune one's GMAIL anti-spam filters.⁵⁷

PICTURE THIS: HTML SPAM

The nasty people who flood our email with unwanted advertising have been using increasingly deceptive means to elude spam-filtering software, most of which runs on the same principle as signature-based antivirus software or misuse-detection IDS. The defensive products rely on intelligence from the field to identify known patterns of subject lines and content to screen spam from their users.

A simple technique that spammers have used recently is to find synonyms for the keywords that are blocking their junk; thus, they may use the chemical or generic name of various drugs instead of the brand name. The names are also spelled wrong in a wide range of ways – not by mistake, one can be sure. Some spammers use the hacker's alphabet (*Leet*) which uses numbers for some letters; others use letters from different alphabets (e.g., Cyrillic) that look like standard Roman letters.⁵⁸

Some spammers have shifted to almost exclusively HTML email with embedded images that represent their text. Thus, instead of being able to scan for the keywords that characterize so much of this repetitive garbage, the antispam tools are faced with bland HTML for a couple of links and an unscannable bit-image that contains no machine-readable text.⁵⁹



FIGURE 16.18 A famous food – and now a name for electronic abuse.



FIGURE 16.19 HTML code can hide signs of fraud.

A particularly nasty feature of a lot of spam is the *unsubscribe* link that actually sends a response to dozens or even hundreds of other spammers, adding the naïve victim's email address to those criminals' collections. Clicking on such a link can increase the recipient's spam flow by an order of magnitude. No one should *ever* click on *any* link in email without checking its definition (hovering the cursor over the link usually works fine).

ORGANIZING THE RESISTANCE: FIGHTING SPAM TOGETHER

The spam situation reminds me of the early days of the antivirus industry, when I was the first Secretary of the *Anti-Virus Product Developers' Consortium* (AVPD) sponsored by the then-NCSA (later called *ICSA Labs* and then *TruSecure*). In the early 1990s, the idea of sharing virus signature strings among competing antivirus vendors struck some observers as ludicrous. However, I remember NCSA founders Bob Bales (z'l) and Paul Gates arguing with the vendors that it was no stranger than having medical or biochemical information about diseases and toxic materials shared among competing pharmaceutical companies: companies could compete on how well they fought the problems rather than concealing information about the problems. The industry agreed, and since then antivirus companies have routinely worked with what became known as the *Anti-Malware* group of the ICSA Labs.⁶⁰

Antispam-software developers are also sharing knowledge of the spam recognition strings too. After all [I can hear the complaints already], *domain thing* is to fight the spam (groan).

The *Realtime Blackhole List* (RBL) is dedicated to providing ISPs with the information needed to block email from organizations that send spam. In particular, the RBL is used to help ISPs identify open spam relays – SMTP servers that do not require I&A to send email through them from outside their home network. Such unprotected servers are ripe pickings for the criminal spammers who cheerfully send out millions of messages through other people's equipment without permission.

The RBL prevents system abuse by halting spam. However, the blacklisting process must be handled carefully. It cannot prohibit appropriate or authentic source connections or open-source networking. If an ISP subscribes to the RBL, the ISP may determine which IP addresses should be blocked and added to the RBL. If an IP address matches an IP address listed on the RBL, the connection is automatically dropped.

The RBL was first implemented by the Mail Abuse Prevention System (MAPS), which was acquired by Trend Micro in 2005. Trend Micro adheres to strict guidelines and policies in its continuous effort to nominate and remove spam IP addresses from its blackhole data listings.⁶¹

Trend Micro briefly summarizes the features of what they call *Email Reputation Services* (ERS) as follows:

- **Known Spam Source List Service**

In this service, a single DNS query is sent to the *Known Spam Source List + DB*, which contains documented sources of spam and list of dynamic IP addresses. If the sender is included in this DB, your mail server will return a '550' error or reject the connection.

- **Network Anti-Spam Service (NAS)**

This feature includes the *Dynamic Real-Time Spam Blocking*. If the first query to the *Known Spam Source List+ DB* does not return a positive response, a second query is sent to the QIL DB [*Quick IP*



FIGURE 16.20

The resistance is growing.

List, also called the *Dynamic Reputation Database*]. In this case, a positive response returns a '450' error or a temporary failure of the requested connection. This DB may occasionally list legitimate-mail servers with compromised hosts behind them that are temporarily sending spam. If this is the case, it will re-queue and try again later, causing a delay in mail delivery until the listing expires.

Other tools are also available.⁶²

NOT AN OPTION

The *Direct Marketing Association* (DMA) has been fighting for the right of its members to spam us for a long time. Their website had an illuminating article back in 2003.⁶³ The document pointed out that spam was tarnishing all direct marketers and piously announced that, "... we're all losing - consumers, businesses, and, yes, even email marketers."

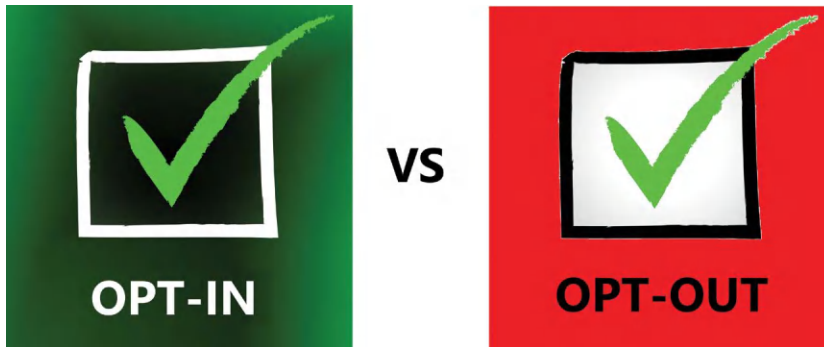


FIGURE 16.21 Which do you prefer?

The DMA proposed what it calls *four pillars of responsible email* which I quote verbatim:

- Honest subject lines.
- Accurate header information that has not been forged.
- A physical street address for consumer redress.
- An opt-out mechanism that truly works and is honored.

They also proposed to

- Forbid automated, surreptitious harvesting of email addresses.
- Define a universal opt-out technique to be incorporated into all junk email.
- A bond (at least \$500 per entity) for organizations agreeing to abide by the DMA principles in case they violate the standards.
- Support U.S. federal laws that would preempt state laws on spam.
- Subsidize investigation and prosecution of spammers.

The DMA raised my hackles because it specifically argued for an *opt-out* approach to spam. All of us are supposed to be happy to receive one junk email message from any organization in the United States (since the DMA deals exclusively with U.S. spammers) and just decline to receive more.

There are millions of firms in the United States. Receiving one message from each of them occasionally could fill anyone's email in-basket quickly. And why does the DMA nowhere suggest a DO NOT EMAIL list equivalent to the DO NOT CALL list (which is admittedly a complete failure⁶⁴) that is supposed to stop telephone calls from organizations and criminals? Having to opt out of thousands of individual lists strikes me as a ridiculous solution to the problem.

The DMA also failed to recognize that offshore spam is growing. Spammers know that other countries are years or even decades behind Europe and the United States in regulating the use of Internet resources; annoy them here and they can simply move away or contract with overseas organizations to continuing sending their spam without concern.

I think the fundamental problem is economic. The entire issue boils down to abuse of the commons: greedy people sending out their garbage at virtually no cost to themselves. We may someday see enraged Internet users insisting on a micropayment per email message – say, \$.001 per message – that would lead to trivial costs for consumers and normal users of the Internet but cost spammers a great deal of money. Fail to pay your bill and you *can* be sued successfully for fraud. ISPs could collect these fees and put them in a general fund for legal proceedings against abusers.

Now *that's* the kind of option I'd like to see for hurting spammers.

VULNERABILITY EXPOSURE

Many years ago, I was having a chat with one of my graduate students and we started talking about people who release details of vulnerabilities to pressure software firms for rapid fixes to problems. The student felt that releasing details of security vulnerabilities was a good way of forcing companies to pay attention to weaknesses. He told me that in his company, where he was a security administrator, he and his colleagues told a major vendor about what they considered a serious vulnerability in a firewall. Months went by without action. Finally, they lost their patience and posted full details of the vulnerability in an appropriate USENET group – and the problem was fixed within days.

I said this smacked of extortion and told him about various times when computer-security specialists had actually gone further than merely posting information but actually demanded payment NOT to do so. For example, in the RISKS DIGEST 20.82, a correspondent wrote about a case of quality assurance failure in the Paris subway system:

“The *Times* (London) reported on 26 Feb 2000 that Serge Humpich, a hacker, was convicted of fraud and given a suspended sentence. The young man discovered how to trick the Carte Bleue system and claimed he could have gone on an unlimited spending spree. Instead he hired lawyers and negotiated with the company that runs the system for payment in return for detailing the problems. The company turned around and prosecuted him for fraud after they arranged for him to demonstrate the system. What a brilliant way to discourage folks from rooting around in a system _and_ reporting security flaws! I wouldn't be surprised if their system proves to be so impervious that the number of bug reports drop to zero. What a wonderful solution for creating bugfree code!”⁶⁵

I can see the author's point: punishing people for pointing out quality-assurance flaws is hardly going to encourage wide contribution to quality assurance. However, it seems to me that the issue was not the identification of a security flaw; the problem was that M. Humpich tried to get payment for his knowledge of the security flaw he found by withholding that information unless he were paid. We call that *extortion*.

Of course, this was not the first case where someone tried to get payment for information about a bug they have discovered. In June 1997, Christian Orellana, a Danish computer consultant, threatened to release information to the press about a serious security weakness in the old *Netscape*



FIGURE 16.22 So is exposure good or bad?

Navigator browser unless he were paid more than the \$1,000 prize offered by Netscape to encourage independent quality assurance tests. His message included the words,

I think the person most suited for handling this is somebody in charge of the company checkbook.... I'll leave it to you to estimate what impact that would have on Netscape stocks.

His actions were almost universally reviled by professional security specialists. Ironically, Netscape already had a program in place to reward volunteers who notified them of bugs. They refused to pay the consultant the \$1,000 honorarium he would have received had he not demanded the larger payment.⁶⁶

Now, extortion is defined as “the act or an instance of inducing or attempting to induce someone to do something by threats, real or false criminal accusations, or violence.”⁶⁷ It seems to me that the men in both stories above were coming pretty close to – or crossing into – extortion.

VULNERABILITY DISCLOSURE ONLY FOR A FEE?

But isn't it normal for someone to charge for access to their knowledge? Why shouldn't someone offer to trade their pointers on a vulnerability in exchange for money? Isn't that what consultants and employees do all the time? After all, when a security specialist is working for an employer or for a client, how is getting paid for their penetration testing or advice on quality assurance or recommendations on security policy any different from offering to tell a firm about a security vulnerability in return for a fee?

One way of thinking about the difference is to think about ordinary life. Haven't we all pulled up next to a car and notified the driver that their brake lights don't work? Would you refuse to tell the driver about their brake lights unless they paid you a fee? How would you feel if someone said, “If you give me <a large amount of money> I'll tell you about a dangerous problem with the safety system of your car.” Would you perceive the offer as a legitimate invitation to engage in a commercial transaction? I wouldn't. I make it a personal hobby to spot cars with any of their brake lights out and to tell the drivers kindly about it as soon as it is safe to do so. I figure that my *Goody Two-Shoes*⁶⁸ hobby may have saved a few lives in my 50 years of driving.

There are many faithful contributors to bug lists who routinely warn software companies about problems at no cost. I personally know many security experts who have warned companies about threats and vulnerabilities without expecting monetary reward; indeed, many people speak at conferences for no pay at all to share their knowledge and experience freely with colleagues. Thousands of individual professionals, scholars, non-profit organizations and companies, and government agencies contribute countless pages of useful information on the Web at no cost to the recipients.

The warnings are often carefully structured so that enough information is provided to help identify the vulnerability but not enough to let clueless wannabees launch attacks using precise scripts.

These folks are doing the cyberspace equivalent of giving blood. I am sorry that there are people whose economic circumstances make it reasonable to sell their blood, but that doesn't change my admiration for those who donate blood freely.

So returning to extortion, I think the issue here is the sense of community. Those of us who feel that we are all in the battle against computer crime together feel the same obligation to help a vendor or a system improve as we do toward other drivers who have burned-out brake lights. I see this spirit of collegiality whenever I'm talking to colleagues who are in some sense direct competition for my employer – yet we feel a camaraderie in trying to fight computer crime and abuse. Rarely have I seen hostility among consultants working for different firms, let alone with that thin line of security professionals in corporations, government departments and other organizations who work day after day to protect the interests of their employers and their stakeholders.



FIGURE 16.23

Professionalism or greed?

Unfortunately, some of us feel isolated and excluded from the wider society. Anomic people do not feel the sense of connectedness that makes it feel good and right to share knowledge freely. For people who feel like outsiders – for example, some of those involved in the criminal-hacker subculture – helping others altruistically may not make emotional sense. For these folks, an argument to consider is that helping others as a professional courtesy is a far better way of forging one's reputation as a trustworthy and helpful resource than trying to extort payment by withholding information.

MANAGING VULNERABILITY DISCLOSURE

Corporations have to shoulder their share of the blame for the frustration felt by users who fruitlessly batter at their doors to get a hearing. Yes, corporations do have priorities for using limited resources, but the frustration comes from not being listened to. From experience in technical support, I'd say that the critical elements in gaining the cooperation of users who are experiencing difficulties are:

- Paying attention to the calls for help or for repairs.
- Having a systematic method for tracking all calls and correlating problems so that you know what is causing most of the trouble.
- A system for assigning priorities to specific fixes or repairs.
- Reliable, frequent communications with the people who called in the trouble report
- Involving the callers in solving the problem if possible.



FIGURE 16.24
Virtuous disclosure.

The worst thing a company can do is brush off a trouble report; the next worst is to claim that they will resolve the problem when in fact there is no intention to do so. Honesty is essential in all our work, and especially when dealing with clients and with the public at large.

When I was an operating-systems and DB performance specialist for *Hewlett Packard* in the early 1980s, it always seemed wonderful to me that HP consistently published a complete list of all the known problems they had registered for their products. The *Systems Status Bulletin* was published quarterly, with biweekly updates; it was a compendium of all the problems that had been localized in every software product the company made, with patch numbers for those that were fixed, release numbers for patches that had been integrated into installation releases, and work-arounds if possible for those problems that were not yet fixed.

I recommend this honest and complete approach to all companies, especially those working with security products.

Finally, users and specialists should understand that using the threat of publishing detailed exploits – or actually publishing them before informing the vendors – is a crude, extreme and unprofessional approach to resolving a problem. Instead, try to build pressure using a graded series of actions instead of jumping to threats:

- Define a timetable for acceptable responses that takes into account the severity of the security hole – don't ask for instant repairs on a minor item.
- Contact higher levels of management at the vendor firm to discuss the issue.
- Get the cooperation of upper management in your own firms, if appropriate.
- Arrange for face-to-face meetings between the top managers of your firm and those of the vendor firm.
- Contact your professional colleagues for joint letters pressing for a solution.
- Raise the issues in professional forums (usenet, mailing lists, professional association meetings) without giving enough details in public that would allow instant exploits by the black-hat crowd.

- Set up a BOF (*birds-of-a-feather group*) at an upcoming meeting specifically to discuss solutions and workarounds to a longstanding or fundamental design problem.
- Look for alternative suppliers – and make sure that you do so openly by telling your supplier you are not satisfied with their product quality or their service.
- Contact certifying bodies to withdraw certification of products that remain unrepaired for a long time after notification.
- Get your corporate counsel involved to discuss possible legal action for breach of contract if possible.
- Publish information about the problem, again without giving away so much detail that you make the problem worse than it already is. The last thing you want is to give some twisted ten-year-old script kiddie (or a twenty-year-old with the same level of moral development as a ten-year-old) a prefabricated attack script.

In summary, I think that a sound approach to preventing extortion in our business involves making it unnecessary. We should establish norms for professional, collaborative responses to reports of vulnerabilities. The other powerful tool we can use is peer pressure: let's establish a consensus about not trying to extort compliance with our own priorities when we run into trouble with software and systems. But in any case, demanding money to avoid publication of a vulnerability is just plain sleazy.

In the world of INFOSEC, we need people who are the equivalent of blood donors, not blood suckers.

VIRUS-WRITING IN COURSES

A storm of criticism washed over a *University of Calgary* Professor in early summer of 2003 when he announced his intention to teach a fall course entitled “Computer Science 599.48: Computer Viruses and Malware.” Assistant Professor John Aycok shocked the anti-virus world by including his intention to have his undergraduate students write some malicious code. Many experts objected on the following grounds:

- *Writing* malicious code was unnecessary in teaching how viruses, worms, and Trojan horses work or how to fight them.
- Keeping the malicious code *contained* within the class for laboratory would be difficult or impossible.
- Some students would take the wrong message home about the ethical implications of creating malicious code.
- Students with experience writing malware would be unemployable by antivirus firms, always concerned about the widespread rumor that they engage in writing viruses for profit.⁶⁹



FIGURE 16.25

Writing malware in a course.

Supporters of the course rejected these arguments, assuring critics that the laboratory would be well secured and insisting on the pedagogical value of such exercises. In addition, they stressed that virus writing would be only a small part of the course, which would also teach students about the history of malware, economic consequences of these programs, countermeasures, legal and ethical considerations, and wider principles of computer and network security.

After the course was over, there appeared to have been no breaches of security and University spokespersons insisted that they would offer the course again despite their critics.

It seems to me that writing real viruses may be less valuable to the students than analyzing a wide range of existing viruses and thinking about, designing, and implementing antivirus mechanisms.

However, given the relatively minor part that this exercise plays in the overall course, it also seems to me that critics may have overreacted.

I have been involved with the antivirus (AV) industry in a peripheral way since the early 1990s, when I was the recording secretary at the organizing meetings of the AVPDC of the NCSA. I can personally attest to the intense emotions of people in the AV industry about virus writers: they detest them. Perhaps some of the vitriol thrown at Professor Aycock resulted from an emotional response rather than from a wholly rational appraisal of risks and consequences.

I wrote to the University of Calgary about this situation. Dr Ken Barker, Head of the Department of Computer Science, responded as follows:

A thorough understanding of any material requires that we look at it from as many perspectives as possible. Students in high school learn that the most effective way to prepare an argument for a debate is to prepare to argue both the affirmative and negative sides. The most competent and insightful economists are those who can clearly articulate and understand both a fully free market system and a controlled socialist strategy to the economy. The better we understand something, even if we radically disagree with it, the more likely we are to provide effective mechanisms to counteract them.

These analogies provide the context for the approach taken by the University of Calgary's CPSC 599.48 course. A very small portion of the course is spent on understanding how viruses are created and deployed in an extremely protected environment while ensuring that the students have a complete understanding of the legal and ethical framework surrounding this kind of code. The students are thereby better prepared to learn how to best fight the plethora of viruses and malware found in the modern compute environment.

The cautionary approach demanded by our critics during the first offering of the course was incorporated into the way we delivered the material. The alarms raised by the anti-virus community were addressed carefully and diligently to ensure that the course would be offered in a safe and valuable way. After a careful review of the first offering and upon considering the ongoing need for this level of expertise, the University of Calgary believes that it is in the greater public good to continue to offer the course.

I commend my colleagues for having responded constructively to the concerns of AV professionals and wish them well in their project. I sincerely hope that the reasoned approach they have adopted will indeed result in a net gain to security in the long run.

ANTI-VIRUS LAWS?

Every now and then the topic comes up of whether it makes any sense to pass *laws* against writing viruses.

For as long as I have been involved in antivirus work (since the early 1990s), some people have argued that writing a virus should itself be illegal. Such laws would make it clear to everyone that writing viruses is *bad*. Having legally prescribed punishments for virus writing would discourage some (not all) casual hobbyists from contributing their pathetic efforts to the pool of viruses.

However, others object that such laws would make antivirus work more difficult. They warn that regulating virus writing might justify a new bureaucracy dedicated to virus control. The law might be unenforceable and therefore ill-advised. Even more fundamentally, the harm from a virus, they argue, comes not from its existence but from its dissemination to unsuspecting victims. In that view, writing the virus does nothing as long as other people don't infect their computers. Even sending the virus to a willing recipient doesn't seem to be a problem: after all, people are free to run whatever programs they want on their own computers. Making virus *writing* illegal would be a form of prior restraint and divert attention away from monitoring or punishing clearly harmful acts.

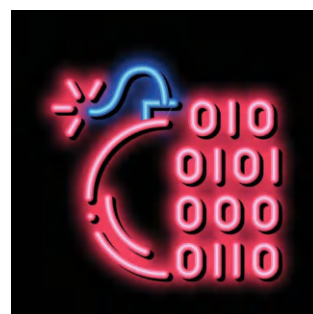


FIGURE 16.26

Illegal or useful?

How would these defenders of malware respond to exactly the same arguments, but substituting “lethal poison” instead of “virus”?

Even defining a virus in legal terms would be difficult, especially given the low level of technical knowledge among the legislatures of the world. Some humorists argue that a sloppy definition might classify Windows itself as a virus.

Furthermore, say the sceptics, viruses are written all over the world and the damages often occur in other countries. How will antivirus laws be enforced internationally?

I would like to see clear laws in place worldwide making it a serious crime to write *and release* computer programs which, without permission, insert their own code into programs or other executable code. To include worms, we might have to include programs which propagate without authorization. This simple idea would focus on the fundamental attribute of viruses and worms: their sneaky invasion of *our* computers. Ideally, the U.N. would frame a convention urging nations to allow extradition of people alleged to have written viruses that have harmed the citizens of another nation.

As discussed in the section on writing viruses in courses, no responsible academic institution would willingly allow students or faculty to release viruses into the wild. The proposed convention mentioned above might help ensure that academics hold to that principle.

VIRUSES ARE NOT SPEECH

Could laws be applied to *publishing* functional virus code?

A January 1993 discussion in the NCSA section on the *CompuServe* network for which I was the WizOp considered the issue of forbidding publication of functional viral code. Participants drew parallels between writing down viral code and writing down instructions on creating harmful devices such as bombs. The slippery-slope argument was invoked by one prominent member of the antivirus community, who said: “My concern is that if we can justify the suppression of information as ‘undesirable’ or ‘potentially dangerous’ is it that much further a jump to ... suppression of other ‘information?’”

People who build antivirus products need the code but can get it through private, controlled channels. People who build computer system hardware and want to devise better antivirus traps can also use real viruses obtained through controlled channels, and so can operating-system gurus. Computer scientists and antivirus product developers wishing to publish research on specific features of viruses can share their knowledge constructively by printing portions of the code in question without making the entire functional virus available to all and sundry. As long as what is disseminated does not work if entered directly as printed or transmitted, I see no problem.

But public, unrestricted dissemination of functional viral code to, say, disturbed 15-year-olds intent on causing havoc is unnecessary and harmful and ought to be punished in the same way we place preemptive restrictions on other potentially harmful acts.

Some U.S. attorneys have invoked *First Amendment* rights protecting certain kinds of speech against government interference to argue against any legal restriction on writing and sharing malicious code.

But is viral code speech at all, let alone protected speech? For that matter, is any kind of computer program necessarily speech? U.S. District Judge Marilyn Patel certainly thought so in August of 1997 when she ruled against the U.S. government attempt to stop Professor Daniel Bernstein from publishing his source code for the encryption algorithm *Snuffle* [I love that name]:

This court can find no meaningful difference between computer language, particularly high-level languages as defined above, and German or French.... Like music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who



FIGURE 16.27
Speech or not?.

can read it.... Thus, even if Snuffle source code, which is easily compiled into object code for the computer to read and easily used for encryption, is essentially functional, that does not remove it from the realm of speech.... For the purposes of First Amendment analysis, this court finds that source code is speech.⁷⁰

I think that legal decision is wrong. Considering programs to be a form of speech rests on a misperception due to the way we represent programs. Programs look like written language. Programs use letters and numbers and can be interpreted by human beings.

However, it's irrelevant how we *represent* computer programs. A program is the instructions themselves, not the medium in which they're coded. A program in assembler is a program whether it resides on a hard disk, a CD-ROM, or a portion of a memory array. Indeed, that sequence of computer instructions would be the program itself even were it written on a papyrus, chiseled in stone, signaled by semaphore or printed in a book.

If computer programs were represented as colored squares and circles with lines coming out of them, perhaps the Justices might be less inclined to think of them as speech. For example, consider a wire-board controlling a card sorter. Is the wire-board speech? Not in any sense most people would use the word. How about a paper punch tape controlling a machine tool? What about a useful computer program expressed as machine language codes (0001010000110101)? I don't consider these codes to be speech and I don't think anyone else should either.

Here are some scenarios to think about:

- Alice works in a factory with Bob. Alice decides to kill Bob by publishing a printed tape for the robotic equipment they all use. Alice cuts out the machine-readable tape and includes it in Bob's pile of tapes for the next day's operations. Bob doesn't notice anything wrong and gives the tapes to the robot, which reads the instructions into its memory. Sometime later, Bob's robot punches 2,000 extra holes at random, four of which end up in Bob's head. Is Alice's act protected because the published paper tape contains letters and numbers such as "A0 1F 22 BB?"
- A molecular geneticist named Gene Hacker is arrested by police for having made several colleagues very ill with a new biological virus. Gene constructed the virus from bits and pieces of known RNA. Gene argues in court that his act is protected by the First Amendment: the virus, he claims, is speech. It is speech because it consists of four nucleotide codes, A, U, C and G, put together in a particular way. He claims to "write" using ribonucleotides just as computer virus authors "write" using machine instructions. Gene argues that his biological virus is just as much a symbolic expression of his opinions and feelings as the computer-virus authors' printing their viral codes in publications. Indeed, he argues, he has been "publishing" his biological virus just as they have published their computer viruses.
- A virus-writer named Ignominious (Iggy) Scoundrel publishes completely functional source code for a virus in the underground publication "3711." An eight-year old with an IQ of 79 types it into his C++ compiler and releases the object code at his school. The virus spreads to a hospital system with poor network topology and no internal firewalls and kills three patients in the intensive care unit. Iggy is arrested. At his trial for manslaughter, Iggy's lawyer argues that (a) Iggy had a perfect right under the First Amendment to express his creativity by publishing the viral code and (b) it's entirely the *eight-year old's* fault that something bad happened. I think programs are not speech and therefore malware code is not speech. Thus, it is possible in theory to craft laws which make it a punishable offense to publish fully functional viral code.

Quod erat demonstrandum?

NOTES

- 1 U.S. Congress (1986).
- 2 U.S. Congress (1956).
- 3 U.S. Congress (1986).
- 4 U.S. Congress (2000).
- 5 U.S. Congress (2008).
- 6 Zeigler (2009).
- 7 National Conference of State Legislatures (2021).
- 8 European Union (2018).
- 9 European Data Protection Supervisor (2018).
- 10 European Union (2018).
- 11 White (2020).
- 12 Wired Staff (2000).
- 13 Kerr (2015).
- 14 Bhardwaj (2018).
- 15 Kabay, Privacy at Work (2012).
- 16 FindLaw (2019).
- 17 Cate (2007).
- 18 McGuireWoods (2009).
- 19 U.S. Congress (1791).
- 20 Warren (2021).
- 21 U.S. Congress (2006).
- 22 Melber (2010).
- 23 Maltby (2009).
- 24 Electronic Frontier Foundation.
- 25 Mangan (2023).
- 26 Halpert (2023).
- 27 Speyer (2017).
- 28 Folkenflik (2023).
- 29 Suciu (2020).
- 30 Skowronski (2019).
- 31 McCoy (2021).
- 32 Burns (2018).
- 33 Criminal Defense Lawyer (2021).
- 34 Ward (2021).
- 35 Otten (2023).
- 36 World Intellectual Property Organization.
- 37 Schachter (2014).
- 38 U.S. District Court, C.D. California (2006).
- 39 U.S. Court of Appeals, Ninth Circuit (2008).
- 40 Google (2021).
- 41 Olsen, Le Meridien Hotels vs. Google France (2005).
- 42 Viener (2005).
- 43 Kirk (2008).
- 44 Sweney (2010).
- 45 Fox (2021).
- 46 Kenton (2021).
- 47 U.S. Congress (1952).
- 48 Bessen and Meurer (2012).
- 49 Lederer (2021).
- 50 Frazier (2002).
- 51 Bennett (2004).
- 52 Open Invention Network (2021).
- 53 LOT Network (2020).
- 54 Global Patent Solutions (2020).
- 55 Moorthy (2023).
- 56 Statista Research Department (2021).

- 57 Clean Email Team (2021).
- 58 Rouan (2021).
- 59 Le (2021).
- 60 ICSA Labs (2021).
- 61 Techopedia.
- 62 Keary, 9 Best Anti-Spam Software Tools for 2021 (2021).
- 63 Wientzen (2003).
- 64 van Zuylen-Wood (2018).
- 65 Wayner (2000).
- 66 cnet (1997).
- 67 Ambeau (2020).
- 68 British Library.
- 69 Fisher (2003).
- 70 Electronic Frontier Foundation (1996).

WORKS CITED

- Ambeau, J. P. (2020, November 22). *8 Examples of Extortion to Know*. Retrieved November 29, 2021, from Ambeau Law Firm | Recent News: <https://www.ambeaulaw.com/blog/2020/november/8-examples-of-extortion-to-know>
- Bennett, A. (2004, March 30). *PanIP Drops Patent Litigation Against Small Businesses*. Retrieved November 19, 2021, from ComputerWorld | Enterprise: <https://www.computerworld.com/article/2802777/panip-drops-patent-litigation-against-small-businesses.html>
- Bessen, J. E., & Meurer, M. J. (2012, June 25). The direct costs from NPE disputes. *Cornell Law Review*, 99(387), 54. Retrieved November 19, 2021, from Cornell Law Review: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2091210
- Bhardwaj, P. (2018, May 17). *Here's How to Send Emails That Expire With Gmail's New 'Confidential Mode'*. Retrieved December 19, 2021, from Business Insider | Tech: <https://www.businessinsider.com/google-gmail-new-feature-confidential-mode-expiring-emails-guide-2018-5>
- British Library. *The History of Little Goody Two-Shoes*. Retrieved November 29, 2021, from British Library | Collection Items: <https://www.bl.uk/collection-items/the-history-of-little-goody-two-shoes>
- Burns, W. (2018, February 22). *Is It Time to Require Identity Verification For Everyone Using Social Media?* Retrieved October 2, 2023, from Forbes: <https://www.forbes.com/sites/willburns/2018/02/22/is-it-time-to-require-identity-verification-for-everyone-using-social-media/?sh=a19adaa8683b>
- cnet. (1997, June 13). *Danish Bug Buster Defends Himself*. Retrieved November 29, 2021, from cnet | Tech | Services & Software: <https://www.cnet.com/tech/services-and-software/danish-bug-buster-defends-himself/>
- Cate, F. H. (2007, August 6). *European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom*. Retrieved June 29, 2021, from American Society of American Law: <https://www.asil.org/insights/volume/11/issue/21/european-court-human-rights-expands-privacy-protections-copland-v-united>
- Clean Email Team. (2021, November 18). *Gmail Spam Filter: When It Is Not Enough to Stop Spam*. Retrieved November 23, 2021, from Clean Email: <https://clean.email/gmail-spam-filter>
- Criminal Defense Lawyer. (2021). *Trolled Online: What You Can Do When You're Bullied on Social Media*. Retrieved November 24, 2021, from CriminalDefenceLawyer | Criminal Law | Common Crimes | Cyber Crimes: <https://www.criminaldefenselawyer.com/resources/trolled-online-what-to-do-when-bullied-social-media.html>
- Electronic Frontier Foundation. *Online Defamation Law*. Retrieved November 24, 2021, from EFF | Legal Guide for Bloggers | Liability: <https://www EFF.org/issues/bloggers/legal/liability/defamation>
- Electronic Frontier Foundation. (1996, Apr 17). *Federal Court Denies Government's Motion to Dismiss Bernstein Case, Acknowledges Source Code as Speech*. Retrieved November 29, 2021, from EFF | Press Releases: <https://www EFF.org/press/archives/2008/04/21-40>
- European Data Protection Supervisor. (2018, May 25). *The History of the General Data Protection Regulation*. Retrieved November 17, 2021, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
- European Union. (2018). *Chapter 5: Transfers of Personal Data to Third Countries or International Organisations*. Retrieved November 17, 2021, from Intersoft Consulting: <https://gdpr-info.eu/chapter-5/>
- European Union. (2018, May 18). *General Data Protection Regulation*. Retrieved November 17, 2021, from Intersoft Consulting: <https://gdpr-info.eu/>

- FindLaw. (2019, June 25). *Privacy at Work: What Are Your Rights?* Retrieved June 29, 2021, from FindLaw – Learn About the Law: <https://www.findlaw.com/employment/workplace-privacy/privacy-at-work-what-are-your-rights.html>
- Fisher, D. (2003, May 27). *Virus-Writing Course Stirs Controversy*. Retrieved November 29, 2021, from eWeek | Cybersecurity: <https://www.eweek.com/security/virus-writing-course-stirs-controversy/>
- Folkenflik, D. &. (2023, April 18). *Fox News settles Blockbuster Defamation Lawsuit With Dominion Voting Systems*. Retrieved October 2, 2023, from NPR: <https://www.npr.org/2023/04/18/1170339114/fox-news-settles-blockbuster-defamation-lawsuit-with-dominion-voting-systems>
- Fox, T. (2021, October 28). *Fake Forever Stamps*. Retrieved November 18, 2021, from Etsy | Forums | Shipping: <https://community.etsy.com/t5/All-About-Shipping/Fake-Forever-stamps/m-p/136233339/highlight/true>
- Frazier, L. M. (2002, December 1). *You May Be Next: It's a Threat to Smaller Online Merchants*. Fort Wayne Chocolatier Fights Back. Retrieved November 19, 2021, from Indiana Business Magazine <https://www.thefreelibrary.com/You+may+be+next%3A+it%27s+a+threat+to+smaller+online+merchants.+Fort...+a095689515>
- Global Patent Solutions. (2020, January 7). *How Small Businesses Can Protect Themselves from Patent Trolls*. Retrieved November 19, 2021, from SCORE: <https://www.score.org/blog/how-small-businesses-can-protect-themselves-patent-trolls>
- Google. (2021). *Create Your First Ad and Help Customers Choose Your Business*. Retrieved November 18, 2021, from Google: https://ads.google.com/intl/en_us/getstarted/how-it-works/
- Halpert, M. (2023, September 6). *Trump Suffers Loss in Second E Jean Carroll Defamation Case*. Retrieved October 2, 2023, from BBC | News | World-US-Canada: <https://www.bbc.com/news/world-us-canada-66733736>
- ICSA Labs. (2021). *ICSA Labs Certified Anti-Malware Products*. Retrieved November 23, 2021, from ICSA LABS: <https://www.icsalabs.com/technology-program/anti-virus>
- Kabay, M. E. (2012, December 13). *Privacy at Work*. Retrieved June 29, 2021, from M. E. Kabay: http://www.mekabay.com/perception/065_privacy_at_work.pdf
- Keary, T. (2021, May 28). *9 Best Anti-Spam Software Tools for 2021*. Retrieved November 23, 2021, from CompariTech: <https://www.comparitech.com/net-admin/anti-spam-software/>
- Kenton, W. (2021, April 12). *Patent*. Retrieved November 19, 2021, from Investopedia | Business | Business Essentials: <https://www.investopedia.com/terms/p/patent.asp>
- Kerr, O. S. (2015, May 2). Norms of computer trespass. *Columbia Law Review*, 116(4). Retrieved November 17, 2021, from <https://columbialawreview.org/content/norms-of-computer-trespass/>
- Kirk, J. (2008, June 4). *Google, Louis Vuitton Face Off in Trademark Spat*. Retrieved November 18, 2021, from NetworkWorld: <https://web.archive.org/web/20081006231853/http://www.networkworld.com/news/2008/060408-google-louis-vuitton-face-off.html>
- Le, M. (2021, August 26). *Experts Say: Why You Shouldn't Send Image-Only Emails*. Retrieved November 23, 2021, from Litmus Blog: <https://www.litmus.com/blog/why-you-shouldnt-send-image-only-emails/>
- Lederer, S. (2021, July 22). *The Growing Problem of U.S. Patent Trolls, and What Should Happen Next*. Retrieved November 19, 2021, from Forbes | Business Council | Small Business: <https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/22/the-growing-problem-of-us-patent-trolls-and-what-should-happen-next/>
- LOT Network. (2020). *Prevent Unwanted Litigation While Preserving the Use of Your Patents*. Retrieved November 19, 2021, from LOTNETWORK: <https://lotnet.com/>
- Maltby, L. (2009). *Can They Do That?: Retaking Our Fundamental Rights in the Workplace*. Portfolio Hardcover. Retrieved November 18, 2021, from <https://smile.amazon.com/Can-They-That-Fundamental-Workplace/dp/1591842824>
- Mangan, D. (2023, September 6). *Trump Suffers Big Loss in E. Jean Carroll Defamation Case, Judge Says He's Liable*. Retrieved October 2, 2023, from CNBC: <https://www.cnbc.com/2023/09/06/trump-suffers-big-loss-in-e-jean-carroll-defamation-case-judge-says-hes-liable.html>
- McCoy, J. (2021, October 7). *10 Effective Tactics to Defeat Internet Trolls*. Retrieved November 24, 2021, from <https://www.searchenginejournal.com/defeat-online-trolls/323439/#close>
- McGuireWoods. (2009, May 8). *Personal Privacy in the Workplace: An EU Perspective*. Retrieved June 29, 2021, from McGuireWoods Client Resources – Alerts 2009: <https://www.mcguirewoods.com/Client-Resources/Alerts/2009/5/Personal-Privacy-in-the-Workplace-An-EU-Perspective>
- Melber, A. (2010, January 29). *Can Bosses Do That? As It Turns Out, Yes They Can*. Retrieved November 18, 2021, from NPR | Your Money: <https://www.npr.org/templates/story/story.php?storyId=123024596>
- Moorthy, J. (2023, August 8). *23 Email Spam Statistics to Know in 2024*. Retrieved March 10, 2024 from mailmodo | Guides: <https://www.mailmodo.com/guides/email-spam-statistics>

- National Conference of State Legislatures. (2021). *Computer Crime Statutes*. Retrieved November 17, 2021, from NCSL | Research | Telecommunications & Information Technology: <https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>
- Olsen, S. (2005, January 20). *Le Meridien Hotels vs. Google France*. Retrieved November 18, 2021, from International Hotels & Restaurant Association: https://web.archive.org/web/20080720094652/http://www.ih-ra.com/html-ihra/ihra30/I30_AlerteLe_Mer.htm
- Open Invention Network. (2021, n/a n/a). *Linux Defenders*. Retrieved November 19, 2021, from OpenInventionNetwork: <https://openinventionnetwork.com/community-initiatives/linux-defenders/>
- Otten, T. (2023, August 17). “We Will Kill You”: Trump Supporters Threaten Judge, Jurors Amid Indictments. *Trump Is Facing Four Indictments—and His Supporters Are Setting Out to Hurt Those Trying to Hold Him Accountable*. Retrieved October 2, 2023, from The New Republic | Post: <https://newrepublic.com/post/175032/trump-supporters-threaten-judge-jurors-amid-indictments>
- Rouan, R. (2021, April 30). *Fact Check: Hackers Using Visually Similar Characters to Deceive in Phishing Schemes*. Retrieved November 23, 2021, from USA TODAY: <https://www.usatoday.com/story/news/factcheck/2021/04/30/fact-check-hackers-use-similar-looking-characters-phishing-schemes/4891437001/>
- Schachter, D. (2014, November 10). *Strategies: Employee Copyright Infringement Can Bite the Employer*. Retrieved November 18, 2021, from Denver Business Journal | Professional Services: https://www.bizjournals.com/denver/blog/broadway_17th/2014/11/strategies-employee-copyright-infringement-can.html
- Skowronski, J. (2019, July 30). *Trolls and Bots Are Disrupting Social Media — Here’s How AI Can Stop Them (Part 1)*. Retrieved November 24, 2021, from Towards Data Science: <https://towardsdatascience.com/trolls-and-bots-are-disrupting-social-media-heres-how-ai-can-stop-them-d9b969336a06>
- Speyer, J. (2017, September 24). Retrieved October 2, 2023, from LinkedIn | Pulse: <https://www.linkedin.com/pulse/honesty-only-policy-when-competitors-lie-jimmy-speyer/>
- Statista Research Department. (2021, October 21). *Daily Spam Volume Worldwide 2020-2021*. Retrieved November 23, 2021, from Statista | Internet | Communications: <https://www.statista.com/statistics/1270424/daily-spam-volume-global/>
- Suciu, P. (2020, June 4). *Trolls Continue to Be a Problem on Social Media*. Retrieved November 24, 2021, from Forbes: <https://www.forbes.com/sites/petersuciu/2020/06/04/trolls-continue-to-be-a-problem-on-social-media/>
- Sweney, M. (2010, March 23). *Google Wins Louis Vuitton Trademark Case*. Retrieved November 18, 2021, from The Guardian: <https://www.theguardian.com/media/2010/mar/23/google-louis-vuitton-search-ads>
- Techopedia. *Techopedia Explains Real-Time Blackhole List (RBL)*. Retrieved November 23, 2021, from Techopedia: <https://www.techopedia.com/definition/25294/real-time-blackhole-list-rbl>
- U.S. Congress. (1791, December 15). *First Amendment*. Retrieved November 18, 2021, from Legal Information Institute | U.S. Constitution: https://www.law.cornell.edu/constitution/first_amendment
- U.S. Congress. (1952, July 19). *35 U.S. Code Title 35—PATENTS*. Retrieved November 19, 2021, from Legal Information Institute | U.S. Code: <https://www.law.cornell.edu/uscode/text/35>
- U.S. Congress. (1956, July 11). *18 U.S. Code § 1343 - Fraud by Wire, Radio, or Television*. Retrieved November 16, 2021, from Legal Information Institute | U. S. Code | Title 18 | Part I | Chapter 63 | § 1343: <https://www.law.cornell.edu/uscode/text/18/1343>
- U.S. Congress. (1986, October 16). *18 U.S. Code § 1030 - Fraud and Related Activity in Connection With Computers*. Retrieved November 16, 2021, from Legal Information Institute | U.S. Code | Title 18 | Part I | Chapter 47 | § 1030: <https://www.law.cornell.edu/uscode/text/18/1030>
- U.S. Congress. (1986, n/a n/a). *Electronic Communications Privacy Act of 1986 (ECPA)*. Retrieved November 17, 2021, from U.S. Department of Justice | Office of Justice Programs | Justice Information Sharing | Privacy And Civil Liberties | Federa; Authorities | Statutes: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285>
- U.S. Congress. (2000, December 19). *18 U.S. Code CHAPTER 41—EXTORTION AND THREATS*. Retrieved November 17, 2021, from Legal Information Institute | U.S. Code | Title 18 | Part I.: <https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter41&edition=prelim#>
- U.S. Congress. (2006, January 6). *10 U.S. Code § 888 - Art. 88. Contempt toward officials*. Retrieved November 18, 2021, from Legal Information Institute | U.S. Code | Subtitle A | Part II | Chapter 47 | Subchapter X: <https://www.law.cornell.edu/uscode/text/10/888>

- U.S. Court of Appeals, Ninth Circuit. (2008, November 5). *ENTERTAINMENT 2000 INC v. ROCK STAR VIDEOS INC MMM*. Retrieved November 18, 2021, from FindLaw | Caselaw | United States | US 9th Cir.: <https://caselaw.findlaw.com/us-9th-circuit/1485435.html>
- U.S. Congress. (2008, October 13). *18 U.S. Code CHAPTER 110—SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN*. Retrieved November 17, 2021, from Legal Information Institute | U.S. Code | Title 18 | Part I: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-110>
- U.S. District Court, C.D. California. (2006, July 28). *Summaries of ESS Entertainment 2000, Inc. v. Rock Star Videos, Inc.* Retrieved November 18, 2021, from Casetext | Summaries: <https://casetext.com/case/ess-entertainment-v-rock-star-videos/case-summaries>
- van Zuylen-Wood, S. (2018, January 11). *How Robo-Callers Outwitted the Government and Completely Wrecked the Do Not Call list*. Retrieved November 23, 2021, from Washington Post: https://www.washingtonpost.com/lifestyle/magazine/how-robo-call-moguls-outwitted-the-government-and-completely-wrecked-the-do-not-call-list/2018/01/09/52c769b6-df7a-11e7-bbd0-9dfb2e37492a_story.html
- Viener, A. (2005, February 8). *Louis Vuitton vs Google*. Retrieved November 18, 2021, from CORANTE | Weblog Columns | GoYaMi: https://web.archive.org/web/20060316165559/http://goyami.corante.com/archives/2005/02/08/louis_vuitton_vs_google.php
- Ward, M. (2021, October 17). *Facebook May Identify Trolls in Defamation Cases*. Retrieved February 28, 2024 Financial Review: <https://www.afr.com/companies/media-and-marketing/facebook-may-identify-trolls-in-defamation-cases-20211017-p590ls>
- Warren, A. M. (2021, February 11). Free speech and expression in the 2021 workplace. *The National Law Review*, 11(322), p. n/a. Retrieved November 18, 2021, from <https://www.natlawreview.com/article/free-speech-and-expression-2021-workplace>
- Wayner, P. (2000, February 28). *How to make friends, influence hackers, and build bugfree code Paris style*. Retrieved November 29, 2021, from Risks Digest: <https://catless.ncl.ac.uk/Risks/20/82#subj2>
- White, G. (2020, September 12). *The 20-Year Hunt for the Man Behind the Love Bug Virus*. Retrieved November 17, 2021, from WIRED | Backchannel: <https://www.wired.com/story/the-20-year-hunt-for-the-man-behind-the-love-bug-virus/>
- Wientzen, H. R. (2003, August 16). *Tackling the Spam Issue: The DMA's Answers to One of the Nation's Toughest Questions*. Retrieved November 23, 2021, from The Direct Marketing Association: <https://web.archive.org/web/20030816012126/http://www.the-dma.org/membersguide/tacklingspam.shtml>
- Wired Staff. (2000, June 29). *Suspect Charged in Love Bug Case*. Retrieved November 17, 2021, from WIRED | Security: <https://www.wired.com/2000/06/suspect-charged-in-love-bug-case/>
- World Intellectual Property Organization. (n/a, n/a n/a). *What Is Intellectual Property?* Retrieved November 24, 2021, from WIPO: <https://www.wipo.int/about-ip/en/>
- Zeigler, S. L. (2009, n/a n/a). *Communications Decency Act of 1996 (1996)*. Retrieved November 17, 2021, from The First Amendment Encyclopedia: <https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996>

17 Protecting Your Organization's Reputation in Cyberspace

The Internet offers organizations exciting opportunities to find timely information and to reach potential clients. This very power brings with it risks of damaging corporate and professional reputations. Non-technical problems in cyberspace include relying on or propagating bad information, violating the conventions of proper behavior established by custom in cyberspace, and outright fraud.

This chapter reviews

- Corporate policies for avoiding embarrassment, lawsuits, and criminal prosecution.
- Policies for professional standards in email.

I first started using email in 1981 at work, when I was a systems engineer for *HP Canada*. In the early 1980s, email was restricted mostly to businesses and academic users; a few thousand individuals exchanged messages through *bulletin-board systems* (BBSs), and there were various schemes for mail relay among BBSs and *value-added networks* (VANS) such as *Prodigy* and *CompuServe*. Basically, amateurs did not have much exposure to electronic communications.

In contrast, today billions of people use email¹, many having grown up using email, chat rooms, and news groups from their childhood or youth, quite apart from businesses and formal organizations. Because of the rapid rise of these high-tech communications media, there has been a rupture in civility. There is a disjunction between the customs of civility and courtesy that were defined for earlier generations in terms of speech, telephone, and written communications and the habits of a couple of generations who have developed their own style almost free of guidance from older people.²

There is nothing unusual about different modes of communication for different contexts; conversational spoken language, for example, sounds quite different from the formal speech of conferences or the structured writing of an article.

Speech between two long-married people, for example, is highly idiosyncratic. A good marriage is like a conversation that never ends, but the conversation becomes quite peculiar after a while. I remember my wife's and my amusement when we heard a recording, we accidentally made during a car trip: it sounded completely off the wall ["Is that surprising?" I imagine some of you thinking] with sentence fragments, long companionable pauses, code words (e.g., "Do I have baboons?" "No, you have no baboons."), resumption of topics many minutes later as if there had been no intervening content, and a general lack of any obvious structure.

From a business point of view, however, some of the people most comfortable with electronic communications have developed some bad habits. This section serves as a guide to standards of appropriate behavior when employees are communicating online.

BAD INFORMATION

The first issue with Net-based information is that some of it is just plain wrong (i.e., misinformation or MISINFO) even when it is first posted. As discussed in the section on violations of data integrity, the Internet provides access not only to responsible professionals, mature children and adults

REPUTATION



FIGURE 17.1

Reputation can be damaged.

but also to incompetents, immature people, rumor-mongers, and lunatics. Worse still, some postings are from anonymous people or from people using pseudonyms. Far from taking Net-based information at face value, we should be skeptical about unsubstantiated claims on the Net. News media and legally constituted organizations have much to lose by publishing errors, lies and rumors unless they are deliberately and consciously supporting autocratic, undemocratic movements; untraceable individuals can spread falsehood with few consequences.

In *corporate* communications, it is essential that everyone be trained to *check the credibility* of information they may want to circulate within the organization. Even more critical is for *no one* to post or distribute information which may be traced to the organization unless it has been carefully verified by appropriate officers of the organization. Posting nonsense on social media by individuals using accounts that can be traced to an employer or an association can lead to public-relations disasters.



FIGURE 17.2

Don't spread
MISINFO!

VIOLATING NETIQUETTE

When we post information to the Net, we normally indicate who we are (electronically) in our message headers. In particular, all employees using a corporate email account identify their employer in every posting. It follows that when an employee (joe@acme.com) misbehaves on the Net, it's likely that everyone seeing the misbehavior will associate it with the employer, regardless of futile attempts to dissociate the employee from the employer (e.g., "The opinions above are not necessarily those of my employer").

In brief, employees can embarrass their employers by using their corporate email service in many ways such as



FIGURE 17.3

Manners matter.

- *Flaming*: Launching rude verbal attacks on others.
- *Flooding*: Sending copies of a message to multiple (and often unrelated) discussion groups and mailing lists.
- Sending junk email with unsolicited advertising and sales promotions to people's email addresses without their permission.
- *Mail-bombing*: Sending many email messages (often rude or obscene) to a single email address to annoy the victim.
- Posting or sending astounding or astonishing misinformation without bothering to see if it's true or accurate.
- Sharing offensive information (nude pics of a drunk neighbor).
- Posting other people's information without their permission.
- Never removing old parts of an email discussion from a reply (resulting in three months of comments spanning 40 pages of text from 18 different people).

All such violations of *netiquette*³ should be explicitly forbidden by corporate Internet-usage policies. Corporate training should include exercises for identifying and preventing such violations of professionalism in email.

ILL-ADVISED EMAIL

There have been too many cases of foolish use of email in recent years. Employees have caused a hostile working environment by sending internal email with lewd or hateful jokes and images; staff members have insulted their bosses or their employees in email that later became public; people have made libelous accusations about other workers or about competing companies. All of these uses are wholly inappropriate for a medium that removes control over distribution out of the hands of the originators, that can usually be read by technical staff, and that usually gets backed up and archived for indefinite periods of possible retrieval and unauthorized distribution.

As a striking example of the consequences of foolish postings, in February 2013, an 18-year-old online gaming enthusiast called Justin Carter responded to insulting remarks in a Facebook posting that questioned his sanity. He responded that he would shoot children in kindergarten and eat a victim's heart.

Another Facebook user reported Carter to local police in his hometown in Texas. Local police arrested him for "making a terroristic threat" and locked him up from February 14 until March 13, which is when he was first questioned about his comment. After five years of legal proceedings, he finally accepted a plea deal and was released from jail.⁴ Can you imagine the consequences if this twit had been an employee with an identifiable link to an employer?

Common sense dictates that anything you send in email should not be illegal or even embarrassing were it widely known. One commentator listed "11 things never to send over work email." The list included:

- Huge videos
- Stupid chain letters threatening disaster unless they are forwarded immediately
- Inappropriate "humor" such as racist and sexist jokes
- Confidential or classified information
- Animated GIFs
- Gossip
- One's job applications to potential employers (!)
- Pornography
- Announcements that a specific employee has been fired (or that a mass dismissal is in progress)
- Anything requiring extensive face-to-face discussion
- Criticism of specific people⁵

INAPPROPRIATE USE OF CORPORATE IDENTIFIERS

In addition, and more controversially, I believe that corporate policy should forbid the use of corporate IDs for any *personal* use in some sectors of the Internet. Most professionals, for example, have no business posting messages to news groups in the *alt* hierarchy, and especially not in groups catering to or sympathetic to criminal activity. It seems to me that if employees of an organization want to participate in vigorous political discussion, conversations about sexual activity, and any other topic unrelated to our work, they are free to do so using their own Internet identities. Employers pay for corporate email identities; people who want to post opinions about, say, basket weaving techniques should pay for their own access and leave their employer out of their postings.



FIGURE 17.4

Stupidity isn't good
for employers.



FIGURE 17.5

Will the employer
benefit – or suffer?

The risks of damaging an organization's reputation by violating netiquette are high. Some abusers have themselves been abused by angry and unscrupulous Internauts. In one notorious early case, back in 1994, a naive executive spammed the Net – he posted messages in a couple of dozen newsgroups. In retaliation, his company's 800-number was posted to phone-sex discussion groups in the *alt* hierarchy, resulting in thousands of irate and expensive phone calls by seekers of, ah, aural sex. Regular customers were unable to get through and some staff resigned because of the offensive calls. The executive nearly lost his job.

Employers cannot, however, block employees from posting whatever they want on social media *on their own time* even if the employer is being identified. A legal-advice site explains,

Section 7 of the National Labor Relations Act (the Act) guarantees employees “the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection,” as well as the right “to refrain from any or all such activities.”

Section 8(a)(1) of the Act makes it an unfair labor practice for an employer “to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7” of the Act.

....

While at first glance it may seem that the Act has nothing to do with social media, in fact, an employer's attempt to curtail an employee's social media activity or comments can be a violation of the Act if it is determined that the statements posted on social media are part of “concerted activity” for “mutual protection.”

For example, Section 7 of the Act allows employees to criticize their employer or their working conditions, even if the criticism is inaccurate, and in some cases, even if it is abusive or defamatory. An employer cannot discipline or terminate an employee for making these statements and may not make a rule prohibiting employees from making these statements.

According to the National Labor Relations Board (NLRB), employers may not, “promulgate, maintain, or enforce work rules that reasonably tend to inhibit employees from exercising their rights under the Act.” Some corporate employee handbooks attempt to prohibit this kind of activity on the part of an employee by developing rules about what employees can or cannot post on their social media accounts. Employers should use caution or consult an attorney when including these rules as part of an employee handbook, since too many restrictions could be considered to violate the employee's rights under Section 7 of the Act.

However, the lawyers continue,

An employer does have the right to control what an employee does on the employer's time (i.e. during working hours) and with the employer's equipment. An employer also has a right to restrict employees from posting confidential information online, including trade secrets, customer information, and to prohibit posts that would threaten or harass other employees. An employer can prohibit employees from using the company's name, logo or other protected marks online, and can prohibit them from making false statements about the company.⁶

FRAUD

Some people in cyberspace are criminals – no surprise there. The danger for organizations is that it's easy to be dishonest in cyberspace. People get funny ideas sometimes; employees have been known to act as *shills*; that is, to pretend to be customers posting positive reviews on public discussion boards. Such dishonesty inevitably gets known; dishonest employees who think their employers are dishonest are unlikely to preserve silence after they try to trick victims into believing false claims of customer satisfaction.



FIGURE 17.6

Fraud isn't a good strategy.

Another nasty trick is to pretend to be a customer *dissatisfied* with a competitor's product or services. This won't work either and can easily lead to civil litigation.

In a recent case, Google sued a criminal,

...who perpetrated a coordinated campaign to deceive consumers and business owners by fraudulently attempting to manipulate our services for small businesses. As our lawsuit shows, this bad actor posted more than 350 fraudulent Business Profiles and tried to bolster them with more than 14,000 fake reviews. It then attempted to sell information about consumers who had been lured in through such false claims. While we detected and removed this deceptive content, we're taking proactive legal action to stop this bad actor from scamming other platforms and to protect our users.⁷

SPOOFING ORIGATION ADDRESSES

Any misrepresentation from employees of a publicly traded company or which causes artificial fluctuations in stock prices may fall afoul of U.S. *Securities and Exchange Commission* (SEC) (or their equivalent in other countries) regulations about market manipulation.⁸

Several U.S. states enacted laws making it a crime to use forged headers in email (*email spoofing*).⁹

Email spoofing is a growing problem and has unfortunately reached the point where you can't reliably trust the information associated with an email to tell you who actually sent the message. Malicious individuals commonly use email spoofing to hide the origin of an email message, in turn increasing the chances that you will respond, when sending out spam, phishing or malware laden emails. Unfortunately it is possible because the main protocol used in sending email (SMTP) does not include an authentication mechanism. The risks associated with spoofed emails range from being a nuisance to endangerment of personal safety. Some jurisdictions have enacted legislation against this form of email identity fraud, but many agree that this is a technical problem that calls for a technical solution.

....

At the time this article was written [2023], roughly 31 states have adopted legislation regulating spam and prohibiting spoofing. Many state anti-spam laws, such as those of Indiana, Illinois, Colorado and Washington explicitly prohibit the use of a third party's domain name or mail servers without the permission of the third party. Some states even go so far as to offer compensation to the wronged party. Illinois' statute generously offers both the ISP and the wronged person the right to recover both attorney's fees and costs incurred in a successful lawsuit, or the lesser of \$10 for each unsolicited illegal email transmitted, or \$25,000 per day.

In addition, the federal CAN-SPAM Act of 2003 makes it illegal to send unsolicited email with deceptive subject lines or false/misleading headers. However, the problem with such legislation is that spoofing conceals the identity of the sender and thus makes it very difficult to prosecute. Nevertheless, it doesn't hurt to report deceptive email to the Federal Trade Commission (FTC). The FTC has a special email address set up for receiving reports, uce@ftc.gov.¹⁰

In spite of general agreement about the criminality of spoofing, a shocking decision in 2008 by the *Virginia Supreme Court* ruled that fake email addresses are protected speech, even if used by criminals for fraud.¹¹

Any fraudulent email requesting the use of the USPS may be in violation of federal interstate mail-fraud laws.¹² On some occasions when I receive a chain email letter with mailing addresses for responding to a pyramid-sales fraud, I send copies to the Postmasters in each ZIP code requesting investigation and appropriate prosecution for mail fraud. It is easy to file a report of suspected crime involving U.S. Mail directly with the *Postal Inspection Service* of the USPS.¹³



FIGURE 17.7
Lying is frowned upon.

CHAIN-EMAIL PYRAMID FRAUD

As all network administrators know, there are many letters circulating around the Net which tout the miraculous successes of adding your name to a mailing list, sending \$5 (or whatever) to four other people, and sending the letter on to everyone you know. Some of the more recent letters include the claim “As seen on TV.” Many include letters from starry-eyed proponents of the scheme claiming that their kitchen tables have been covered with money within weeks of participating in the plan; several preface their comments with assurances that they normally throw away such letters, but this one has changed their lives.¹⁴

These letters are examples of pyramid frauds (also known as *Ponzi Schemes*); they are a method of funneling money from later participants to earlier participants. Eventually the fraud runs out of new victims and the last waves of participants are left with no revenue. Effectively, everyone participating in the pyramid fraud is hoping to reap unearned cash from gullible later victims.¹⁵

I sometimes report the U.S. participants in such fraud to the U.S. Postmasters in the ZIP codes involved (and no, I don’t have “far too much free time” – I just get irritated by fraud). Here is the exact text of a letter sent to me on 1 December 2000 by V. J. Bellinger of the *Operations Support Group* of the *U.S. Postal Inspection Service* in Newark, NJ. It has some interesting information that I hope will be helpful to readers attempting to convince employees (or family and friends) that such chain email involving postal addresses is illegal.

A chain letter or a multi-level marketing program is actionable under the *Postal Lottery, False Representation, and/or Mail Fraud Statutes* if it contains three elements: prize, consideration and chance. *Prize* is usually in the form of money, commissions, or something else of value that the solicitation claims you will receive. *Consideration* is the required payment to the sponsor in order to obtain the prize. *Chance* is determined by the activities of participants over whom the mailer has no control. These types of schemes constitute lotteries and are barred from the mails because they violate the following statutes: *Title 18, U.S. Code, Sections 1302 and 1341* and *Title 39, U.S. Code, Section 3005*.

In attempts to appear legal, many chain letter or multi-level marketing mailings offer, for a fee, a product or ‘report.’ However, since the success of the program is dependent on the number of people willing to participate, all three elements that constitute a violation continue to be present.

The promoter of this scheme has been advised of the potential violations involved and has been requested to discontinue this type of mailing activity....

In 2022, news exploded about the failure of the FTX cryptocurrency exchange, which had many elements of a Ponzi scheme:

Sam Bankman-Fried, who was once hailed as a virtuoso in cryptocurrency trading, is on trial over the collapse of FTX, the financial exchange he founded.

Bankman-Fried is accused of shuffling billions in customer funds from FTX into Alameda Research, a hedge fund he also founded.

....

The one-time crypto wunderkind faces seven counts, on fraud and conspiracy charges. Manhattan federal prosecutors allege that Bankman-Fried’s fraud ran from 2019 to November 2022, when FTX collapsed. The prosecution alleges that he “misappropriated and embezzled” FTX customers’ deposits and funneled “billions in stolen funds” to line his pockets and bankroll risky investments.



FIGURE 17.8 No, not THAT sort of pyramid!

They claim that the diverted funds propped up his luxe lifestyle. This “exorbitant spending unrelated” to FTX, they claim, covered his personal expenses — including more than \$200m in Bahamas real estate, wild investments, and to also repay entities that had loaned money to Alameda.

....

The failed crypto whiz faces a maximum 110 years behind prison if convicted on all counts.¹⁶

FRYING PAN AND FIRE: HOW NOT TO HANDLE Spam-FILTER FALSE POSITIVES

A troubling aspect of the deluge of spam we are all suffering is that antispam techniques can turn into DoS techniques if they are not handled properly. In 2004, I received a sad story bearing on this subject from a reader who asked to be kept anonymous for fear of repercussions if these comments were traced to him or her. The following is the reader's text with minor editorial changes.

I'd like to tell you about a problem we're facing with the way our administrators are handling false-positives in their anti-spam solution.

In March 2004 we had an average of 24,740 items of mail entering daily. Of these, 9,697 or 39% were identified as junk by the [name suppressed] appliance for spam filtering.

On average, there were complaints about 16 pieces of mail per day that were subsequently released as not junk. The system administrators calculated that the false-positive rate was 16 out of 9,697 or about 0.16%.

I disagree with the last statistic since most people don't realize that mail intended for them hasn't arrived. They don't even know that the email is being filtered because the email administrator made no announcement about the tool's implementation. I personally realized that something was wrong when many of the mailing lists I subscribe to vanished. It was only after a few weeks of lower activity in my mailbox that I realized that they had stopped arriving. I had people from abroad who correspond with me on a somewhat regular basis calling me asking why I didn't respond to their letter, to their reminder about the original letter, and to their second reminder! That was the way I found out that the filter was activated. And I am an IT senior staff member.

This product doesn't let the individual user go in and see the mail that has been classified as junk. You have to go and speak with the administrator if you think something didn't arrive. As a company with 11,000 users and multiple sites this is unrealistic.

It also doesn't let you have any individual control, like a personal blocking list. It doesn't let an employee set his own level for filtering. You either filter out all the mail for an individual or let it all flow into his mailbox. MSN Hotmail has a better setup for its millions of users. MSN Hotmail lets a user choose different levels of filtering; you can return letters to your inbox by yourself; and you can tell the filter that a particular letter is not junk for future reference.

The absolute worst thing was a comment by one of the IT managers in a recent management meeting when his response to my criticisms was, “If an employee doesn't know that he didn't get a letter then it means that it wasn't an important letter and he can do without it.”

PERSONAL LINKS ON A CORPORATE WEBSITE

When a friend of mine from another university was visiting many years ago, he told me about a peculiar situation at work.

His department was experiencing financial difficulties, so his department decided to reduce expenses by eliminating the extensive full-color brochure they had published for many years to entice students and parents into considering their program. Instead, they would publish a much simpler, less expensive brochure and put lots of exciting information on



FIGURE 17.9
Oops.



FIGURE 17.10
Links to personal pages.

the departmental website. This plan would also offer the opportunity for including links to each professor's personal webpage, where the faculty could post valuable and impressive materials such as their curriculum vitae, list of publications, photos, and so on.

Then he hit a brick wall.

The IT security officer at the university flatly disallowed all external links from the main departmental webpage. University policy precluded such links. "Why?" asked my friend. They would, said the security administrator, "compromise the security of the institutional website." And that was it: end of discussion. The impression was that the security officer would have said, "Go away and stop bothering me" had my friend not been a faculty member.

My friend asked me about the security implications of having external links. Was it true, he asked, that they could allow an attack on the university's website?

Well, no, not in the normal sense of the word "attack."

Hypertext transfer protocol (http) is a system for giving client systems (the computer running a browser) an address that can be translated into a numerical Internet Protocol (IP) address using the Domain Name System (DNS). An address in HTML is simply a string that is usually formatted in a particular way (e.g., underlined and in a particular color) according to the settings on the client system. As far as the website is concerned, an HTML page that contains only URLs is just a bunch of text.

Note that I am not discussing active content here; there are certainly ways to open holes in a website using URLs that are dynamically generated. For example, URLs that contain detailed information that are interpreted by the website as instructions or as user identification codes and authentication sequences can easily be abused from the outside. A specific example is some mailing list administrators' (or spammers') practice of giving members (or victims) URLs like this to remove themselves (or believe that they remove themselves) from the list:

<http://www.something-or-other.domain/account=12345abc8910>

People who are irritated by spammers have been known to generate lots of similar URLs and automatically cause mass removals from the lists using this vulnerability – that is, assuming that the link doesn't merely confirm the existence of the accounts!

INSULATION FROM EXTERNAL LINKS

However, a more serious issue is the possibility that someone will create a link from an official website (read: stuffy, reserved, decent) to an informal website (read: exciting, expansive, pornographic). I recall one security case I worked on in the 1990s in which a system administrator for a law firm had placed a link on from the official home page of the firm's website to his or her personal website; I say "his or her" because this person ("Jules") was male on Mondays, Wednesdays and Fridays and female ("Julie") on Tuesdays and Thursdays [I am not making this up]. I am not criticizing the administrator's personal lifestyle, since I have been supporting transgender rights for decades, but I do understand the law firm's partners' concern when they realized that their home page was exactly two clicks away from quite a number of, shall we say, *vivid* websites about transvestism and transgenderism.

I think there is a straightforward method for insulating the employer – academic institutions in particular – from the personal values of individual employees without having to forbid all links to personal webpages. Many websites, especially government sites, have automatic disclaimer pages that flash an announcement when one clicks on a hyperlink that points outside the site. For example, on the NIST site, there was once a list of links to academic institutions. The first link



FIGURE 17.11
Insulation.

happened to be for *George Mason University's Center for Security Information Systems*, whose URL (still) is:

< <http://csis.gmu.edu> >.

However, the link was embedded in another link as follows:

< http://www.nist.gov/cgi-bin/exit_nist.cgi?url=http://csis.gmu.edu >

and that link went to a page that included the following text:

Thank you for visiting. We hope your visit was informative and enjoyable.

We have provided a link to this site because it has information that may be of interest to our users. NIST does not necessarily endorse the views expressed or the facts presented on this site. Further, NIST does not endorse any commercial products that may be advertised or available on this site.

Click on the following link to go to:

<http://csis.gmu.edu>

(or you will be taken there in 15 seconds)

I think that this approach pretty well insulated the NIST site from the outside links, and I think that the same method can be used to insulate my friend's university from any problems resulting from their faculty members' personal proclivities as expressed on their websites.

A final note on this topic: at *Norwich University*, I established a website in 2000 as instructed by the IT group at:

www2.norwich.edu/mkabay

but when my site reached 10 GB in 2008, I was told to stop adding materials. It was then that I created:

www.mekabay.com

which at the time of writing has 34 GB of data in 7,892 files and 488 folders; it gets about a million unique visitors and two million pages opened per year. And in my totally biased opinion, it has nothing objectionable on it (except opinion pieces that offend bigots).

RECOGNIZING HOAXES

All of us have likely encountered a frantic email warning from a friend about some dreadful worm, virus, involuntary organ-donation, homicidal gang members who shoot helpful motorists and so on.

The more technically oriented warnings sent by friends or colleagues who know little about computing are often very funny; one famous hoax that was printed on April Fool's day during Operation Desert Storm claimed that a virus had been introduced into printer ROMs in printers being sent to Iraq. The virus would then supposedly crawl up the parallel cable and infect the CPU. Ironically, this joke was later taken seriously and printed in a mainstream news magazine as if it were not only possible but actually true.¹⁷



FIGURE 17.12
Recognizing hoaxes.

So what to do about this nonsense when some well-meaning soul passes it on to everyone on his or a mailing list?

One approach is simply to delete the junk and go on to other things. Unfortunately, this strategy fails to reduce the problem in any way. We are likely to continue receiving scare-stories from the same sources unless they come to understand the problem.

My own preference is to send a gentle explanation to my hot and bothered correspondent explaining how to recognize a hoax and where to get more information about them.

Here's a text I use to answer such messages with a couple of keystrokes (I've used text macros since the early 1980s). Please feel free to use your own version yourselves.

* * * A FRIENDLY MESSAGE ABOUT THE WARNING YOU JUST SENT ME * * *

The warning you have forwarded is a hoax. The danger is imaginary and the problem is nonexistent.

Security experts request that no one circulate unverified warnings of vague, alarming dangers.

Key indicators that a message is a hoax:

- Use of exclamation marks (no official warning uses them).
- Use of lots of uppercase text (typical of youngsters).
- Misspellings and bad grammar.
- No date of origination or expiration.
- References to official-sounding sources (e.g., microsoft, ciac, cert) but no URL for details.
- No valid digital signature from a known security organization.
- Requests to circulate widely (no such request is made in official documents).

Some guidelines for avoiding viruses and Trojan Horse programs:

- Always run a good antimalware program in background.
- Keep your antimalware strings up to date (e.g., at least daily or hourly automatic updates).
- Don't execute unknown software even if you know and like the person who went it to you.
- Don't forward executables – instead, provide the URL for the legitimate, trustworthy origin of the executable file.

In addition, before alerting anyone to apprehended threats, check SNOPEs < <https://www.snopes.com/> >, a reliable anti-hoax site on the Web.

USING EMAIL SAFELY AND WELL

When you receive an email message, do you care whether it has spelling mistakes and grammar mistakes? What about offensive language and off-color humor? Does the context matter? For example, do you apply the same standards to email referring to business matters and to informal communications about, say, a hobby or interest?

Researchers at the *University of Chicago* have been investigating the effects of email on perceptions of character. Psychologist Nicholas Epley and colleagues examined conversations carried out exchanges on conversational topics by phone between randomly selected people using six assigned questions. They then transcribed the answers and used them for the email version of the Q&A sessions.

Their results were interesting. The questioners had been given false biographical sketches of the people they were communicating with indicating substandard intelligence or normal intelligence as well as different pictures showing neat people or slob. Questionnaires who used the phone to listen to the prescribed responses had favorable impressions of their interlocutor's intelligence regardless of the bios and pictures. In contrast, via email, students held onto their first impressions, continuing to assume their partners had substandard intelligence, for example, if that's what the biographical sketch indicated.



FIGURE 17.13
Wholesome email practices.

One of the more widely touted advantages of computer mediated communication, and of email in particular, is its capacity as a socially “blind” medium. On the internet, no one knows whether you are white or black, male or female, rich or poor—features that allow inter-actants to express their “true selves” and increase the frequency of close relationships.... Yet, despite its potential as a social equalizer, the research presented here suggests that email can have the very opposite effect. When individuals interact over email with someone about whom they already have a stereotype, they are more, not less, likely to come away from the communication with those stereotypes still intact.¹⁸

Looking like an idiot is easy; correcting that impression via email may not be so easy. This section provides useful guidelines for not making fools of ourselves when we use email.

DISCRETION IN EMAIL COMMENTS

This section looks at awareness about email protocol and specifically discretion in sending off-the-cuff critical comments to someone via corporate email.

All of us encounter times where we disagree with something our colleagues are saying or doing; however, not every impulse to respond should lead to an official email. Those should be regarded as on-the-record communications that may be interpreted – and misinterpreted – by others in the organization who may jump to conclusions that are unwarranted.

Let's take a look at a scenario and analyze what's happening.

Albert sends Bob an email message addressed only to Bob. In it, Albert speculates about possible business strategies for their employer. Bob disagrees with his perception of the suggestion and writes a highly critical memo back to Albert using the company's email. However, it turns out that either through unclear writing from Albert or misunderstanding by Bob, the information and assumptions detailed in Bob's response can easily be viewed as indicating that Albert is undermining the interests of his own employer.

What are the possible sources of disagreement whenever people don't see eye to eye?

- They may differ in fundamental assumptions.
- Their vocabulary may differ: They use words differently.
- Their unspoken goals and values may differ.
- Their implicit reasoning may differ.
- They may lack essential shared information.
- They may have made a mistake in observation, reasoning, or articulation of their views.

What are some of the elements that lead to a perception of impoliteness in communications? In a 2008 book called *Impoliteness in Interaction*, the author analyzes elements of impoliteness using detailed records of less-than-pleasant interactions.¹⁹ In [Chapter 6](#), “The dynamics of impoliteness I,” he discussed several stages and levels of impoliteness. Elements he analyzes in detail include (examples are my own):

- *Pre-impoliteness sequences*: words and phrases that set the stage for aggressive or defensive speech; for example, “I'd like to ask you....” Or “Listen to me....”
- *Repetition of challenges*: rapid sequences of accusatory language that emphasizes hostility; for example, “Don't you think that.... Isn't it obvious that.... Why can't you see that....”
- *Insertion of taboo words*: obscenities, shocking images; for example, “Why the **** can't you see that....” or “What's the matter with you, you have your head stuck up your ****?”

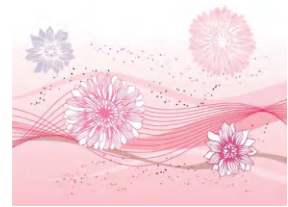


FIGURE 17.14
Be nice!

- *Derogatory nominations*: demeaning descriptions of the interlocutor or of ideas; for example, “You’re a real [insert insult here] sometimes” or “Well that idea is really off the wall.”
- *Forcing feedback*: demanding a response at the end of a hostile interaction; for example, “Why did you do that?” or “So what are you going to do about it?”

In my experience, many people don’t edit their email messages at all before sending them; some don’t even check their spelling. Under those circumstances, an email that seems like a collection of blurted-out insults can make any situation worse.

I think that any time we find ourselves starting to use hostile expressions in our email, it’s time to stop and think:

- Will this interaction contribute to solving a problem or will it make it worse?
- Would it be better to meet the interlocutor face to face instead of relying on email?
- Failing that, can we use a video link (e.g., Skype) to discuss the issue with a modicum of body-language that can clarify feelings instead of letting them be guessed from written, often poorly edited, spontaneous reactions in email?
- If video isn’t available, can we at least telephone the interlocutor or use voice over IP tools for the interaction? At least there will be verbal cues about the feelings involved.
- If none of the live-contact interactions are available, is instant messaging available, with its menus of emoticons that can provide clarification of emotional context – and lead to rapid interaction point by point instead of forcing a delayed response to an extensive message?

A true story from one of my students illustrates the danger of stupidly sending offensive remarks by email – especially in a **REPLY ALL**, as will be discussed later in this section. It seems that one of our Norwich students was an intern at a large company one summer when he and everyone else in the company received a message from the CEO of the company on the second day of the internship; the message included a question. A fellow intern – NOT a Norwich student! – wrote something along the lines of “That’s the stupidest question I’ve ever read” and hit **REPLY ALL**. He was fired that afternoon.

In my email client, I have a five-minute delay for every message sent; unless I force an immediate **SEND**, my email sits in an outbox for those few minutes before it gets sent. Those minutes of buffering have saved me from errors of content and of judgment; perhaps an appropriate delay will be useful for you too.

Another (risky) trick I use for fun is that sometimes I deliberately write a horrible, insulting and funny response to a message, laugh about it, and then immediately delete it *before* it is sent. The automatic send-delay ensures that the insulting response does not get out even if I accidentally hit **SEND**—as long as I remember to cancel the **SEND** in time! **GMAIL** allows you to *unsend* a message if you are quick enough.

Think carefully about the responses your message will elicit; work for collaboration and cooperation, not conflict by default. The cardinal rule I have used for decades is, *If you’re angry, don’t send the email until you’ve cooled down.*

TO AND CC + **REPLY ALL** = TROUBLE

One day a nice lady in the *Human Resources* department at my university sent out a note to a dozen people reminding us that we had not yet finished signing up for our new medical-insurance coverage.

Unfortunately, she put all the email addresses into the **CC** (*carbon copy*, which is a term younger readers will have to look up) field where they were visible to everyone in the list. Predictably,



FIGURE 17.15

Don’t cause mailstorms.

someone on the list composed a response to her, unthinkingly hit REPLY ALL and sent some mildly personal information about the state of her medical concerns to all the recipients on the original list, none of whom cared a whit about her problems.

Luckily, there wasn't much that was very private in that message, but it did prompt me to write to the head of Human Resources about the incident. Part of my message was as follows:

- Many people unthinkingly use the TO and CC fields for addresses in distribution lists.
- Many people unthinkingly use REPLY ALL for replies and unknowingly send their comments to everyone listed in the email message's visible distribution lists.

The combination can lead to embarrassing violations of confidentiality; when the HR department staff use CC instead of BCC (the BLIND CARBON COPY function that conceals the distribution list), the REPLY ALL function can inadvertently violate privacy.

In this case, there was no particularly sensitive material revealed, but a different case could easily violate HIPAA (Health Information Portability and Accountability Act) and the University's rules on employee confidentiality.

I'm sure that once your colleagues understand the issue, they will learn not to use CC for distribution lists when the intention is to communicate with individuals; by default, all of us should use the BCC list unless we need to stimulate group discussion of an issue or it's important for the members of the group to know who received the message.

It's important that we not dismiss this issue as too easy or too obvious to bother with. "Against stupidity, the gods themselves contend in vain," wrote Friedrich Schiller in his "Maid of Orleans" (*Die Jungfrau von Orleans*) in 1801.²⁰ Nonetheless, the CC + REPLY ALL habit becomes a covert channel for release of confidential information for people who refuse to keep an address book and simply look up any old email and REPLY ALL to it as a lazy way of sending a new message.

If you doubt the seriousness of the problem, I suggest you look through your own archives of email and count how many obvious cases there are of emails with inappropriate subject fields and inappropriate distribution lists sitting in your received-folders. I think you will be dismayed by the results of your research.

BCC PREVENTS EMAIL NUISANCES

In the previous section, I presented an example of careless or ignorance that can bypass technical security. I pointed out that combining the unthinking use of REPLY ALL with visible distribution lists from a CC field can lead to violations of privacy even inside an organization. In this section, I want to finish my discussion with a few more points about the dangers of using visible distribution lists.

The problems caused by CC are worse when the recipients *do not know each other*. I have often received messages from technically unsophisticated correspondents who put dozens of email addresses in the CC field even though many of the recipients are total strangers to each other. Such exposure of email addresses always makes me nervous; who knows whether everyone on the list is trustworthy? Even if the list is not misused for outright spam, people often REPLY ALL with what I consider useless information, effectively adding me to a discussion list that I never wanted to be on.

One particularly annoying habit is to REPLY ALL with a joke stemming from some initial message. People then generate a series of increasingly long messages including copies of all the previous copies of the ostensibly clever repartee, driving me to generate an addition to my junk mail filter.

In one embarrassing case I was personally involved in, I added a new course developer to my MSIA faculty list and put the list name in the CC field by mistake in an all-points-bulletin. To my

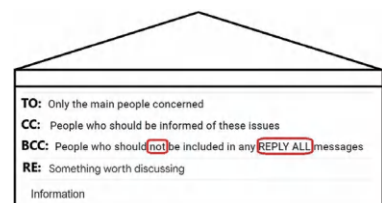


FIGURE 17.16

Use BCC to reduce mailstorms.

horror, the course developer cheerfully added my faculty members to a newsletter without permission. You can imagine the repercussions; there were two red faces that day and apologies to everyone.

The habit of using REPLY ALL is annoying enough when a reply does not in fact have to go to everyone on the original distribution list. However, REPLY ALL is a positive menace if it is coupled with the abhorrent practice of using an existing email message as a shortcut to creating a new one with a completely different topic. Not only do many lazy users fail to modify the original message subject – thus running the risk of having their new message ignored or filtered or misfiled – but they may easily send sensitive information to the wrong people. This sloppy use of email can result in gross violations of confidentiality.

So remember:

- TO— field for people directly involved in the correspondence and to whom replies are required for action or response.
- CC— field for people who need to know about the correspondence and to whom replies are helpful but who are not expected to respond unless they have specific information or comments.
- BCC— for people who need to receive a widely distributed announcement but who should not receive commentary sent back to the originator(s) of the original message.
- Remove unnecessary information (such as chains of previous correspondence) from a message to which you are replying or which you are forwarding before sending it.

In conclusion, you may want to put a note in your corporate-security newsletter about the proper use of CC and BCC fields the next time you're casting about for a topic.

BURYING YOUR EMAIL MESSAGE

As the end of the semester rolled around at Norwich University one year, my special-topics students were busily sending their examining committees their final reports. One lad – let's call him "Albert Baker" – noted that he was re-sending his report because one of his examiners mentioned that he hadn't received it; the student apologized for possible duplicates.

I responded that I hadn't seen it either.

An hour later, I opened an email message from a sender I didn't recognize; albert@biepald.com (all names and addresses have been changed to nonexistent ones). The topic was "C'est fini" or "it's done" in French. I had left this message in my in-basket for most of the day because I always open messages with obvious subject fields and from people I know before dealing with reader correspondence, messages from strangers, or possible junk email.

The mysterious message turned out to be from Albert and included the missing report. Had he sent it from his Norwich account, which would be bakera@norwich.edu, or at least included his real name, I would have opened it sooner. Had he used a meaningful subject field, such as "IS406 Final Report," it wouldn't have sat there unopened for so long.

This incident got me thinking about the current overload of email that so many of us are suffering and what it means for effective use of this communications channel.

From a security standpoint, sending email that doesn't get opened is a breach of security: it violates the principle of utility. What's the use of sending a message that gets ignored? Or at least, that gets ignored longer than it should? That slowdown could also be viewed as a breach of availability of the message.



FIGURE 17.17

Don't bury your emails!

So here are some simple suggestions that you can circulate among your colleagues in your next newsletter to help improve the usefulness and timeliness of email that matters – by which I mean email that is work-related and needs a response:

- **Configure your email client to include your real name, not a blank or a pseudonym.** Your email address is usually assigned by your organization's IT department following strict policies; however, if you are using private email, be sure that you use an email address a bit more descriptive than, say, bob123@gmail.net.
- **Use a meaningful subject field.** Don't be cute: "Something sweet for you" is more likely to be dumped in the spam/porn receptacle than opened in these days of swarming unwanted email.
- **Don't use the FORWARD or REPLY function of your email to start a completely new topic without changing the SUBJECT field.** Especially if the topic you've been discussing is low priority and your subject field just continues using that string instead of indicating a new, more important topic, don't be surprised if some of your recipients assign low priority to your new message, too. It can be disconcerting to open a message apparently discussing, say, "Refund policy for out-of-town expenses" and discover that it's actually dealing with what should have been labeled, "Emergency employee meeting called for 15:00 today" – especially when you open the message the day after the meeting.
- **Be modest.** Not everything you say or find interesting is worth sending to everyone you know. Contrary to the apparent belief of some egoists, their colleagues do not in fact sing Sting's *Every breath you take* song²¹ as they wait expectantly for the next "Me too" or "Yeah! Right on! You go, girl!" comment appended to 12 pages of copies of copies of copies of some two-week old message they've already seen 32 times. Send too much junk and all your mail will be relegated to the virtual dust bin.

This last point bears a little elaboration. At one point, someone in my university decided to send the entire faculty a "Thought for the Day" consisting of a cute quotation. Well, I pretty quickly added that person's email address to my "PLACE IN JUNK EMAIL FOLDER" filter. Unfortunately, the same person was responsible for sending out faculty notices that really did matter, so I ended up having to check all this rubbish anyway. Someone must have complained, because the junk did eventually stop.

In general, don't block a colleague's email address; if you are getting flooded with trivia, politely ask to be removed from that *particular* mailing list.

OK, now if this section were part of a junk email, it would end "SEND THIS TO EVERYONE YOU KNOW!!!!"

But it isn't (I hope).

MISLEADING SUBJECT FIELDS

Another problem with mislabeled subjects occurs when someone embeds more than one distinct topic in an email message whose subject field implies otherwise. For example, suppose an email message subject reads "Next week's meeting" but the sender *includes* an urgent request for action today on some critical issue; there's a good chance the receiver may not open the message right away if other messages seem more important.

Try to make your subject field as descriptive as possible without turning it into a paragraph. Some email systems truncate subject fields in the display of messages that a user sees; it makes sense to put keywords at the front of the subject. I encouraged my graduate-program staff to use prefixes such as "MSIA:" or "ACCREDITATION:" to help organize our messages.

Using standard formats in subject fields can help, too. For example, in our work in the MSIA, I asked that faculty and staff referring to an issue in a particular seminar use the form "MSIA c.s" in

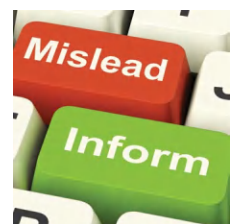


FIGURE 17.18

Use accurate subjects.

their subject field, where *c* represents the class (e.g., 7 for students starting in September 2005) and *s* represents the seminar number (thus MSIA 7.3 for seminar 3 in the MSIA 7 class).

I asked my undergraduate students always to start their emails to me using the class ID (e.g., CS120) so that I didn't have to look up which class they were referring to. That practice also allowed me to grab a bunch of messages from my INBOX and file them all in the appropriate course folder in one operation.

In summary,

- Use an appropriate agreed-upon prefix in the SUBJECT if possible.
- Use a properly descriptive SUBJECT field.
- Don't REPLY to an old message on a different topic and then leave the old SUBJECT and a copy of the original message.
- Don't mix separate topics in a single message.

EMAIL DISCLAIMER STIMULATES EXPLETIVES

One year, I received a 30-word email message from a very nice reader in Britain and noticed that his email system added the following astonishing disclaimer, which I quote in its sonorous totality after scrubbing it of identifying details:

This email, its contents and any files or attachments transmitted with it are intended solely for the addressee(s) and may be legally privileged and/or confidential. Access by any other party is unauthorized without the express written permission of the sender.

If you have received this email in error you may not copy or use the contents, files, attachments or information in any way nor disclose the same to any other person. Please destroy it and contact the sender on the number printed above, via the <Name of Bank> switchboard on +44 (0) nnnn nnnnnn for <place1> and + 44 (0) nnnn nnnnnn for <place2> or via email by return.

Internet communications are not secure unless protected using strong cryptography. This email has been prepared using information believed by the author to be reliable and accurate, but <Name of Bank> makes no warranty or representation, express or implied, as to its accuracy or completeness and is not liable to you or to anyone else for any loss or damage in connection with any transmission sent by the Bank to you over the Internet. <Name of Bank> makes no warranty that any information or material is free from any defects or viruses.

In particular <Name of Bank> does not accept responsibility for changes made to this email after it was sent. If you suspect that this email may have been amended or intercepted, please contact the sender in the manner stated above. If this transmission includes files or attachments, please ensure that they are opened within the relevant application to ensure full receipt. If you experience difficulties, please refer back to the sender in the manner stated above.

Any opinions expressed in this transmission are those of the author and do not necessarily reflect the opinions of the Bank and may be subject to change without notice.

Please note that for the purposes of this document all references to <Name of Bank> or the Bank shall be taken to mean <Name of Bank> (place) Limited or any other member of the <Bigger> Bank Group. Nothing in this transmission shall or shall be deemed to constitute an offer or acceptance of an offer or otherwise have the effect of forming a contract by electronic communication.

I commented in my response to my correspondent,

Did you know that your message has 30 words (152 bytes including spaces) whereas your disclaimer has 367 words (2177 bytes)? That's the lowest signal-to-noise ratio (6.5% useful info out of the total and a



FIGURE 17.19

Excessive disclaimers.

72.6:1::noise:signal ratio) I've ever seen outside a copy-of-copy-of-copy REPLY chain. Please congratulate your attorneys on making maximal use of bandwidth!

Really, this disclaimer does seem excessively detailed to me. If the same level of legalistic caution were applied to phone calls, it would make a wonderful Monty-Pythonesque skit:

"OK then, I'll see you at lunch tomorrow."

"Yep, but wait – you have to listen to the automated legal disclaimer our attorneys have programmed into our phone system. Just hang on [buzz, click]. [metallic voice] This phone message is intended solely for the recipient(s) and may be legally privileged and/or...." [CLICK!]

Or what about introducing this degree of caution into face-to-face interactions?

"So how do you want your hot-dog, with mustard and relish or without?"

"With both, please. And this verbal instruction is intended solely for the recipient(s) and may be legally privileged and/or...."

On a more serious level, cluttering up email messages this way is a waste of bandwidth. It's worse in offices where people copy entire messages without editing the contents, resulting in copy-of-copy-of-copy chains that spread like diarrhea through inboxes throughout the organization. I have personally seen messages that are 20 levels deep, all of them including the headers, salutations, copies of previous messages and disclaimers in a long string of garbage contributing nothing whatever to enlightened discourse. Some well-meaning folks even include the detailed headers in their copies.

As a matter of courtesy and good sense, when one replies to a message, it's a simple matter to strip non-essentials out of the copy of the original. I use ellipses (... for cuts within a sentence, ... for cuts crossing sentence boundaries) to signal gaps, but usually one or two snips are enough to clean up the copy so that the reader can get the gist of the conversation without having to wade through reams of superfluous stuff.

So the next time you encounter a huge disclaimer laid like an unsightly pile of refuse at the bottom of a colleague's email message, you can use a slightly modified British expression in your response: "UNSTUFF IT!"

FORWARDING CORPORATE EMAIL

A reader from Singapore wrote,

I would like to know what are your views on email forwarding; i.e., should staff be allowed to forward mails to their external accounts (Internet mail accounts)? I work in a hospital and I have request from Doctors who asked that the auto-forward feature of their Lotus Notes email messages be enabled to forward their email to their external Internet mail account so that they can read it while at home or overseas. There were some security concerns here that confidential mails would then end up circulating in the Internet.



FIGURE 17.20

Be careful when forwarding.

This question forces us to confront the conflict between theory and practice. Email and other traffic on the Internet has no inherent confidentiality. In theory, anyone capable of intercepting TCP/IP packets anywhere during transmission can breach confidentiality. Thus, again in theory, anyone

with access to the equipment of ISPs, Internet backbone transmission lines, and even to the public switched telephone network can intercept packets. With downlink footprints from satellite relays amounting to square miles, practically anything can in theory be intercepted from much of the traffic circulating on the Internet.

However, in practice, reported breaches of confidentiality have almost all resulted from data access at the end points, not in transit. Insider attacks and breaches of server security have been responsible for most of the data interceptions that have reached the press and the courts.

A practical impediment to effective interception of meaningful data in transit is the datagram routing that underlies the Internet: datagrams are packets of information with origin and destination information; store-and-forward transmission allows these datagrams to be sent through the Internet via different routes from other packets in a message stream. Routing tables can be updated in real time to reflect changes in traffic density or availability of specific links to other destinations on the Internet, so there is no guarantee that packets from the same message will travel the same route or arrive in the proper sequence (sequence numbers allow reassembly of the original message). Therefore, seizing individual packets at random anywhere other than the origin and destination of packets is unlikely to result in very much result for the effort.

Nonetheless, best practices do recommend that encryption be used for communication of sensitive data; therefore, many organizations install *Virtual Private Networks* (VPN) for communication with established trading partners. VPN software is also available for “tunneling” through the Internet from a remote workstation over non-secure communications lines. A simple example of such a link-encryption function is the Web-based email services that use SSL to establish a secure link to the email server (i.e., they use HTTPS instead of just plain HTTP). The user can pick up email from the corporate server without having it forwarded in the clear to an insecure external email service. Some of the email products include facilities for direct communication between a secure email server and the users’ email clients.

Using *VPN tunneling software* as a search string in the GOOGLE search engine at the time of writing brought up about two million hits, many of them for specific products and data sheets, so I am sure you will be able to find a solution that fits your needs.

In your specific case, the fact that some of the email might include confidential patient data means that the relatively modest investment in VPN technology would make a lot of sense for you in complying with your local legal requirements for protecting such data. But once you have the VPN in place, please make sure that all your users have also implemented driver-level data encryption on their computers so that the received, decrypted data are not susceptible to discover if someone steals their laptop or home computer.

Finally, this entire problem is eliminated (in theory) when the organization’s policy explicitly forbids accessing corporate emails (or for that matter, any internal information) using a non-employee email identity. The IT or security staff must then monitor log files regularly to identify violations of this policy.

EMAILWARE

One morning two decades ago I received a bounce for an email that I didn’t send.

Now, partly because I don’t like opening potentially executable code automatically, I don’t use HTML-enabled email, so it is not feasible for a worm to launch infected messages from my system; in addition, my *BitDefender*²² security system is automatically updated, so it’s unlikely that I would be infected. Finally, I don’t open unexpected attachments in native (executable) mode: at the



FIGURE 17.21
Fraud.

time, I used a utility (*Keyview*²³) to examine the content as text. So this is what I saw in the text of the “bounced” message:

```
Date: 9 May 2002 16:36:40 +0800
-RuADZVmR31l68x591fL6
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable
<HTML><HEAD></HEAD><BODY>
<FONT>The following mail can't be sent to
chnserv@globalsources.com:<br>
<br>
From: mkabay@compuserve.com<br>
To: chnserv@globalsources.com<br>
Subject: how are you<br>
The file is the original mail</FONT></BODY></HTML>
-RuADZVmR31l68x591fL6
Content-Type: application/octet-stream;
name=most.exe
Content-Transfer-Encoding: base64
Content-ID: <T57z06Z4>
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAA
.... 8>= [SNIP] ....
```

Hmm, I have never had < mkabay@compuserve.com > as an email account; I hadn't sent any messages with subject “How are you;” there is no one in China (.cn) that I've written to recently, and I block all unknown writers from most top-level international domains involved in heavy spam-generation (e.g., .cn, .ru, and so on) anyway. So, prima facie, this is likely to be a forged header. Sure, enough the free tool *Sam Spade*²⁴ revealed the offender:

```
* * * HEADER ANALYSIS USING SAMSPADE v1.14 * * *
Sender: wangjl@dsp.ac.cn
Received: from dsp-ns.dsp.ac.cn ([159.226.219.1]) by
siaaglaa.compuserve.com (8.9.3/8.9.3/SUN-1.12) with ESMTP
id EAA18353 for <mkabay@compuserve.com>; Thu, 9 May 2002
04:07:45 -0400 (EDT)
This received header was added by your mailserver
siaaglaa.compuserve.com received this from someone claiming
to be dsp-ns.dsp.ac.cn
This host doesn't exist, so all headers below this one
are probably forged
Received: from Uhpooz ([159.226.219.34]) by
dsp-ns.dsp.ac.cn with Microsoft SMTPSVC(5.0.2195.2966);
Thu, 9 May 2002 16:36:40 +0800
dsp-ns.dsp.ac.cn received this from someone claiming
to be Uhpooz
This host doesn't exist, so all headers below this one
are probably forged
From: postmaster <postmaster@compuserve.com>
To: mkabay@compuserve.com
Subject: Returned mail-"how are you"
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary=RuADZVmR31l68x591fL6
Message-ID: <DSP-NSNYgEj4v5iJarn00000cfb@dsp-ns.dsp.ac.cn>
X-OriginalArrivalTime: 09 May 2002 08:36:40.0549 (UTC)
FILETIME=[A408E150:01C1F734]
Date: 9 May 2002 16:36:40 +0800
```

Many other worms use misleading subject fields; for example, the *Melissa.I* variant of the notorious *Melissa* worm²⁵ used any of eight different subject fields:

- Question for you
- Check this!
- Cool Web Sites
- 80mb Free Web Space!
- Cheap Software
- Cheap Hardware
- Free Music
- Free Downloads

SIRCAM went one better (OK, worse) by using the name of the attached infected document (minus the file suffix), thus providing an infinite variety of subject fields.²⁶

Finally, a quick note on a curious reversal of the well-known hoax warnings that circulated years ago such as the following:

There is a new virus going arround [sic] in the last couple of days!!! DO NOT open or even look at any mail that you get thar [sic] says: "Returned or Unable to Deliver" This virus will attach itself to your computer components and render them useless. Immediately delete any mail items that says this. AOL has said this is a very danderous [sic] virus, and there is NO remedy for it at this time, Please Be Careful, And forward to all your on-line friends A.S.A.P.²⁷

Ironically, this fake message really did include malicious code in the attachment. Forwarding this kind of fraudulent warning is simply playing into the hands of the criminals trying to trick uninformed victims into doing the criminals' work for them.

Moral: don't trust the subject field of any email message that has an unexpected attachment.

Other guidelines:

- Before you open any email message that includes an attachment, examine it to see if you recognize the sender; be suspicious if you don't.
- Before sending anyone an attachment of any kind, ensure that the recipients know what's coming to them and in what format (so they can open it)
- Do not send anyone executable files of any kind by email; if, exceptionally, you have some extraordinary reason to send executables, convert them to a non-executable form and then sign the converted version digitally (e.g., using PGP), then follow rule (2). Many email systems automatically block sending and receiving executables.
- Name every file you are sending in a descriptive way; for example, **2016-01-16_weekly_opsec_report.pdf** rather than **a3948vm7.pdf**.

And the ever-popular general principles,

- Choose antimalware products that can update themselves automatically and make sure they do so.
- Enable automatic scanning by your antimalware product on every file-open and file-save.
- Scan your entire system regularly for malware infections (I configure my antimalware software to scan all disks automatically at 01:00 in the morning every Saturday night).

RESTRICTING EMAIL TO AND FROM THE ORGANIZATION

External email of all kinds can be filtered through a firewall system which strictly controls the addresses of inbound and outbound messages. Specifically, such a firewall must include detection of fraudulent addresses on inbound email: addresses implying that external email originated from within the organization. For consistency, and as a service to the greater community, such a firewall should also restrict outbound email to ensure that no such messages have addresses implying that they originated outside the organization. These measures help to filter unsolicited commercial email ("spam") on the Net.

All email sent outside the organization by internal users raises important issues about authorized functions and the image of the organization in the outer world.

Although email-only gateways are feasible to allow users to exchange messages with other users in the wider world, it must be mentioned that there are ways for users to perform unauthorized functions such as file transfers simply using email. Email FTP servers receive search or file-transfer requests (scripts or batch files) by email and carry out those instructions anywhere on the Internet. The server then packages the results of the file transfer (or search, etc.) and sends it back to the originator as an email message. Binary files are converted using MIME, UUENCODE, PGP, or other transformation to 7-bit ASCII. This mechanism thus provides a covert channel for receiving binary files without going through normal security restrictions imposed on the import of executables.

Another form of binary file that may cause considerable embarrassment to the organization is graphics. There have been several cases in the United States in which government workers have been discovered using official computer resources to retrieve, store, and exchange pornographic and other undesirable materials. The legal consequences have been severe.²⁸

In addition, many discussion or news groups can be joined using email. Subscribers receive information about specific subjects of interest as ordinary messages and can reply if the system provides outbound Internet email. Given the wide range of topics available in the USENET, it is important to establish which news groups may be joined by corporate-email users. Many of the news groups cover highly technical areas and are legitimate sources of information for special purposes. However, many news groups are of questionable value to the work of organizational employees. Some news groups would be extremely undesirable: those dealing in extremist propaganda, organized hatred, and pornography would be embarrassing for the organization if there were to be organizational subscribers. Some could lead to prosecutions for violations of various laws.

Such activities using corporate email accounts must be carefully controlled and require explicit policies to prevent abuse. If intelligence gathering requires monitoring of questionable groups, analysts should subscribe using IDs not traceable to the organization and maintain written authorization from appropriate authorities in their organization; investigations crossing the lines into access of illegal activities should obtain official clearance from appropriate law-enforcement agencies.

It is important to realize that any outbound contribution to any news group or other discussion group in cyberspace by a user will be identifiable as coming from the employer's organization simply by the user's email address. This implies that every message sent out of the organization into the Internet must be considered as potentially damaging to the interests of the organization.

The opposite is also true: professional, helpful contributions by individuals affiliated with an organization enhance the organization's image and reputation.

The organization must frame and implement clear policies on participation in such news groups. For users authorized to participate in selected groups, the organization must provide training on appropriate "netiquette" to ensure that employees consistently project their professionalism. It would be embarrassing for the organization, for example, to discover that an employee had "flamed" another user (sent offensive email) using their corporate ID. Attempts to absolve the employer



FIGURE 17.22
Filtering email.

from blame by adding cute signature lines are futile: no one believes that someone with an ID of ralphm@megacorp.com [this is made-up!] is criticizing a competing product without knowing that MegaCorp [also imaginary] will be assumed to support his attacks.

Email users, even polite and professional ones, are subject to mail-bombing runs by disgruntled or mischievous Internet users. For example, two lawyers who sent out thousands of email messages by “spamming” the Internet with advertisements for their Green Card advisory services in the early 1990s were deluged by messages from angry users around the planet, bringing their Internet access provider’s servers to a halt.²⁹

In another incident, a naive sales manager posted two dozen similar commercial messages in what he thought were appropriate news groups; angry Internet users then posted his company’s 800-number in various recreational sex groups in the “alt” domain, describing them as free sex-chat lines. The resulting wave of offensive phone calls caused one of the receptionists to resign in disgust and completely swamped the inbound 800 service and denied service to legitimate customers. The company decided that they could not afford to change their 800 number, so they had to suffer through the loss and embarrassment of the episode until the calls died down.

In my own case, I locked a rude user out of the NCSA Forum on CompuServe around 1993 after repeated warnings not to use vulgarity or to attack other participants. As a result, I suffered through a couple of months of rambling, obscene verbal assaults – and so did about 50 other people to whom the disturbed individual sent copies. He eventually had to be removed from CompuServe altogether.

THE KEEPER OF THE LISTS

An organization I worked in years ago was large enough that there was significant turnover among the staff. At that time, we were adding new staff members periodically and we also moved staff members from one group to another; for example, a staff member might change from being an assistant director in one program to being an administrative director in another. Occasionally we also had staff members who left the group or even the entire organization altogether.

One of our staff members (the *Keeper-of-the-Lists* or KL) maintained the list of all of our staff members; however, there was no link between the XL file she maintained and the mailing lists that each member of the group had to maintain to be able to distribute email to appropriate groups. I remember one time, I noticed that on all the group mail messages sent by a colleague seemed to have an abnormally short distribution list. Sure enough, when I checked the names, I found seven errors: two missing deletions and five missing additions. One of the undone deletions was the name of a staff member who no longer worked in the organization at all.

Trying to make dozens of people (we had 41 staff members) maintain several distribution lists was a hopeless cause: even with the best will in the world, people were inevitably forgetting to update their lists and therefore:

- Some mailings missed legitimate recipients.
- Some people received messages they had no business reading.

There are easy solutions to rectify these problems:

- IT could install widely available list-server software to allow the KL to create and maintain specific lists; for example, ALL, DIRECTORS, STAFF, INSTRUCTORS, etc. that all of us could use as addresses for email.
- IT could switch all our users to any email client that supports exportable mailing lists (e.g., Outlook). The KL could maintain and distribute updated corporate distribution lists. However, this solution would still require manual intervention by users: everyone has to replace their old list by the new list.



FIGURE 17.23

Keep mailing lists up-to-date.

- IT could implement Microsoft Exchange Server, switch all users to Outlook and define corporate distribution lists maintained by the KL. All users would automatically access the one and only distribution list for each group without manual intervention.

Students reading this article should consider how the points apply to people running clubs and other groups at their college or university. Relying on individuals to coordinate their own versions of mailing lists of members or of executives simply doesn't work. Assign the task to a single person (with a backup for continuity of operations) and keep the lists up to date and properly documented.

MAILSTORMS

Most of us belong to mailing lists; many of us have more than one email address; some of us use autoforwarding to shift email from one address to another automatically; and a few of us use automated responses on our email accounts to let correspondents know when we are out of the office or unable to respond quickly.

All of these factors can contribute to mailstorms.

A mailstorm occurs when computers begin sending mail to each other without human intervention and one or both have limited storage capacity for unread messages. Sometimes mailstorms can become a denial of service by saturating communications channels and other resources. The email enabled worms such as Melissa, the I-love-you message, and so on are examples of malicious software whose authors deliberately wrote them to create mailstorms.

Let's start with a simple situation I learned about that actually happened in the early 1990s (all names changed to protect the silly):

- Sally goes on vacation and decides to receive her company email using an email service with a global presence but a limited capacity for unread emails, such as the old *CompuServe* or *AOL* services. She sets an autoforward command on her company account and sends all incoming mail to her more mobile *CompuServe* email account, figuring that she'll be able to log on to that one from wherever she goes.
- Unfortunately, when she reaches the remote tropical island where she will spend her vacation, she discovers that it is impossible for her to access even her worldwide ISP without paying a surcharge of \$6 a minute for long-distance service to the mainland. She cheerfully shuts down her computer and forgets all about email for the next three weeks.
- Meanwhile, back on the Internet, her company account dutifully forwards every message it receives to her *CompuServe* account. Unfortunately, Sally has forgotten that there is a limit of 250 messages on her *CompuServe* account and she reaches that limit within the first week of her vacation. At that point, every inbound message generates a bounce informing the sender that her *CompuServe* mailbox is full.
- The very first bounce message *CompuServe* sends her company account is cheerfully autoforwarded back to her *CompuServe* account. So now that message generates yet another mailbox-full message which then gets bounced back to her company account and so on without let up. Eventually, even her company mailbox fills up and then the two email systems continue chattering at each other indefinitely in a dialogue of demented robots.
- When the corporate email server finally crashed – about an hour after the first mailbox-full bounce – technicians found over 20,000 bounce messages on their server.

The number of email messages that can be generated by this kind of infinite loop is a function of the latency of the positive feedback system that the user has accidentally created. For example, if it takes exactly one minute for a bounce message to be returned to the originating site, then each



FIGURE 17.24

Overflowing
in-baskets.

message causing an initial error can create sixty additional messages per hour. However, because new messages are arriving at the originating mailbox all the time, new sets of bounced messages are constantly added to the fun. It is not uncommon to see tens of thousands of messages accumulating in the recipient mailbox if nobody notices the loop.

Imagine now that David belongs to a list where the FROM address is actually the broadcast address that sends his response to the entire list. You can see that his very first automated out-of-office response to the list will generate an infinite sequence of messages to and from that list. However, in this case, the *entire membership* of the list will be receiving his autoresponse – very embarrassing for the list administrator and intensely annoying for everyone else.

Something analogous to a mailstorm results from thoughtless behavior when using a public list. I'm sure that all of us have experienced irritation when a list member posts personal comments obviously intended only for the poster of a public message and for no one else. For example, Mike asks for a list of readings and Norman answers on the list, "I'll send you a list tomorrow." Several thousand unwilling readers now know about this projected email message. One of these irritated people, say Orville, now posts a message to Norman – but sent to the entire list – saying, "Did you really have to post that message to the entire list?" Orville's message is so irritating to Paula that she now posts a message to the entire list criticizing Orville for criticizing Norman. And so the useless tempest of email continues via the public list, creating thousands of copies of useless information.

In conclusion, here are some simple suggestions for reducing the likelihood of mailstorms:

- Minimize the use of automated responses on your email accounts.
- If you do autoforward your email, don't let your target mailbox fill up.
- If you are receiving autoforwarded email from your primary mailbox, don't autoforward back to the original mailbox.
- Email-system administrators should receive exception reports identifying accounts with excessive numbers of email messages or excessive traffic so that they can investigate for mailstorms.
- Firewalls that inspect the content of email message should be able to react to an excessive number of bounce messages from a single originating address and delete the traffic or inform system administrator of a likely mailstorm.
- Managers of unmoderated lists should configure a FROM address different from the address that participants use to post messages to the list.
- Users of list servers who want to send personal comments in response to posted messages should reply to the sender, not to the entire list.

DELIVERY NOT GUARANTEED

Some years ago a colleague wrote on her Facebook page,

Just found out that the University is expecting me to teach this semester. Last evening was the first I officially hear of this. I got a strange email from a student in the morning asking about the class, so I contacted the school to find out why a student was asking me. The response was, "Didn't you get the contract back in December?" No, I didn't. Then the comment, "See you on Wednesday for class!" Like in TOMORROW??? OMG! That is why I couldn't sleep."

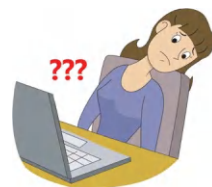


FIGURE 17.25
Surprise!!!

I added to the thread of shocked, sympathetic comments as follows:

People don't realize that the definitions of email from the *Internet Engineering Task Force* (IETF) *Requests for Comments* (RFCs) *do not include guaranteed delivery*. Anyone using email to communicate operationally important information *must* use (a) read-receipts and (b) out-of-band confirmation (e.g., telephone calls) to confirm delivery – and agreement if there's a contract involved!

The unfortunate incident got me thinking of the wider issue of confirming communications. Supplementary, optional information need not require confirmed delivery, but any operationally

significant information or instruction must have not only confirmed delivery but confirmation that the message has been read!

Medical offices routinely use a phone-answering message that warns callers *not* to leave a message if they need emergency help but to call a specific emergency-response phone number. When the emergency-response operator answers a 999 or 112 call in the United Kingdom or a 911 call in the United States and Canada, every transfer to the appropriate service (fire, ambulance, police) is done with the caller on the line. The caller is immediately transferred to another agent – not told to leave a message.

For technical support and computer-security emergency-response teams, it's essential that the problem-ticket system automatically sends a confirmation message to the client indicating the ticket number for every request for help – a particularly important function when the lines are busy and a client leaves a voicemail message, or when a client sends a help request through email. With enough exposure to such a policy, clients quickly come to expect the confirmation; if their original request is lost, misdelivered, or ignored, the lack of prompt confirmation from the helpdesk alerts the client to the likelihood that their message never reached anyone in technical support so they can try again.

When transferring responsibility for a technical-support case from one agent to another, the transferring agent must make person-to-person contact with the agent who will pick up the case; leaving a voicemail message or sending an email message is not good enough. An interrupted chain of communication will leave a client hanging without support for an indefinite period. An alternative to telephone or in-person contact is instant messaging (IM); an IM request can elicit an immediate response – and failure to respond can prompt further attempts to make contact or perhaps a switch to a different resource person. In any case, the client will never be abandoned because of an interrupted communication attempt.

When I arrived at Norwich University in 2001, I consistently refused to accept student essays or assignments on paper. For the first few years, I told students to submit term papers and exams using University email; however, a few years later, when our learning platform became available, I switched to using the intranet functions to have the students upload their assignments to an online repository for each assignment. It provided a detailed record of exactly when each student uploaded their file, so there was no ambiguity or uncertainty about whether the student submitted the work on time.

When planning for, say, adjunct-faculty staffing, every proposed contract should be confirmed before the contract is sent. My policy would be to make live contact by phone, VoIP, or some other form of live *synchronous* message (e.g., Skype or Messenger) to ensure that the instructor agrees to teach and accepts the terms of the contract. Then the director of the school or department should send instructions by email to the HR group asking for a contract to be sent – and the standard procedure should be that the request is copied to the instructor. The HR group should always send an email confirmation to both the issuing department and to the instructor. If a paper contract is the only format permitted, an HR official should verify that it was received, signed, and returned within a reasonable period (say, a week). Lack of response within the stated time would prompt a follow-up call. A checklist would make it easier to ensure that every step of this procedure is completed.

Don't count on luck when interacting on critical, time-sensitive issues: Verify email delivery and reading as a matter of course using a different communications channel for positive confirmation of receipt.

ON WRITING

A general principle for all operationally significant text in an organization is that clarity is essential. Confusing, vague comments are a waste of time. Unfortunately, my experience as a graduate student, professor, and employee has convinced me that the Whole-Language Movement, also known as Balanced Literacy, has severely compromised the ability of people who grew up after the 1960s to write clear English.³⁰ As Director of the Master of Science in Information Assurance (MSIA) program at Norwich



FIGURE 17.26
Writing clearly
is important.

University during the 2000s, I prepared a series of essays on how to write clear expositions of technical information. These principles may be helpful for readers of this textbook, but I have chosen simply to provide a reference to the work:

“On Writing”: < <http://www.mekabay.com/methodology/writing.pdf> >. Topics are:

- Organizing Your Thoughts
- Writing Top-Down
- Invisible Writing
- On Communicating Precisely
- Why We Cite Sources
- Reference Materials
- On Having Your Papers Edited
- Integrating Feedback from Your Instructors
- Egoless Work
- Critical Thinking and Disintermediation
- Resources for Improving Your Writing
- Strunk & White’s Rules from *The Elements of Style*

The other document that may be helpful for technical writing is:

“Frequently Corrected Errors”: < <http://www.mekabay.com/methodology/fce.pdf> >

which is a checklist and reference source to identify and correct common grammatical and usage errors.

SUMMARY

Employees acting badly in cyberspace may not only embarrass their managers and cause civil suits for damages, they may actually lead to criminal investigations and prosecution – hardly the kind of publicity any organization wants. The overall message to employees must be clear:

- Treat electronic mail as if it were written on company letterhead.
- Anything posted to the net is public and may be permanent.
- Never click on a link in email without verifying where it connects.
- Don’t forward unverified warnings.
- Think carefully before posting information or opinions you and your employer may regret later.
- Don’t forward confidential internal information to outside recipients.
- Don’t include employees’ unsupervised personal web-links on corporate websites.
- Don’t spam.
- Use the TO, CC, and BCC fields properly.
- Use a descriptive subject line.
- Be careful when using automated email responders.
- Don’t mix up operationally significant topics with non-essential email content.
- Don’t depend solely on email to announce mission-critical, time-sensitive information.
- Do your best to write clearly.



FIGURE 17.27
Main points.

NOTES

- 1 99Content (2021).
- 2 NORC at the University of Chicago (2016).
- 3 Hartney (2020).
- 4 Sanders (2018).

- 5 Cain (2017).
- 6 Legal Services Link (2019).
- 7 Hwant (2023).
- 8 U.S. Securities and Exchange Commission (2021).
- 9 Loshin (2021).
- 10 Purdue University (2023).
- 11 Boyden (2008).
- 12 U.S. Congress (1948).
- 13 U.S. Postal Service (2021).
- 14 U.S. Postal Inspection Service (2019).
- 15 Carroll (1999).
- 16 Beikiempis (2023).
- 17 Smith (2003).
- 18 Epley and Kruger (2004).
- 19 Bousfield, (2008).
- 20 Schiller (2004).
- 21 Sting and The Police (2008).
- 22 Bitdefender (2021).
- 23 Microfocus (2021).
- 24 Atkins, Sam Spade (2023).
- 25 U.S. Federal Bureau of Investigation (2019).
- 26 Matthews (2019).
- 27 F-Secure (2002).
- 28 U.S. Department of Justice (2021).
- 29 Everett-Church (1999).
- 30 Winter (2022).

WORKS CITED

- 99Content. (2021). *How Many Email Users Are There?* Retrieved December 19, 2021, from 99firms | Blog: <https://99firms.com/blog/how-many-email-users-are-there/>
- Atkins, S. (2023). *Sam Spade*. Retrieved October 11, 2023, from LO4D.com | Windows: <https://sam-spade.en.lo4d.com/windows>
- Beikiempis, V. (2023, October 4). *Sam Bankman-Fried trial: What Is He Accused of and Does He Face Prison Time?* Retrieved October 5, 2023, from The Guardian | Business: <https://www.theguardian.com/business/2023/oct/03/sam-bankman-fried-crypto-ftx-fraud-trial-explainer>
- Bitdefender. (2021). *Bitdefender Home Page*. Retrieved November 25, 2021, from Bitdefender: <https://www.bitdefender.com/>
- Bousfield, D. (2008). *Impoliteness in Interaction* (1st ed., Vol. 1). England: John Benjamins Publishing Company. Retrieved November 25, 2021, from <https://www.amazon.com/Impoliteness-Interaction-Pragmatics-Beyond-New-dp-9027254397/dp/9027254397>
- Boyden, B. E. (2008, September 14). *Court Finds First Amendment Right to Forge E-mail Headers*. Retrieved April 17, 2024, from Marquette University | Law School Blog | Computer Law: <https://law.marquette.edu/facultyblog/2008/09/court-finds-first-amendment-right-to-forge-email-headers/>
- Cain, A. (2017, April 23). *11 Things Never to Send Over Work Email*. Retrieved October 2, 2023, from Business Insider: <https://www.businessinsider.com/things-never-to-send-over-work-email-2017-4>
- Carroll, R. T. (1999, January 17). *Pyramid Schemes, Chain Letters and Ponzi Schemes*. Retrieved November 25, 2021, from The Skeptics Dictionary: <https://web.archive.org/web/19990302065826/http://www.dcn.davis.ca.us/~btcarroll/skeptic/pyramid.html>
- Epley, N., & Kruger, J. (2004, November 5). When what you type isn't what they read: The perseverance of stereotypes and expectancies over e-mail. *Journal of Experimental Social Psychology*, 41, 414–422. Retrieved November 25, 2021, from https://uploads-ssl.webflow.com/5c484e0f4aa6f839dc553c45/5c86cb636a253b062d22ff09_EpleyKruger2005.pdf
- Everett-Church, R. (1999, April 13). *The Spam That Started It All*. Retrieved November 25, 2021, from <https://www.wired.com/1999/04/the-spam-that-started-it-all/>
- F-Secure. (2002, February 9). *Hoax Warnings*. Retrieved November 25, 2021, from F-Secure | Hoaxes: <https://web.archive.org/web/20020209095432/http://www.europe.f-secure.com/hoaxes/returned.shtml>

- Hartney, E. (2020, January 12). *10 Basic Rules of Netiquette or Internet Etiquette: Know Your Manners When Using Technology*. Retrieved November 24, 2021, from VeryWellMind: <https://www.verywellmind.com/ten-rules-of-netiquette-22285>
- Hwant, R. (2023, June 16). *We're Taking Legal Action to Stop Fake Review Scams*. Retrieved October 2, 2023, from Google | Outreach Initiatives | Public Policy | Legal Action: <https://blog.google/outreach-initiatives/public-policy/legal-action-stop-fake-review-scams/>
- Legal Services Link. (2019, January 22). *Employee Use of Social Media: What Can Employers Control?* Retrieved October 2, 2023, from Legalservices | Blog: <https://www.legalserviceslink.com/blog/employee-use-of-social-media-what-can-employers-control/>
- Loshin, P. (2021, March). *Email Spoofing*. Retrieved from November 24, 2021 TechTarget | Threats and vulnerabilities | Network security: <https://www.techtarget.com/searchsecurity/definition/email-spoofing>
- Matthews, T. (2019, July 2). *Sircam: Worm, Virus, Trojan Horse?* Retrieved November 25, 2021, from Exabeam | Information Security: <https://www.exabeam.com/information-security/sircam/>
- Microfocus. (2021). *KeyView Overview*. Retrieved November 25, 2021, from Microfocus | Products | File Viewer: <https://www.microfocus.com/en-us/products/file-viewer-filter/overview>
- NORC at the University of Chicago. (2016, April 22). *Americans Believe Civility Is on the Decline*. Retrieved November 25, 2021, from ScienceDaily: <https://www.sciencedaily.com/releases/2016/04/160422201040.htm>
- Purdue University. (2023, July 5). *How Do I Identify and Deal with Email Spoofs/Spoofing?* Retrieved October 2, 2023, from Purdue University | Knowledge Base: <https://service.purdue.edu/TDClient/32/Purdue/KB/ArticleDet?ID=392>
- Schiller, F. (2004, August 1). *Die Jungfrau von Orleans*. Retrieved November 25, 2021, from Project Gutenberg: <https://www.gutenberg.org/ebooks/6383>
- Smith, G. (2003, March 10). *One Printer, One Virus, One Disabled Iraqi Air Defence: You Can't Keep a Good April Fool's Down*. Retrieved November 25, 2021, from The Register: https://www.theregister.com/2003/03/10/one_printer_one_virus_one
- Sting and The Police. (2008, November 27). *Every Breath You Take*. Retrieved November 25, 2021, from Youtube: <https://www.youtube.com/watch?v=cEnJDaqT3-0>
- U.S. Congress. (1948, June 25). *18 U.S. Code §1341 - Frauds and Swindles*. Retrieved December 19, 2021, from Legal Information Institute | U.S. Code: <https://www.law.cornell.edu/uscode/text/18/1341>
- U.S. Department of Justice. (2021, July 23). *Former U.S. Government Employee Pleads Guilty to Sexual Abuse and Obscenity Offenses Committed Over 14 Years*. Retrieved November 25, 2021, from U.S. DoJ | Public Affairs | News: <https://www.justice.gov/opa/pr/former-us-government-employee-pleads-guilty-sexual-abuse-and-obscenity-offenses-committed>
- U.S. Federal Bureau of Investigation. (2019, March 25). *The Melissa Virus: An \$80 Million Cyber Crime in 1999 Foreshadowed Modern Threats*. Retrieved November 25, 2021, from FBI | News | Stories: <https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519>
- U.S. Postal Inspection Service. (2019, July). *Chain Letters*. Retrieved November 25, 2021, from USPS | Publications: https://about.usps.com/publications/pub300a/pub300a_v04_revision_072019_tech_007.htm
- U.S. Postal Service. (2021). *How to Contact th U.S. Postal Inspection Service*. Retrieved December 19, 2021, from USPS.com | About: https://about.usps.com/publications/pub300a/pub300a_v04_revision_072019_tech_024.htm
- U.S. Securities and Exchange Commission. (2021, December). *Market Manipulation*. Retrieved December 19, 2021, from Investor.gov | Introduction to Investing | Glossary: <https://www.investor.gov/introduction-investing/investing-basics/glossary/market-manipulation>
- Winter, J. (2022, September 1). *The Rise and Fall of Vibes-Based Literacy*. Retrieved October 11, 2023, from The New Yorker | News | Annals of Education: <https://www.newyorker.com/news/annals-of-education/the-rise-and-fall-of-vibes-based-literacy>

Index

RU, 45

18 U.S. Code, Sections 1302 and 1341, 362

18 US Code 1030(a), 146

18 USC §§1367, 2232, 2510, 224

18 USC §1030, 224, 322

18 USC §1343, 322

18 USC §1367, 323

18 USC §2251-2252, 323

18 USC §2701, 224

18 USC 1030(a), 98, 198

2016 election, 312

29 USC § 2001, 183

2FA, 22

3 USC § 414, 183

35 USC, 340

35 USC §101, 340

35 USC §102, 340

39 U.S. Code, Section 3005, 362

404s, 110

4-1-9 Nigerian Fraud, 84

4chan, 69

4GL, 178

4GL compiler, 148

8chan, 69

A

A/C, 20, 21

AAAS, 148

ABIDS, 152

absence of positive feedback, 231

absolute freedom of speech, 330

abstraction from reality, 305

abuse of power, 35

abuses, 146

abusive confrontations, 154

academic dishonesty, 76

academic freedom, 37, 39

acceptable service, 141

acceptable-use policy, 337

access, 2, 11, 21, 22, 51, 56, 61, 79, 87, 89, 110, 250

access controls, 79, 135

access illegal activities, 377

access patterns, 114

access speed, 107

access to medical records, 148

access to weapons, 189

access-control, 5, 11, 24, 79

access-control systems, 16, 290

accidental use, 19

accounting, 22, 35, 211

accounting standards, 144

accuracy of recognition, 75

AccuVote, 48

ACDCA, 224

ACLU, 74

ACM, 140, 251

acoustic tiles, 14

Acrobat, 51, 90

Acrobat Reader, 298

Acrobat script, 198

ACSC, 150

act in the best interest of the client, 158

actinic light, 91

action plan, 159

activate the zombie programs, 137

Active Cyber Defense Certainty Act, 224

actively used data drive, 123

ActiveX, 24, 137, 297

ActiveX controls, 99

Actor-Observer Effect, 254

actuary, 215

ad hominem attack, 258

ad hominem attacks, 68

ad hominem comments, 334

adblockers, 61

address in HTML, 364

addresses in copy field, 368

Admail, 59

administrative manager, 179

administrator privileges, 227

Adobe, 51

Adobe Acrobat, 298

Adorno, 176

Advanced Topics in Incident Handling, 249

advanced-document properties sheet, 126

advance-fee fraud, 82, 84, 310

advisories, 29

adware, 61, 62

AdWords, 338

aerospace, 181

AES, 108

Africa, 12

after-hours party, 202

age, 66, 74, 158, 176, 323

agreement, 6, 38, 85

Ahmed, 67

AI, 92

air conditioners, 5, 10

air conditioning, 19

air gap, 22

air intakes, 21

air-blast horns, 100

air-conditioning, 20

air-conditioning ducts, 21

airport, 9, 30, 33, 82, 159

Aite Group, 87

alarm, 31, 225

alarms, 12, 152, 225

ALE, 215

ALE calculations, 216

alert services, 150

Allport, 176

alt hierarchy, 359

alternate hypothesis, 246

Alternic, 98

- amateurs*, 3, 64, 137
- Amazon, 115
- ambiguity, 326
- American Association for the Advancement of Science, 148
- American Civil Liberties Union, 74
- American Polygraph Association, 182, 183
- Amiable, 257
- Amiable personality type, 257
- Analytical, 257
- Analytical personality type, 256
- analyzing the successful cases, 153
- anarchistic, 25
- anatomically impossible instructions, 100
- announcing changes, 298
- annualized loss expectancy, 215
- anomalies, 35
- anomaly-based IDSs, 152
- anonymity of the equipment rooms, 11
- Anonymizer.com*, 29
- anti-discrimination laws, 176
- antimalware, 30, 62, 136
- anti-malware, 30
- Anti-Malware group, 343
- antimalware updated, 95
- anti-spam, 36, 342
- antispam becomes DoS, 363
- antispam filters, 342
- anti-spam laws, 361
- anti-vaccine, 67
- anti-vaxxer propaganda, 335
- antivirus, 348
- antivirus laws, 350
- Anti-Virus Product Developers' Consortium, 343
- API, 306
- application fraud, 87
- application software, 92, 109
- application-program bugs, 118
- application-program interface, 306
- approaches to problem solving, 238
- appropriate-use policies, 23
- approved service providers, 151
- April Fool's printer hoax, 365
- archived records, 111
- archives, 113
- Ardita, 325
- area code, 84
- Argentina, 325
- Army Information Systems Engineering Command, 316
- arrival*, 74, 79
- arrow keys, 92
- art of technical support, 238
- Arthur Andersen, 111, 143
- artificial fluctuations, 361
- artificial intelligence, 92, 114, 149, 181, 222, 292, 313
- ASCII, 51
- assault, 158
- assign responsibility, 149
- Association for Computing Machinery, 251
- assume an attitude of paranoia, 185
- assume responsibility, 286
- assumptions, 36, 37, 63
- assumptions based on group membership, 255
- astragals, 13
- asymmetric encryption, 53
- asymmetric information warfare, 94
- asynchronous information transfer, 90
- ATM, 10, 88, 89
- AtomicTangerine, 10
- attachment, 36
- attachment payload, 95
- attack assessment, 311
- attack prodromes, 225
- attackers, 75, 76, 137, 146, 221, 224
- attain our strategic objectives, 173
- attention to outliers, 286
- attention to security policies, 276
- attitude, 282
- attract children, 98
- attractive targets, 134
- attribution, 73
- audience variables, 283
- audit, 9, 63, 142
- audit looks for compliance, 155
- audit trail, 55, 76
- auditing, 57, 142, 149
- auditing standards, 144, 145
- auditor, 143
- auditors, 135, 142, 143
- audits, 57
- audit-trail, 63
- Australian Cyber Security Centre, 150
- authenticate, 53
- authentication, 22, 53, 55, 56, 73, 74, 75, 77, 78, 79, 87, 98, 197
- authentication of Internet traffic, 114
- authentication rules, 76
- authentication software, 135
- authenticity, 1, 2, 45, 53, 54, 55, 73, 309
- Authenticity, 2, 73
- authenticity of documents, 140
- author rights, 59
- authoritarian behavior, 177
- authoritarian personality, 176, 255
- authoritarian regimes, 28
- authority, 54, 55, 177
- authorization, 24, 26, 27, 28, 190
- authorization code, 89
- authorized personnel, 151
- authors, 6, 145
- autistic child hacker, 230
- AUTOEXEC.BAT, 95
- auto-forward, 373
- automate surveillance, 221
- automated attack tools, 138
- automated attacks, 138
- automated banking machines, 88
- automated responses, 36, 223, 379, 380
- automatic caching, 151
- automatic color-coding, 219
- automatic inactivation of accounts, 223
- automatic logout, 223
- automatic-teller machines, 10
- auto-responder, 116, 117
- availability, 1, 2, 3, 37, 107, 118, 138, 240, 309, 323
- Availability, 2, 37
- availability heuristic, 254
- availability of archival data, 108

availability of DDos tools, 137
 availability of IPv6, 224
 availability of the tool, 305
 average, 77, 94
 average of CAC scores, 161
 average power drain, 16
 avoid candidates excessively sensitive to structural power, 185
 avoid candidates intolerant of ambiguity, 185
 avoid candidates likely to follow charismatic leaders, 185
 avoid counter-productive personality traits, 176
 avoid process-oriented candidates, 185
 AVPDC, 349
 awareness, 4, 49, 146
 Aycock, 348

B

back doors, 48, 222
 background checking, 177
 backhoes, 10
 backup personnel, 239
 backup power generators, 234
 backups, 4, 11, 63, 107, 108, 113, 122, 128, 129, 130, 131, 136, 311
 backward compatibility, 109
 bad electrical power, 18
 bad management environment, 155
 badges, 74
 badly normalized data structures, 307
 baggage, 31
 Balanced Literacy, 381
 Bales, 343
 ballot, 47
 ballots, 46, 47
 bank, 88
 bank record, 45
 Bankman-Fried, 362
 Barings PLC, 190
 baseline data contaminated, 222
 basic system hygiene, 148
 batteries, 17
 battery power, 16
 BBSs, 357
 BCC, 369
 BCP, 216, 220
 beacons, 224
 behavioral extinction, 142
 being indispensable, 187
 beliefs and attitudes, 282
 beliefs can change, 282
 ben-testers bonded, 153
 Bernstein, 38, 350
 better client service, 240
 beyond their competence, 157
 Biden, 67
 bigotry, 68, 176
 biological virus, 351
 biometric authentication, 88, 135
biometrics, 22, 74, 77
 birds-of-a-feather group, 348
 birth certificate, 55
 Bitcoins, 45
 BitDefender, 374

Black, 164, 231, 253
Black Hat security conference, 49
 black-hat hackers, 137
 blacklist, 225
 blacklisted, 225
 blacklisting process, 343
 BLIND CARBON COPY, 369
 blocking IP traffic, 317
 blooper, 36, 50
 Board of Directors, 143
 body-enhancing drugs, 342
 bogus insurance policies, 142
 boilerplate, 127
 bollards, 5
 boot camps, 10
 Boston University School of Law, 340
 bots, 91
 bottom and top quartiles, 161
 bounce, 379
 boundaries, 48, 197
 bounds violations, 48
 brainstorm countermeasures, 153
brainstorming, 160, 161, 216
 brake lights, 346
 breach, 27, 240
 breach of contract, 204, 212, 348
 breach of ethics, 24
 breaches, 37, 74, 282
 breaches of security, 134
 breaker, 20
 breaker panels, 18, 19
 break-even point, 215
 break-even points, 216
breaking security, 90
bribes, 143, 145
 British Department of Trade and Industry, 196
 broad target sets, 150
 brown-outs, 18
 browser, 22, 29, 58, 61
 browser plug-in, 59
 browser window, 60
 browser's home page, 59
 browsers, 58
 browsing, 22, 23
 brute-force, 92
 brute-force cracking, 227
 brute-force searches, 214
 Brzezinski, 67
 budget process, 145
 buffer overflows, 48, 301
 bug in the operating system, 173
 bug notification, 30
 bug reports, 29, 345
 bug-tracking, 118
 bug-tracking tools, 118
 bugs, 29, 78, 135
 building alarm(s), 10, 13
 building collapse, 10
 building design, 12
 building layout, 11
 building maintenance, 211
 Building Relationship Versatility: Social Styles at Work, 255
 bulk email, 195

bulletin-board systems, 357
 Bullwinkle Show, 111
 Bureau of Engraving and Printing, 91
 burglars, 225
 Burma Shave, 141
 business-continuity planning, 216
 Buy.com, 115
 BUY.COM, 50
 buyer beware, 196
 bypass normal security restrictions, 306
 bypassing the 4GL, 178
 bystander effect, 285

C

C++, 301
 CAC, 160, 161, 216, 262
 Calce, 115
 call-blockers, 87
 caller-ID spoofing, 87
 call-tracking statistics, 241
 cameras, 5, 13, 116
 Canadian International Development Agency, 12
 candidate, 46, 88, 177
 candidate's job experience, 179
 candidates, 46, 137, 158, 174, 177
 canonical passwords, 21
 CAN-SPAM Act, 361
 capabilities matrix, 216
 CAPTCHA Project, 91
 car registration, 54
 card skimmer, 89
 Carnegie Mellon University, 91, 149, 248
 Carpenter, 316
 Carroll, 333
 Carte Bleue subway system, 345
 Carter, 359
 cat, 82, 84
 CATA, 162, 164, 165, 166, 262
 catastrophic errors, 16
 category code, 163
 Caveat emptor, 196
 CD, 21, 65
 CD-ROMs, 109
 Cellini, 224
 cell-phone camera, 91
 censorship, 38, 39, 323
 Center for Countering Digital Hate, 67
 Center for Information Technology Policy, 48
 Center for Security Information Systems, 365
 Central Military Commission, 316
 central processing units, 11
 central route to persuasion, 285
 Central Vermont Medical Center, 107
 centralized policies, 228
 CEO, 10, 27, 35, 52, 53, 67, 144, 202, 203
 CERT/CC, 149, 248
 certificate, 54, 55, 56, 57, 85
 certificate authority, 54, 57
 certificate format, 55
 certificate policies, 57
 certificate users, 56
 certificates, 54
 Certified Information System Security Professionals, 322

CFAA, 325
 CFO, 135, 143
 chain email letter, 361
 chain letters, 4
 chain of trust, 55, 56
 chain-mail pyramid fraud, 362
 challenge your initial views, 157
 challenging a question and answer, 154
 change colleagues's perception of information security, 278
 change in personality, 189
 change initial scores in CAC, 161
 change interpersonal style, 188
 change of lifestyle, 189
 change schemas, 282
 change the corporate culture, 281
 changing attitudes toward security, 283
 channel variables, 268, 284
 chaotic software update, 24
 characterize the attack, 243
 Charles Cresson Wood, 24
 chases, 12
 cheating, 62
 check answers for consistency, 175
 check the credibility, 358
 checklist, 113, 201, 382
 Checkster, 174
 checksum, 47
 checksums in production, 302
 chicken crossed the road, 156
 Chief Executive Officer, 10
 Chief Financial Officer, 143
 Chief Information Security Officer, 135
 Chief Moderator, 332
 Chief Operating Officer, 143
 Chief Technology Officer, 143
 child pornography, 23, 323
 children, 64, 65, 66, 323
 Chinese cyberespionage ring, 316
 Chinese-sponsored industrial espionage, 316
 chocolate factory, 340
 chocolate on keyboard, 283
 chocolate on keyboards, 142
 chunks, 166
 C-I-A, 1
 CIDA, 12
 CIO, 135, 143, 144, 326
 ciphertext, 53, 90, 148
 CISA, 28, 66, 67, 150
 CISO, 135, 143, 144, 197
 CISSPs, 322
 CITES, 82
 civil lawsuits for damages, 224
 civil litigation, 361
 civility, 26
 civil-liberties problem, 174
 class-action lawsuit(s), 50, 203
 Classic Triad, 1
 classical conditioning, 283
 clay tablets, 247
 cleartext, 53, 90
 client confidentiality, 137
 client support, 258
 climate crisis, 20

- climb building, 12
- clipart, 125
- [ClipArt.com](#), 337
- close-knit work groups, 276
- closets, 12
- closure-time statistics, 241
- clothing factory, 305
- cloud backups, 113
- cloud-based backups, 129
- cloud-based software, 129
- CMU, 248
- CNN, 115
- COBOL, 178
- Codd, 305, 307
- code, 49, 50, 64, 82, 84, 86, 92, 146, 190, 197, 301, 357
- code inspection, 63
- COINTEL, 3, 314
- collaborative responses, 348
- collapse of Enron, 142
- collapse of FTX, 362
- colleagues, 47, 49, 64, 86, 116, 122
- collecting statistics about problems, 241
- collegiality, 346
- colluding with a thief, 225
- collusion, 144, 186, 191
- color, 75, 158
- Colorado lottery, 47
- color-coded tape, 15
- color-shifting ink, 91
- COM, 60, 66, 218
- combination-code to the lock, 277
- COMINT, 314
- comma-separated-value(s), 62, 241
- commercial data-destruction firms, 230
- Committee on Commerce, 230
- Committee to Review the Scientific Evidence on the Polygraph, 182
- Common Gateway Interface, 39
- Common Vulnerabilities and Exposures, 150, 248
- communications among team members, 240
- Communications Decency Act, 67
- communications intelligence, 314
- communicator variables, 284
- Community Action Center, 36
- Community Standards, 336
- community-college courses, 262
- competitive advantage, 140
- competitors, 194, 310, 314
- compilations of standards, 221
- compiler, 64
- complaining of unfairness, 204
- complaints about the draft policies, 292
- complaints dismissed, 233
- Completely Automated Public Turing test to tell Computers and Humans Apart, 91
- complexity of social cognition, 281
- compliance, 78, 79, 80, 141, 149, 232, 277, 286
- compliance curve, 231
- compliance efforts, 196
- compliance officer, 197
- compliance rate, 142, 231
- compliance rates climbed, 283
- compliance with legal requirements, 122
- compliance with logoff policy, 142
- compliance with policies, 155
- compliance with regulations, 177
- compound key, 306
- compromise, 3, 11, 75, 112
- Compulife Software, Inc., 310
- compulsive gambler, 189
- CompuServe*, 36, 37, 108, 332, 350, 357, 378, 379
- CompuServe email, 36
- CompuServe Security Forum, 332
- Computer Assisted Instruction, 263
- Computer Based Training, 263
- Computer Crime Law, 27
- Computer Desktop Encyclopedia, 37
- Computer Emergency Response Team Coordination Center, 248
- Computer Fraud and Abuse Act, 146
- Computer Fraud and Abuse Act of 1986, 224, 322
- Computer Insecurities at DOE Headquarters, 230
- Computer Output to Microfilm, 109
- computer room, 5, 10, 11, 12, 13, 14, 19, 20, 21, 190
- Computer Science Laboratory, 251
- Computer Security Handbook, 1, 116, 182, 253
- Computer Systems Laboratory, 276
- Computer Viruses and Malware, 348
- Computer-Aided Consensus, 160
- Computer-Aided Thematic Analysis, 122, 162
- Computer-Emergency Response-Team Coordination Center, 149
- computer-operations room, 35
- currency, 304
- currency control, 303
- concurrent access, 247
- confidence limits, 216
- confidential information, 175
- confidentiality, 1, 3, 8, 23, 34, 39, 56, 112, 309, 370
- Confidentiality, 1, 3
- confidentiality agreements, 205
- confidentiality of personal information, 194
- configuration lock, 227
- conflict of interest*, 135, 142, 143, 144, 145
- conflicts of interest, 158
- conformity, 286
- confounding factors, 246
- consensus, 161
- consequences, 4, 11, 23, 59, 78, 87, 117, 144, 146, 148, 190
- consequences of foolish postings, 359
- consideration, 362
- consistency, 50, 204
- consistent* change in behavior, 189
- consoles, 11
- conspiracy, 66, 69
- conspiracy theories, 312
- conspiracy theorists, 46
- conspiracy-cult, 69
- constantly changing technical environments, 149
- Constitution, 67, 332, 340
- consultants, 137, 156
- Consultants' Code of Ethics, 158
- Consulting Alliance, 158
- consulting contracts, 158
- consulting involves teaching, 159
- Contempt Toward Officials, 332
- context, 97, 150

- context influences perception, 165
- ContextPro, 59
- contingency plans, 234
- continued operations, 136
- continuing-education courses, 262
- continuity of operations, 219, 379
- continuity of service of servers, 220
- Continuity-of-Operations Matrix, 218
- continuous operation, 220
- continuous process improvement, 186
- Continuous Process Improvement, 294
- continuous-process-improvement, 154
- contract(s), 4, 57, 141
- contradictory information, 282
- contributory infringement, 337
- Control, 1
- control freak, 219
- control violations, 8
- controversial applications of the polygraph, 183
- Convention on International Traffic in Endangered Species, 82
- conversion, 51
- convince users, 276
- COO, 107, 143
- cookies, 22, 23, 193
- cooling-off period, 199
- cooperation of interviewees, 160
- co-opt colleagues, 276
- copies of copies of copies, 371
- copy*, 55, 60
- copying company information, 113
- copyright, 26, 37, 38, 58, 61, 79, 127
- copyright by employer, 331
- copyright infringement, 284
- copyright-infringement lawsuits, 338
- cordless phones, 19
- core dumps, 118
- corporate culture, 291
- corporate email, 4
- corporate IDs for *personal* use, 359
- corporate liability, 287
- corporate policy, 238
- corporate VPN, 238
- corporate webpage, 37
- corporate website, 6
- correctness, 45
- corruption, 49, 98, 145
- cost estimates, 57
- cost per minute, 77
- cost-effective, 289
- counterattacks must be forbidden, 224
- counterfeit, 74
- counterfeit stamps, 73, 339
- counterfeit-deterrence, 91
- counterfeiting trademarks, 339
- counter-intelligence, 3, 315
- course design, 211
- coverage, 225
- coverage monitors, 136
- covert operations, 264
- cover-ups, 113
- COVID, 66, 67
- CPI, 186, 263, 294
- CPU, 11
- crack programs, 141
- crawl space, 14
- CRCs, 15
- Creating a Computer Security Incident Response Team, 249
- credit bureaus, 88
- credit card, 54, 60, 88, 89, 137
- credit records, 310
- credit-bureau records, 88
- criminal hackers, 137, 181
- criminal record(s), 87, 88, 174
- criminal records of team members, 155
- criminal underground, 137
- criminality, 113
- criminality of spoofing, 361
- criteria for scheduling improvements, 154
- critical applications, 16, 17
- critical components, 20, 62
- critical data, 48, 124, 190
- critical element, 135
- critical equipment, 12, 15
- critical facilities, 6
- critical file, 126
- critical functions, 216
- critical infrastructure, 28, 311
- critical legal issue, 204
- critical operation, 190
- critical processes, 28
- critical programs, 233
- critical servers, 114
- critical services, 5
- critical switches, 19
- critical systems, 48, 211, 290
- critical thinking, 70
- critical vulnerabilities, 248, 302
- criticizing colleagues, 176
- cross-training, 200
- cross-training all personnel, 186
- Crypto-Gram, 140
- Crypto-Gram Newsletter, 251
- cryptographic software, 53
- cryptographically strong authentication, 98
- cry-wolf syndrome, 225
- CSIRT, 249
- CSV, 62
- CSV files, 241
- CTO, 143
- cult leader, 110
- cults, 69, 177
- curiosity, 189
- current version of each manual, 248
- customer *dissatisfied*, 361
- customer-relationship management, 223
- customer-satisfaction techniques, 262
- cutoff switches, 20
- CVEs, 150, 248
- CVEs per day, 248
- CyberCorps, 181
- Cyberlaw & Cybercrime course, 49
- cyberlaws, 322
- cyber-safety, 252
- Cybersecurity & Information Systems Digest, 140
- Cybersecurity and Infrastructure Security Agency, 150
- Cybersecurity Center Development, 249

cybersecurity scholarship programs, 181
 cybervandals, 137
 cyclic redundancy codes, 15
 Cyrillic alphabet, 342

D

daily backups, 130
 Daily Joke Mailing List, 123
 daisy-wheel, 109
 damage to reputation, 153, 205
 damage violating netiquette, 360
 Darley, 285
 DARPA, 98
 Dartmouth, 64
 Dartmouth College, 116
 data anomalies and normalization, 307
 data center, 5, 8, 9, 10, 11, 13, 14, 19, 20, 35, 118, 213
 data centers, 13, 20, 21, 173
 data corruption, 15, 50
 data definitions, 304
 data destruction, 107, 111, 112, 113, 311
 data dictionary, 305
 data diddling, 199
 data integrity, 45, 49, 50, 53
 data privacy, 140
 data retention, 112
 data retention policies, 112
 data safes, 11
 data safety, 140
 data storage, 4, 109
 data subject, 4
 data theft, 316
 database application, 306
 database components, 306
 database is model of a model, 305
 database management and security, 303
 database performance, 347
 databases, 15
 data-center operations, 175, 176
 data-cloning, 129
 data-destruction policies, 112, 113
 data-integrity bug, 60
 data-loss-prevention, 90
 data-management guidelines, 113
 data-retention policies, 113
 datasets, 306
 Date, 305
 Day-Timer, 215
 DB, 46, 63, 73, 74, 77, 137, 145, 186
 DB Administrators, 303
 DB management systems, 303
 DB records, 32
 DBAs, 303
 DBMS, 303
 DBs, 15, 47, 62, 149, 152, 176, 305
 DDoS, 3, 28, 114, 115, 137, 311
 DDoS mitigation, 114
 deadline, 78
 deadly embrace, 50
 dealing with hostile customers, 239
 death, 2, 66
 death threat(s), 87, 310
 debit card, 88
 DeBrand Fine Chocolates, 340
 debriefing, 147, 153
 DEC, 109
 deceit, 146
 deceptive content, 361
 deceptive reports, 314
 deceptive subject lines, 361
 decide on action, 285
 decimal points, 49
 decision-making, 254
 decrypt, 53
 decryption keys, 311
 deep linking, 38
 defamation, 310, 330, 333
 default settings, 135, 223
 defend the network perimeter, 114
 Defense Advanced Research Projects Agency, 98
 Defense Information Systems Agency, 316
 defensive publications, 341
 define the scope of the consulting assignment, 157
 defining a virus, 350
 defining measurable objectives, 140
 defining record structures, 303
 definition of alarm, 225
 definition of new, 340
 degaussing, 229
 degradation, 109
 degree policies enforced, 331
 delay, 77
 delay send five minutes, 368
 deletion anomaly, 307
 Dell, 115
 Delphi Technique, 160
 demilitarized zone, 222
 denial of service, 3, 228, 250, 379
 denial-of-service attacks, 107
 deny access, 228
 Department of Commerce, 339
 Department of Defense, 311
 Department of Energy, 230
 Department of Justice, 112
 Department of Transport, 33
 departure, 74, 78, 79
 deposit, 46, 55
 Depressed People, 255
 depression, 189
 design, 146, 190, 348
 design errors, 48
 design optimization, 238
 designing antivirus mechanisms, 348
 destroy an inoperable disk, 229
 destroying magnetic or optical media, 113
 destruction, 4, 13, 64
 destruction of company documents, 142
 detect breaches, 151
 detect early stages of possible attacks, 221
 detect fraudulent addresses on inbound email, 377
 detect intrusions, 221
 detecting attacks, 222
 developing security policies, 289
 DHS, 66, 67
 diabetes clinic, 49
 dialogue of demented robots, 379
 Die Hard, 10, 13

- Diebold, 48
 - Diebold Corporation, 47
 - different topic, 370
 - differential backup, 131
 - difficult to search quickly, 247
 - Digital Equipment Corporation, 109
 - Digital photography, 3
 - digital signature, 53
 - digital signatures*, 51, 52, 53, 114, 298, 302, 327
 - Dinosaur Prevention, Mitigation and Recovery Planning, 234
 - dinosaurs, 233
 - Dinsdale Piranha, 117
 - direct current rectifiers, 16
 - Direct Marketing Association, 344
 - Director of Technical Services, 20, 177, 213
 - directory, 55, 56, 57
 - directory standards, 57
 - DirectX, 92
 - disability, 158
 - disable auto-execution, 136
 - disadvantages of social engineering, 147
 - disaffected employees, 203
 - disagreement among the scores, 161
 - disaster, 11, 18, 57, 144, 201, 231
 - disaster-recovery planning, 211
 - disaster-recovery plans, 192
 - discard an hypothesis, 178
 - discarded disk drives, 229
 - discarding backup media, 136
 - disclaimer, 39
 - disclaimer pages, 364
 - disclosure, 3, 13, 60, 61, 113
 - disclosure of email, 5
 - discovered vulnerabilities, 153
 - discovery process, 113
 - discrimination, 52, 202
 - disgruntled programmer, 233
 - disgruntled employee, 90
 - disgruntled employees, 136, 198, 203, 205
 - disgruntled users, 378
 - dishonest, 6, 81
 - dishonest employees, 136
 - dishonest intentions, 6
 - dishonesty, 151, 203
 - DISINFO, 3, 64, 66, 67, 70, 311, 312
 - disinformation campaigns, 313
 - Disinformation Dozen, 67
 - disinformation operations, 312
 - disintermediation, 3, 67, 197
 - disk cloning software, 130
 - disk drive sanitization, 229
 - disk drives, 11, 16, 20, 150, 230
 - disk errors, 15
 - disk I/O, 107
 - Disk Operating System, 109, 118
 - diskettes, 108
 - disproof, 246
 - disprove an hypothesis, 246
 - disproving hypotheses, 246
 - disruption, 150, 158, 192, 311
 - disruption of relationships, 202
 - dissemination of virus code, 350
 - distinguish facts from assumptions, 244
 - distributed denial-of-service, 28
 - division of labor, 155
 - DLP, 90
 - DMZ, 222
 - DNS, 62, 86, 98, 364
 - DNS corruption, 98
 - DNS registrations, 339
 - DO NOT CALL list, 344
 - DocFetcher, 215
 - document conversion, 109
 - documentation, 2, 117
 - documents folder, 125
 - DocuSign, 53
 - DOCX*, 51, 136
 - DoD 5220.22-M Wiping Standards, 230
 - DoE, 230
 - DoE Office of Independent Oversight and Performance Assurance Board, 230
 - DOE's Failure To Get Its Own Cyber House In Order, 230
 - domain, 37, 55, 96, 197, 364, 378
 - domain name, 193
 - domain name servers, 98
 - Domain Name System, 62, 339, 364
 - domain names, 96
 - domain-registration service, 84
 - Dominion Voting Systems, 47, 334
 - do-not-spam lists, 196
 - door frame(s), 12, 13
 - door hinges, 13
 - doors, 12, 21
 - DoS, 3, 37, 76, 78, 114, 141, 154, 221, 311
 - DoS attacks, 223
 - DOS kernel, 118
 - double bind, 222
 - Douglas, 29
 - downtime, 141
 - Doxillion Plus, 125
 - doxing, 310
 - doxxed, 336
 - Dr. Diet Mountain Dew, 93
 - drills, 12, 19
 - Driver, 257
 - Driver personality type, 256
 - driver's license, 54, 56
 - driver-level data encryption, 374
 - drop ceilings, 14
 - Dropbox, 113
 - drug tests, 174
 - dual control, 190, 191
 - dual criminality, 325
 - due diligence, 337
 - dummy security cameras, 13
 - duty of care, 149
 - DVDs, 109
 - dynamic biometrics, 74
 - Dynamic Real-Time Spam Blocking, 343
 - Dynamic Reputation Database, 344
 - dysfunctional setup reducing user productivity, 228
- ## E
- ear biometrics, 75
 - easily-accessible records, 214
 - Easter Egg, 93, 94

- Easter Eggs, [47](#), [92](#)
- eat victim's heart, [359](#)
- eavesdrop, [13](#)
- eBay, [115](#)
- ecomm, [3](#)
- e-commerce, [57](#), [140](#), [223](#)
- economic consequences of malware, [348](#)
- ECPA, [323](#), [325](#)
- ECPD, [4](#)
- EFCA, [142](#), [143](#)
- effective communications with clients, [238](#)
- effective problem-solving, [240](#)
- ego, [36](#)
- ego-involvement, [178](#)
- egoists, [263](#)
- egoless work, [35](#)
- EICAR, [4](#), [5](#), [110](#)
- EICAR Conference, [110](#)
- eight-inch disks, [108](#)
- El Gordo, [85](#)
- electric fences, [233](#)
- electric generator, [17](#)
- electrical panel, [18](#)
- electrical power, [15](#), [18](#), [109](#)
- electrical surges, [18](#)
- electricity failed, [220](#)
- electronic archive, [214](#)
- electronic commerce, [3](#)
- Electronic Communications Privacy Act of 1986, [224](#), [323](#)
- electronic perimeters, [203](#)
- electronic sabotage, [94](#)
- electronic version, [247](#)
- electronic voting, [46](#), [47](#)
- elements of impoliteness, [367](#)
- email, [3](#), [135](#), [137](#), [152](#)
- email disclaimer, [372](#)
- email password, [52](#)
- email prefixes, [371](#)
- Email Reputation Services, [343](#)
- email server crashed, [379](#)
- email spoofing, [361](#)
- embarrassing graphics, [377](#)
- embarrassment, [195](#)
- embezzlement, [187](#), [189](#), [190](#)
- emergency, [2](#), [9](#), [18](#), [19](#), [20](#), [21](#), [77](#), [134](#), [141](#), [234](#)
- emergency access, [190](#)
- emergency alarm, [31](#)
- emergency electric generator, [220](#)
- emergency exits, [12](#)
- emergency generator, [220](#)
- emergency lighting, [18](#)
- emergency power, [221](#)
- Emergency Power Off, [19](#)
- emergency rescue, [9](#)
- emergency response, [11](#)
- emergency response teams, [149](#)
- emergency room, [90](#)
- emergency services, [211](#)
- emergency-response planning, [230](#)
- emergency-response plans, [192](#)
- emergency-response team(s), [222](#), [381](#)
- emergent property, [48](#)
- emoticons, [368](#)
- empirical science, [246](#)
- employee communications, [331](#)
- Employee Crisis Line, [189](#)
- employee fungibility, [231](#)
- employee integration, [146](#)
- employee morale, [204](#)
- Employee Polygraph Protection Act of 1988, [183](#)
- employee* self-expression, [332](#)
- employee turnover, [146](#)
- employees *required* to take scheduled vacations, [188](#)
- employer, [23](#), [54](#), [77](#), [189](#), [360](#)
- employment agreement(s), [175](#), [205](#)
- employment contract(s), [175](#), [331](#)
- employment policies, [182](#)
- employment termination, [203](#)
- employment with competitors, [205](#)
- encourage cross-training, [187](#)
- encouraging initiative, [285](#)
- encryption, [22](#), [28](#), [29](#), [53](#), [57](#), [131](#), [135](#), [194](#)
- encryption keys, [6](#)
- end-user license agreement, [61](#)
- enforce work rules, [360](#)
- enforcement mechanisms, [196](#)
- enforcing policies, [283](#)
- Enron*, [111](#), [112](#), [113](#), [143](#), [144](#), [145](#)
- Enron's auditor, [143](#)
- entry cost, [311](#)
- Epley, [366](#)
- EPO, [19](#)
- Equity Funding fraud, [142](#)
- erased information, [136](#)
- erasure programs, [136](#)
- error in firewall configuration, [228](#)
- errors, [3](#), [62](#), [63](#), [68](#), [76](#), [82](#), [260](#)
- errors of interpretation, [254](#)
- errors of judgment, [255](#)
- escalating the problem, [225](#)
- escalation process, [30](#)
- escrow, [264](#)
- espionage, [311](#)
- estimated probabilities, [216](#)
- estimates of time and effort, [159](#)
- ethical debate over computer trespass, [327](#)
- ethnic targeting, [314](#)
- ethnicity, [158](#)
- ETrade, [115](#)
- E-Trade, [115](#)
- EULA, [61](#), [62](#)
- euphoria, [189](#)
- EuroCAUCE, [195](#)
- European Coalition Against Unsolicited Commercial Email, [195](#)
- European Community Privacy Directive, [4](#)
- European Court of Justice, [339](#)
- European Institute for Computer Anti-virus, [4](#)
- European Spreadsheet Risks Interest Group, [62](#)
- EuSpRIG, [62](#)
- evaluate potential consultants, [157](#)
- evaluating the degree of learning, [271](#)
- evaluation, [51](#)
- evaluation of reality, [254](#)
- eversign, [53](#)
- evidence, [52](#), [66](#), [68](#), [69](#), [75](#), [142](#), [174](#), [224](#)
- evidence of authorship, [130](#)

- evidence of ownership, 131
- evil designs, 199
- examine audit trails, 151
- examine log files, 151
- Excel*, 47, 60, 62, 93, 136
- Excel 97, 92
- Exchange, 111
- Excite, 115
- exclude convicted felons, 174
- exclusion of longer-term thinking, 232
- executable email attachments, 95
- executive briefing session, 293
- ex-hacker, 137
- exhortation does not work well, 286
- exit interview, 199, 200
- exits, 12, 234
- expect rapid response to newly identified problems, 154
- expectation of privacy, 331
- expelled, 27, 131, 147
- experience in operations, 185
- experienced operations staff, 179
- experiment, 142
- expert hacker activity, 316
- expert in the next office, 239
- expiration, 55
- expiration deadline, 77
- expiration of patents, 340
- explicit documentation, 238
- explicit documentation available, 238
- exploitation, 131, 136
- exploits, 149, 250
- explore system log files, 243
- exploring current structure of beliefs, 283
- explosives, 9, 12, 31
- exposure*, 11, 290
- exposure of email addresses, 369
- Expressive, 257, 258
- Expressive personality type, 257
- expulsion from professional societies, 157
- external firewalls breached, 150
- external hard drives, 130
- external links forbidden, 364
- external testing can be cost-effective, 155
- external threats, 134
- external vulnerability analysts, 155
- external windows, 13
- extinguishment, 142
- extort compliance, 348
- extortion, 175, 345, 346
- extortion fees, 340
- extradition, 325
- extradition of virus writers, 350
- extranet, 37, 223
- eZula, 59
- F**
- FAA, 33
- fabricated reports, 143
- face recognition, 74, 75
- face value, 358
- Facebook*, 67, 73
- Facebook Messenger, 90, 335
- face-recognition, 74
- face-to-face persuasion, 284
- facial features, 74
- facilities, 8, 21, 57, 79
- facilities management, 191
- factory defaults, 223
- failed to counter social engineers, 153
- failures, 48
- fair-use doctrine, 337
- fake bank accounts, 188
- fake checks, 46
- fake email, 197
- fake email addresses protected speech, 361
- fake link, 97
- fake phishing message, 147
- fake reviews, 361
- fake stamps printed in China, 339
- fake websites, 89
- false alarms, 31, 222, 225, 226
- false attribution, 310
- false biographical sketches, 366
- false light, 61
- false negatives, 152, 222
- false news, 64, 67
- false positives, 152
- False Representation, 362
- falsehoods, 64
- familial status, 158
- Family Educational Rights and Privacy Act, 153, 194
- Faraday cage, 229
- Farah, 183
- farewell party, 198, 201
- Farmer, 27
- Fascist Orange Narcissistic Sociopath, 69
- Fastclick, 59
- FAT, 15, 228
- fault, 255
- fault-tolerant, 186
- fault-tolerant organization, 186
- favor candidates able to assimilate information quickly, 185
- favor candidates with meticulous attention to detail, 185
- favor goal-oriented candidates, 185
- favorable depictions, 255
- fax, 86, 87, 213
- FBI, 67, 98, 112, 150, 227, 339
- FCC, 86
- FDISK, 229
- fear, 64, 66, 79, 187
- fear the unknown, 176
- Federal Aviation Administration, 33
- Federal Bureau of Investigation, 150
- Federal Reserve notes, 91
- Federal Trade Commission, 176
- feeling of inadequacy, 177
- Felten, 48
- FERPA, 153, 194
- fields or columns or attributes, 306
- Fighting Computer Crime, 114
- file-allocation table, 15, 228
- file-conversion utilities, 108
- file-recovery tools, 228
- final set of CATA categories, 164
- financial audit, 145
- financial consequences, 46

- financial difficulties, 363
 - financial record(s), 88, 142
 - fingerprints, 74
 - fire, 10, 11, 20, 31, 32, 136, 145, 180
 - fire alarm(s), 19, 31
 - fire department, 11
 - fire-resistant, 14
 - fire-suppression, 21
 - fire-suppression systems, 14, 21
 - fired, 30, 35, 45, 52, 144, 198
 - firewall, 31, 59, 62
 - firewall configurations, 228
 - firewall failures, 221
 - firewall parameters, 135
 - Firewall Product Developers' Consortium, 223
 - firewalls, 22, 61, 114, 135, 149
 - firing gone wrong, 200
 - firings, 200
 - First Amendment, 67, 323, 330, 332, 350
 - first-hand* knowledge, 244
 - first-person observations, 244
 - fixable errors, 155
 - flag anomalous behavior, 152
 - flagrant breach of security, 277
 - flaming, 358
 - flash drive, 131
 - flash mobs, 312
 - flashdrives, 136
 - flight, 47
 - flight simulator, 92
 - flood, 11
 - flood of attack packets, 223
 - flooding, 358
 - floor plan, 5
 - floor tiles, 14, 21
 - floppy disk, 108
 - flowers.com, 53
 - fluctuations, 16
 - fluorescent light, 91
 - fMRI, 183, 184
 - focus groups, 160, 162, 283, 289
 - foistware, 59
 - folder, 22, 129
 - follow-up call, 381
 - follow-up with clients, 240
 - foolish use of email, 359
 - foot-in-the-door technique, 287
 - for dereliction of duty, 190
 - foreign industrial espionage, 313
 - foreign intelligence service, 314
 - foreign lottery, 85
 - foreign students, 314
 - forge email, 52
 - forged addresses, 100
 - forged email headers, 73, 99
 - forged headers, 100, 114, 342
 - forger, 2
 - forgeries, 73
 - forgery, 52
 - forging, 51
 - forging a log file, 302
 - forging email, 53
 - forging reputation, 347
 - forklifts, 10
 - formal guidelines from neutral third parties, 155
 - format hard disk, 51, 62, 213, 229, 258, 295
 - formatting, 305
 - formatting a disk, 136
 - FORTRAN, 64
 - Forum on Risks to the Public in Computers and Related Systems, 251
 - forwarding *all* suspicious messages, 147
 - forwarding corporate email, 373
 - foundation, 53, 69
 - foundation skills, 140
 - Foundations of Incident Management, 249
 - four pillars of responsible email, 344
 - fourth-generation language, 178
 - Fox News, 334
 - frame exercises as a game, 147
 - frames*, 97, 297
 - framing of problems affects risk perception, 279
 - frantic email warning, 365
 - fraudulent business profiles, 361
 - fraudulent checks, 187
 - fraudulent email, 361
 - fraudulent stamp ads, 339
 - fraudulent version, 99
 - fraudulent warning, 376
 - free sectors, 228
 - freedom of speech, 332
 - free-speech and corporate policy, 332
 - freeware, 61
 - freight elevators, 10
 - French INTEL, 315
 - freshman hacked administrative systems, 147
 - friend, 68
 - friendly, 154
 - friendly discussions, 218
 - friendly tone, 153
 - frustration, 147
 - FTC, 80, 97, 98, 251, 361
 - FTX cryptocurrency exchange, 362
 - fudge factor, 291
 - full backups, 150
 - full disclosure, 28, 29
 - full-text search, 241
 - functional magnetic resonance imaging, 183
 - fundamental attitude change, 291
 - Fundamental Attribution Error, 254
 - fungible automatons, 205
 - fuse-boxes, 19
 - fuses, 19
 - futures, 86, 190
- ## G
- game(s), 64, 65, 92, 135
 - gangs, 3, 311
 - garbage, 32, 116
 - Garfinkel, 229
 - gas-pump meters, 47
 - Gates, 343
 - Gator, 60
 - GDPR, 153, 192, 324
 - Gehl, 29
 - gender(s), 75, 158, 176
 - General Data Protection Regulation, 153

generate ideas, 160
 generator, 16, 17
 generic drug names, 342
 generosity, 202
 genetic information, 158
 George Mason University, 365
 get-out-of-jail card, 27
 gift cards, 310
 gift subscription expiration, 326
 glass, 5, 10, 12
 glass breakage, 225
 glitches, 78
 Global Affairs Canada, 12
 Global Engagement Center, 313
 Global Patent Solutions, 341
 global picture, 82, 84, 90, 212, 243
 global picture of reality, 277
 GMAIL, 73
 Gnu Privacy Guard, 53
 GnuPG, 53
 goal-oriented, 176
 goals, 1, 141, 143
 goals of information assurance, 1
 golden handshake, 175
 good candidates, 157
 good moods increase prosociality, 286
 Good Times Virus, 65
 Goody Two-Shoes, 346
 Google Chrome, 58
 Google Images, 82
 Google search engine, 338
 gossip, 67
 government agencies, 28
 Government Operations Committee, 47
governmental restriction of speech, 330
 GPG, 56
 graceful shutdown, 15, 220
 grade records, 63
 grades, 51, 62
 grammatical errors, 382
 Grand Theft Auto, 337
 Granneman, 317
 graphical user interface, 118
 graphs of spam, 342
 Green Card advisory services, 378
 green logbooks, 212
 GreyMagic, 29
 grief, 202
 group by priorities, 161
 group competition, 255
 group psychology, 277
 group the ideas, 161
 group-think, 176
 guesses about damage, 134
 GUI, 118
 Guide for Selecting Automated Risk Analysis Tools, 292
guilt motivates people to act, 286

H

Habiger, 230
 habituated, 31
 hack-back, 222
 hacked, 27, 309
 hacker's alphabet, 342
 hackers, 3, 32, 92, 112
 hactivism, 138
 hall closet, 14
 hand geometry, 74
 handling difficult calls, 253
 harassment, 158
hash, 53
 Hastings Center Report, 183
 headers, 114, 361
 Health Insurance Portability and Accountability Act, 32, 148
 healthy curiosity, 189
 hearsay, 244
 heart attacks, 148
 heat sensors, 14
 height-to-weight, 74
 HelloSign, 53
 help vendor, 346
 helpdesk, 64, 77, 78, 141, 214, 220
 helpdesk personnel, 77
 helpdesk software, 241
 helpdesks, 211
 Herold, 252
 heuristic tool, 219
 Hewlett Packard, 232, 347
 Hewlett-Packard (Canada), 14
 hidden text, 97
 Hide file extensions, 124
 hierarchical CA, 56
 higher levels of management, 347
 highlight the danger zones, 217
 highly classified computer hard drives, 230
 highways, 9
 Hindi curses, 100
 hinge pins, 13
 HIPAA, 32, 148, 152, 192
 HIPAA violation, 369
 hire candidates, 173
 hiring, 5, 137
 hiring a consultant, 158
 hiring managers, 177
 hiring process, 174
 hiring programmers, 177
 hiring security officers, 177
 hiring staff, 5
 hiring technical support personnel, 177
 history of malware, 348
 history of the Internet, 111
 Hitachi monitor, 50
 hoaxes, 64, 65, 66
 hold the door open, 277
 holidays, 187, 204, 214
 Hollerith, 64
 home page, 39, 59
 homograph attack, 96
 homophobia, 68
 Hormel Company, 79
 Hormel Foods, 3
 hospital, 18, 49
 hospitals, 76
 host, 48
 hostile work environment, 23, 135, 154
 hostile working environment, 359

hostility, 176
 hosting, 114
 Hotmail, 363
 HOTMAIL, 318
 hover their cursor over a link, 97
 hovering cursor over link, 343
 HP, 14, 17, 50, 118, 141, 159, 186, 258
 HP 110 laptop, 160
 HP Canada, 141, 212
 HP Way, 141
 HP3000, 118, 159, 177, 212, 213, 232, 257
 HP3000 minicomputer, 109
 HP3000 Series III, 109
 HP7925, 50
 HTML, 3, 50, 108
 HTML email, 51, 342
 HTML spam, 342
 HTML-enabled email, 374
 Human Resources staff, 289
 human-resources functions, 211
 humiliate children, 177
 Humpich, 345
 hyperlink, 38
 hyperlinks, 37, 38, 58, 61
 Hypertext Markup Language, 3
 hypotheses, 246

I

I am not a lawyer, 28
 I just work here, 258
 IANAL, 28, 60
 IAPSC, 158
 IBM, 75
 ICANN, 86
 ICAT Metabase, 249
 ICSA, 135, 343
 ICU, 18
 ideas, 63, 64
 ideas sorted, 161
 ideas taken for granted, 244
 ideation, 160
 identical photographs, 83
 identification and authentication, 22
 identify the limits of their knowledge, 157
 identity theft, 3, 87, 88
 identity-theft prevention, 88
 ideologically warped adults, 137
 IDS, 28, 31, 149, 152
 IDS initialized with clean data, 222
 IDS sensors, 222
 IDSs, 135, 152, 221
 IEEE Security & Privacy, 229
 IETF, 98, 380
 illegal discrimination, 203
 image, 3, 45
 image backups, 130
 image files, 51
 image manipulation, 311
 Image Properties, 82
 images of children, 323
 imaginary invoices, 73
 iMessage, 27
 immediate notification, 89
 impact metrics, 149
 impersonating a company, 99
 impersonation, 54, 88, 310
 impersonation of business entities, 197
 implement, 1, 74, 149, 150
 implement policies, 281
 implementation, 292
 Impoliteness in Interaction, 367
 imposters, 88
 improper firing procedures, 198
 improve the robustness of fMRI, 185
 improved risk analysis, 221
 improved risk management, 221
 improving algorithms and data structures, 238
 improving risk assessment, 280
 inadequate analysis, 228
 inadequate authentication, 224
 inadequate environmental controls, 109
 inadequate samples, 254
 inadequate security measures, 221
 incident tracking, 240
 incident-handling system, 241
 incitement to violence, 330
 incivility, 332
 include many realistic examples, 288
 incompetent employees, 198
 incomplete and inconsistent laws, 324
 incorrect label, 113
 increase awareness of threats, 153
 increase employee awareness, 282
 increase in connectivity, 149
 increasing spam flow, 343
 increasingly long messages, 369
 indefinite gags, 204
 independence, 158
 independent oversight, 144
 in-detail interviews, 137
 index, 306
 indexing, 186
 individual meetings, 284
 industrial control system, 181
 industrial espionage from China, 315
 industrial spy, 90
 infinite loop, 379
 inflated bottom line, 231
 inflated claims, 174
 influence attitudes, 283
 infodemic, 66
 information infrastructure, 311
 Information Security Policies Made Easy, 292
 Information Systems Security course, 10
 Information Technology Infrastructure Library, 214
 Information Technology Service Management, 214
 Information Warfare: Chaos on the Electronic
 Superhighway, 309
 Information-Protection Group, 294
 information-protection working group, 294
 information-security working group, 291
 information-sharing, 28
 information-warfare, 50, 94, 316
 information-warfare exercises, 311
 informed choices, 118
 informed consent, 5
 INFOSEC policies, 152

- INFOWAR, 309
 - infrastructure, 20, 49, 211
 - infrastructure functions, 211
 - in-group affiliations, 177, 185
 - input domains, 48
 - insecure code, 146
 - insecurity in action, 219
 - insert incriminating data, 131
 - inside* of firewall, 221
 - insider crime, 136
 - instability, 118
 - install the patches, 150
 - installation, 10, 24, 51
 - installation disks, 130
 - instantiation of one interpretation of a view of reality, 305
 - institutional knowledge, 187
 - institutional memory, 240
 - insulin pumps, 49
 - insult bosses in email, 359
 - insulting accusations, 202
 - insurance policies, 87
 - integration of new employees, 263
 - integrity, 1, 2, 34, 37, 53, 61, 158, 196, 309
 - Integrity, 2, 37
 - Intel Corporation, 27
 - intellectual property, 61, 177, 336
 - intelligence, 69, 79, 140
 - Intelligence Authorization Act for Fiscal Year 1995, 313
 - intelligence challenge, 311
 - intensive-care unit, 18
 - Inter Partes Review, 341
 - Interactive Advertising Bureau, 60
 - intercepted email, 59
 - inter-corporate information warfare, 310
 - INTEREX*, 159, 213
 - INTEREX Magazine*, 159
 - inter-group hostility, 255
 - intermediation, 67
 - internal barriers, 149
 - internal dangers, 134
 - internal network firewalls, 149
 - Internal Revenue Service, 112
 - internalization, 287
 - internalize security, 287
 - International Association of Professional Security Consultants, 158
 - international cooperation, 324
 - international coordination, 29
 - International Telecommunications Union, 54
 - Internet Archive, 59, 110, 111
 - Internet connectivity, 136
 - Internet Engineering Task Force, 98, 380
 - Internet Explorer, 29, 58, 59
 - Internet links, 37
 - Internet Network Information Center, 98
 - Internet of Things, 136
 - Internet Service Providers, 197
 - Internet Software Consortium, 98
 - InterNIC, 98
 - interoperability, 54, 57
 - interoperation, 56
 - interpersonal electronic warfare, 310
 - Interpol, 339
 - interrupted chain of communication, 381
 - interstate mail-fraud laws, 361
 - interstate postal fraud, 326
 - interviewing staff members, 160
 - intimidation, 158
 - intolerance of ambiguity, 176
 - intrusion, 12, 135
 - intrusion alerts, 222
 - intrusion-detection systems, 28
 - intrusions, 146, 221
 - inverse order of the lock sequence, 302
 - Invisible KeyLogger Stealth, 226
 - involve users, 276
 - IoT, 136
 - IP address, 55, 96, 193
 - IP address range, 317
 - IPR, 341
 - IPv4, 224
 - IPv6, 224
 - irate clients, 258
 - iris patterns, 74
 - iris recognition, 75, 88
 - irrational, emotional reaction, 154
 - irritability, 189
 - irritating responses, 258
 - isolation switches, 220
 - isolation transformers, 17
 - isomorphic with reality, 305
 - ISP, 114
 - It's Just Not Worth the Risk, 284
 - iterate estimates to stability, 161
 - ITIL, 214
 - ITSM, 214
 - ITU-T, 54
 - IW Executive Board, 311
- J**
- J.C. Penney, 38
 - janitor, 191
 - Java*, 24, 137
 - JAVA*, 297
 - Java applets, 98, 99
 - Javascript, 137
 - JavaScript, 59
 - JCL, 263
 - Jepson, 87
 - JINBU*, 159
 - Job Control Language, 263
 - job counseling, 199
 - Joint Cybersecurity Advisory, 150
 - junk email, 52, 100
 - junk emailer, 53
 - Jurassic Park, 233
 - jurisdictional problem, 324
 - juvenile detention, 115
- K**
- Kabay's Law of Redundancy, 233
 - Kaiser, 148
 - Kashpureff, 98
 - KaZaa, 59
 - Keeper-of-the-Lists, 378

Kerckhoff's Principle, 11
 kernel-level modifications, 90
 Kevin Mitnick, 310
 key escrow, 57
 key issues for preliminary study, 290
 key servers, 56
 keys, 6, 53, 54, 56, 57, 65, 74
 keystroke loggers, 226, 227
 keystroke-logging Trojan, 226
 Keyview, 375
 Kinko, 226
 kiss of death, 101, 157
 kitten, 65
 knowbot, 50
 knowledge-hoarder, 219
 knowledge of technical support, 179
 Known Spam Source List, 343
 Known Spam Source List Service, 343
 known vulnerabilities, 150, 221
 known vulnerabilities introduced into a system, 152
 known-good copy of the operating system, 227
 Krim, 74

L

lab notebooks, 64
 label cables, 14
 label electrical plugs, 15
 labeling storage media, 113
 Labyrinth Society, 92
 lack of expertise, 155
 lack of shared fonts, 51
 LAN, 6
 LAN monitors, 6
 LAN operating systems, 6
 LAN servers, 20
 landscape, 92
 language influences perception, 254
 Lanham Act, 338
 LANL, 230, 231
 LAN-monitor, 6
 LANs, 6
 Laplink, 129
 laptop computer, 30
 laser interferometers, 13
 laser printers, 16
 last copy, 131
 Latane, 285
 Law & Order, 49
 laws against virus writing, 349
 lawsuits, 23, 86
 lawsuits dropped, 341
 lawsuits for defamation, 198
 lawsuits for hostile working environments, 154
 layout, 8, 11
 layout of TODO database, 213
 LCD projectors, 227
 Le Meridien Hotels, 338
 learn from the exercise, 153
 learner variables, 266
 learning curve shorter, 179
 learning platform, 381
 leave of absence, 203
 lectures on leadership, 155

lectures on management style, 155
 lectures on organizational psychology, 155
 lecturing people has little effect, 286
 Leeson, 190
 Leet, 342
 legal consequences, 67, 113
 legal dimensions of spam, 342
 legal liability, 197
 legal responses to defamation by trolls, 335
 Leichter, 110
 levels, 56, 79
 levels of expertise, 259
 levels of INFOWAR, 309
 lewd or hateful jokes, 359
 Lewis, 187, 188
 LGBTQIA, 176
 liability, 28, 112
 libel, 68, 332, 333
 libelous accusations about colleagues, 359
 license management, 24
 License on Transfer Network, 341
 lies, 3, 66, 67, 68, 69, 88
 lifeguard, 146
 lighting, 18, 74
 likelihood of attack, 137
 limitation of speech, 332
 line management, 185
 line manager, 179
 lines of responsibility, 181
 Linux, 215
 lip-service, 276
 lists of valid addresses, 101
 litigation, 5, 157, 158, 341
 live backups, 129
 live contact, 381
 live *synchronous* message, 381
 living far beyond his means, 189
 Local area networks, 6
 location, 8, 9, 10, 82, 84
 location for generator, 220
 lock, 74, 78, 90
 lock account automatically, 223
 lock boxes, 113
 lockwords, 6
 logbooks, 212
 logging, 135
logic bomb, 93, 94, 199, 234
 logic bombs, 48, 136
 logoff, 76, 79
 longevity, 107
 long-term difficulties, 202
 long-term objectives of problems-solving, 242
 long-term storage, 109
 Los Alamos National Laboratory, 230
 loss avoidance, 140
 loss-management computation, 215
 loss-prevention policies, 296
lost update problem, 304
 lottery, 85
 Louis Vuitton, 339
 Love Bug, 325
 low voltage, 18
 low-activity mode, 19
 Luepker, 148

M

- MacOS*, 215
- macro viruses, 93, 137
- Macro.Excel.Sugar, 93
- macro-virus protection, 93
- Mafiaboy*, 115, 116
- magnetic disks, 108
- magnetic media degradation, 108
- magnetic tape, 108, 109
- Mail Abuse Prevention System, 343
- Mail Fraud Statutes, 362
- mail-bomb, 52
- mail-bombing, 358, 378
- mailbox(es), 1, 8
- mailbox-full message, 379
- mailstorm(s), 379, 380
- mainframe, 6, 19, 109, 142
- mainframe computer(s), 14, 16, 20
- maintenance, 22
- maintenance and adaptation, 293
- maintenance payments, 107
- malfeasance, 135, 157, 158
- malformed data, 304
- malformed or spoofed packets, 114
- malicious code, 48, 136
- malicious code contained, 348
- malware, 3, 27, 30, 58, 62, 92, 311
- malware in attachment, 376
- malware scans, 24
- managed-security company, 222
- management, 146, 231, 240, 249
- Management by Objectives, 140
- management by walking around, 141, 306
- Management by Wishful Thinking, 141
- management culture, 231
- management reviews, 233
- management sensitization, 291
- manager, 6, 35
- manager evaluations, 233
- managing capacities and structural relationships, 238
- Managing Computer Security Incident Response Teams, 249
- managing vulnerability disclosure, 347
- mandatory vacations, 188
- Manila, 325
- manual counting, 46
- manual testing, 48
- manufacturers, 6
- marital status, 176
- market share, 140, 216
- market-development strategy, 140
- marketing, 38, 80, 81, 86, 194
- marketing medium, 110
- Marquardt, 37
- Massachusetts Institute of Technology, 62
- Master of Science in Information Assurance, 116, 381
- maximum transfer rates, 114
- MBO, 140, 141
- MBWA, 141
- McAfee, 90
- McBride, 339
- McFadden, 60
- MCFs, 211
- McGill University, 63
- meaningful subject field, 371
- measure of competence, 231
- measure of the quality of the penetration testing, 152
- measure performance, 140, 231
- Medallia, 262
- media-literacy, 70
- medical emergency, 189
- medical records, 151
- medical staff, 192
- medical-information systems, 107
- medical-record systems, 49
- Melissa, 376
- memory card, 48
- mental countermeasures against fMRI, 184
- message variables, 270, 284
- Messenger, 381
- meta-analysis, 63, 94
- metadata, 305
- metadata from data dictionary, 306
- metal detector, 30
- metal oxide, 109
- metatags, 97
- methodologies from neutral third parties, 155
- metrics, 159
- MFA, 89
- microsoft.com, 96
- microdot, 90
- microfilm, 109
- micromanagement style, 145
- Microsoft*, 29, 36, 38, 47, 58, 62, 75, 94, 109
- Microsoft Knowledge Base, 118
- midrange computer(s), 14, 16, 20
- Military Power of the People's Republic of China, 315
- military status, 158
- MIME-encoded text, 36
- minimize stress, 153
- Ministry of Home Affairs, 27
- MINITAB, 216
- Minnesota Heart Survey, 148
- minor encouragement, 283
- mirroring, 124
- misappropriation, 197
- mischief, 115
- MISINFO, 3, 64, 66, 67, 70, 357
- misinformation, 64
- misinterpreting signals, 225
- mislabeled subjects, 371
- misleading advertising, 339
- misleading subject fields, 371
- misleading subject lines, 342
- misogyny, 68
- misprogramming, 48
- misrepresent the links, 97
- misrepresentation, 81, 361
- misrepresentation of the origins, 131
- MISSI, 56
- mission critical, 49
- mission-critical functions, 12, 62, 211
- mission-critical operations, 107, 187
- mission-critical systems, 177
- misspellings, 84, 96
- mistake not permission, 328
- mistake to refuse a good candidate, 178

mistaken attributions, 254
 misunderstanding risks, 279
 misunderstandings, 190
 misuse detection, 342
 MIT, 62
 model of a model, 305
 Model Policy for Law Enforcement PreEmployment
 Polygraph Screening Examinations, 183
 models, 59
 modem(s), 13, 18, 21, 22, 27, 136
 moderated discussion groups, 332
 modifying the registry, 93
 monitor compliance, 286
 monitor programs, 6
 monitoring, 4, 135, 335
 Monitoring and Manipulating Brain Function, 183
 monitoring employees, 329
 monitoring intrusions, 149
 monitoring questionable groups, 377
 monitoring software, 6
 Monte Carlo simulation, 216
 Montpellier, 46
Monty Python, 36, 79, 116, 117
 Monty Python addiction, 116
 Monty Python Society, 116
mood, 286
 mood swings, 189
 moral rights, 61
 morale, 146, 199, 200
 Morris Worm, 248
 Morse, 184
 motion sensors, 5
 mouse trapping, 97, 98
 move the corporate culture, 283
 Mozilla Firefox, 58
 MPE, 118, 177, 212
 Mr Peabody, 111
 MRI scanning, 184
 MS-Access, 213
 MS-DOS, 109
 MS-Outlook, 36
MS-Word, 51, 127, 128, 136
 MS-Word bibliography file, 122
 MSIA, 116, 140, 154, 369, 371, 381
 Mueller, 189
 mule train, 90
 multi-factor authentication, 74, 89
 Multilevel Information Systems Security Initiative, 56
 multi-level marketing, 362
 multiple disk drives, 123
 multiple distribution lists not updated, 378
 multiplexers, 20
 Multi-Programming Executive, 118
mycpworld.com, 59
 MyLittleSecret, 22, 23

N

NACIC, 313
 NAI, 195
 Napoli, 226, 227
 narcissists, 263
 narrated PowerPoint about CATA, 166
 NAS Report, 182
 National Academy of Sciences, 182
 National Advertising Initiative, 195
 National Computer Security Association, 10
 National Computer Security Center, 276
 National Computer Security Conference, 253, 276
 National Counterintelligence Center, 313
 National Defense Authorization Act for Fiscal Year
 2000, 315
 National Infrastructure Advisory Council, 28
 National Initiative for Cybersecurity Careers and
 Studies, 181
 National Institute of Standards and Technology, 39
 National Institutes of Health, 148
 National Labor Relations Act, 360
 National Public Radio, 48
 National Research Council, 182, 279
 national security, 281
 National Vulnerability Database, 149, 248
 Naval Ocean Systems Center, 316
 NBC News, 69
 NCAs, 205
 NCH Software, 125
NCSA, 10, 223, 343, 349, 350
 NCSA Security Forum, 332
 NCSC, 150, 276
 NDA, 204
 need for civility, 258
 needs analysis, 291
 negligence, 111, 140
 NeoFace Monitor, 74
 netiquette training, 377
 Netscape Navigator browser, 346
 Network Anti-Spam Service, 343
 Network Associates, 98
 network center, 10
 network design, 149
 network diagrams, 5
 network management, 246
 network server, 14
 Network Solutions Inc., 98
 Network Systems Department, 316
 network topology/topologies, 22
 Network World, 118
 Network World Security Strategies, 301, 314
 network-monitor programs, 6
 network-security policies, 275
 NetworkWorld, 144
 Neumann, 36, 230, 251
 neuronal activity, 183
never executed, 93
 new exploits, 248
 new vulnerabilities, 248
 New York Times v. Sullivan, 68
 new-employee training, 146
 NewsScan, 29
 NIAC, 28, 29
 NICCS, 181
 Nigerian advance-fee fraud, 287
 NIH, 148
 Nimoy, 254
 NIST, 39, 75, 149, 253, 364
 no information shall be known to only one member of the
 team, 263
 No Lie MRI, Inc., 184

NOC, 11, 12, 14
 non-competition agreements, 205
 non-compliance, 276
 non-copy paper, 91
 non-disclosure agreement(s), 175, 177, 204, 330
 non-disparagement provisions, 204
 non-English character sets, 96
 nonexistent class name, 247
 nonindexed field, 107
 nonrepudiation, 53
 Nonrepudiation, 57
 norm of reciprocity, 286
 normalization, 307
 normal-use patterns, 131
 Norton Antivirus, 100
 Norwich University, 63, 116, 140, 147, 154, 181, 193, 365, 368
 Norwich University School of Graduate Studies, 116
 Nosy Parker, 189
 not invented here, 177
 notes to the interviewee, 160
 nothing to provide linkages, 303
 notice the emergency, 285
 notification, 199
 Nowak, 53
 NSO Group, 27
 NTBugtraq, 29
 nude photos, 1
 nudity, 158
null hypothesis, 63, 246, 267
 NVD, 149, 248, 249
 NVD filter categories, 248

O

OASIS, 108
 obedience, 277, 286
 object code, 11, 93, 351
 objective of problem-solving, 242
 objectivity, 158
 obligatory disclaimer, 203
 obscenities, 68
 obscenity, 330
 obsolescence, 108
 obstruction of correspondence, 81
 off-color humor, 366
 offend clients, 258
 Office Automation, 159
 Office of the Inspector General of the U.S. Department of Justice, 183
 Office of the National Counterintelligence Executive, 313
 official clearance from law enforcement, 377
 offshore spam, 345
 off-site backups, 129
 Olsen, 60
 on/off switch, 14
 ONCIX, 313
 ongoing management, 180
 online bug reports, 248
 online documentation, 265
 online sales systems, 340
 Open Archival Information System Reference Model, 108
 Open Invention Network LinuxDefenders, 341
 Open Source Zone, 341
 OpenPGP, 53

open-source intelligence, 314
 Opera, 29
 operating system(s), 23, 58, 92, 95, 109, 118, 122, 137, 228
 operating system security kernel, 301
 operating-system crashes, 107
 operating-system internals, 258
 operating-system patches, 150
 operating-system revisions, 118
 operational change, 159
 operational equivalent to truth, 246
 operational scale, 161
 operationally critical, 51
 operations, 3, 11, 15, 22, 57, 64, 77, 117, 135, 141, 234
 operations management, 1, 211, 275
 operations personnel, 12
 operations problem-solving timescales, 179
 operations staff members, 177
 Operations Support Group, 362
 operator, 20, 31, 35
 opt in, 195
 optical disks, 109
 optical-mark reader, 46
 optimization theory, 134
 opting-out, 195
 optional explanations using hypertext, 295
 opt-out, 4, 80, 194, 195, 196, 344
 Opt-Out Options, 195
 opt-out tool, 195
 ordinary skill, 340
 Orellana, 345
 Orenstein, 183
 organizational analysis, 160, 162
 organizational resistance, 275
 organized, 64
 organizing and presenting policies, 295
 origin, 53, 73, 86
 origin obscured, 97
 origin of attack packets, 224
 OSINT, 314
 OUCH! Newsletters, 250
 out of the office replies, 379
 outer walls, 13
 out-groups, 177, 253
 outliers, 178, 219
 Outlook Address Book, 95
 outside of firewall, 221
 Outstanding Paper Award, 276
 overkill, 234
 overlay, 58, 60
 overly broad patents, 340
 overpayment scam, 45
 Overprovision bandwidth, 114
 overreaction, 34
 oversight of the intern's work, 180
 overtemperature power cutoff, 20
 Overview of Creating and Managing CSIRTs, 249
 overwriting data, 229
 overwritten, 136
 ownership of email, 4

P

Pace University, 231
 packet checksums, 115

- packet checksums, 115
- packet intercepted, 150
- page jacking, 97
- paggers, 152
- Palin, 110
- PandaDoc, 53
- panic, 45
- panic button(s), 19, 20, 21
- panic switches, 19
- PanIP*, 340
- PanIP Defense Group, 340
- Panko, 63, 94
- paper ballot(s), 46, 47
- Pareto Principle, 134
- Paris Airshow, 315
- Paris subway system, 345
- parity errors, 108
- Parker, 1, 53, 114
- Parkerian Hexad, 1
- parking stub, 326
- partition disk drives, 123
- PASCAL, 301
- passcards, 74
- passphrases, 74
- passport, 54, 55, 56
- password, 22, 23, 36, 74, 75, 76, 78, 89, 90, 131
- password cracking, 223
- password expiration, 78
- password histories, 76
- password management, 78
- password on the projector, 227
- password stealing, 99
- password-cracking software, 232
- password-guessing, 76
- password-resetting process, 77
- password-safes, 89
- passwords, 6, 74, 75, 76, 77, 78, 89
- passwords expire, 76, 77
- passwords terrible methods for authentication, 278
- patch installation, 150
- patch reports, 248
- patches, 29, 118, 150, 311, 347
- patch-management, 150
- Patel, 350
- Patent Act, 340
- patent aggression, 341
- Patent Assertion Entities, 341
- patent trolls, 340
- patent-infringement claims, 340
- patents, 204, 340
- patient confidentiality, 148, 193
- patient records, 148
- patients, 18, 49, 148
- pattern of record-keeping, 212
- patterns, 74
- patterns of use, 152
- payload, 94
- PayPal, 45, 73, 88
- PAYSIMPLE, 151
- PDF*, 51, 108, 296, 298
- peak loads, 16
- Pearl Harbor Dot Com, 94
- peer-to-peer file sharing, 59
- Pegasus Project, 27
- penalties for non-compliance, 177
- penalty clauses, 137
- penetrate a security perimeter, 152
- penetration analysis, 137, 147, 153
- penetration testing, 152
- pen-testing, 152
- People's Liberation Army, 315
- perception management, 311
- perceptions of what is possible, 305
- performance, 48, 57
- performance analysis, 159
- performance reviews, 204
- performance tool, 107
- performance-enhancing indexes, 305
- perimeter, 5
- perimeter firewall, 222
- perimeter weakness, 221
- perimeters breached, 151
- period of reevaluation for employees, 180
- periodic changes of passwords, 75
- perjury, 52
- permission, 1, 24, 27, 28, 35, 38, 146, 189
- permuted keyword index, 214
- personal computer, 16
- personal firewalls, 228
- personal links, 39
- personal links on corporate website, 363
- personal worth, 35
- personal-information questions, 77
- personality, 177
- personality conflicts, 203
- personality style, 257
- personality traits helpful in operations, 175
- personality types, 256
- personally-identifiable information, 192
- personnel, 3, 57, 151, 249
- Personnel Office, 193
- personnel policies, 285
- person-to-person contact, 381
- petition, 329
- PGP, 53, 56
- phantomd, 230
- pharming, 197
- Philippines, 325
- philosophy of science, 246
- phishing*, 3, 27, 89, 94, 96, 137, 147, 197
- phone phreak, 310
- phone switches, 12
- phone-in consulting service, 264
- Phone-In Consulting Service, 240, 256
- phone-sex discussion groups, 360
- photo IDs, 74
- Photoshopping, 3
- physical abuse, 202
- physical access, 48
- physical security, 8, 11, 79, 290
- PICS, 256
- Pig Pen, 337
- PII, 192, 194, 195, 196, 197
- pinging, 154
- PKC, 53, 55, 148
- PKC certificate, 54
- PKI, 53, 54, 55, 56, 57
- PLA Strategic Support Force, 316

- plagiarism, 130
- plain-text, 51
- Planned Parenthood, 39
- planning, 8, 249
- planning penetration analysis, 153
- playing games, 238
- Playpen Gentlemen's Club, 337
- Podonsky, 230
- pointers to records, 306
- pointing out a vulnerability, 154
- pointing out security flaws, 154
- policies, 21, 63, 67, 149, 153, 155, 281, 296
- policies and procedures, 292
- policies to prevent abuse, 377
- policy, 23, 24, 34, 50, 57, 64, 142, 250
- policy document table of contents, 295
- politeness toward users, 261
- political orientation, 158
- polygraph, 182
- polygraphs as a tool for screening applicants, 182
- Ponzi Schemes, 4, 362
- pool management, 146
- poorly structured DB, 307
- poorly supervised children, 137
- pop up ads, 338
- pop-up windows, 59, 297
- porn ads, 98
- porn site, 59
- pornographic website, 59
- pornography, 23, 75
- porn-surfing, 141
- port scanners, 138
- port scans, 221
- portable computer(s), 16, 17, 129, 135
- Portable Document Format, 51, 298
- portable hard disk, 131
- portrait watermark, 91
- positive feedback, 379
- Postal Inspection Service, 361
- Postal Lottery, 362
- post-apocalyptic wasteland, 111
- post-apocalyptic world, 109
- post-employment terms, 205
- posting nonsense on social media, 358
- postmortem(s), 153, 154
- potential conflict of interest, 145
- potential conflicts, 217
- power, 65, 136, 220
- power bar, 15
- power cable unplugged, 15
- power cables, 18
- power conditioner(s), 10, 16, 17, 18, 220
- power cords, 14
- power failure(s), 15, 16, 17
- power fluctuations, 17, 18
- power of deception, 311
- power outage(s), 15, 16, 17
- power quality, 17
- power source, 20
- power-cord extensions, 15
- power-cord-out-of-the-socket virus, 15
- power-line monitor(s), 17
- practice responding, 146
- pranks or crimes perpetrated on mainframe systems, 226
- precise policy, 148
- preconceptions, 91, 157, 254, 255, 281
- pre-employment screening, 183
- prejudice, 176, 255
- prejudice about an ethnic group, 282
- prejudices, 68
- prejudicial communication, 158
- preliminary evaluation, 289
- preliminary inventory, 289
- preparation, 146, 147
- preparation for firings, 203
- prepare for social-engineering simulations, 147
- preparing for penetration test, 147
- prescription, 77, 90
- prescription for failure, 91
- prescription-pad, 91
- prescriptive policies, 294
- president, 35, 67
- pressure software firms, 345
- Pretty Good Privacy, 53
- prevent abusive language about customers, 261
- preventative maintenance schedules, 173
- preventing backups, 142
- primary key, 107
- primary reference, 110
- Princeton University, 48
- principle(s), 26, 29, 35, 73, 80, 84, 153, 370
- principles for effective teaching, 265
- principles of effective training, 239
- principles of human social behavior, 276
- principles of pen-testing, 152
- printers, 11, 20, 51, 54
- prior approval of the content, 332
- prior brainstorming, 161
- privacy, 1, 4, 5, 22, 135, 148, 192, 193
- Privacy & Security Brainiacs, 252
- privacy policy(ies), 5, 151, 193, 192, 196
- privacy rights, 4
- Privacy Rule, 148
- privacy-breaching error, 197
- privacy-protection, 197
- private key, 53, 57
- privilege, 35
- probabilistic models, 216
- probability(ies), 63, 81
- probability of death, 215, 216
- probation for the error-prone or the lazy, 180
- probation not an option for untrustworthy employees, 180
- probationary period, 180
- probationary period for an untrustworthy employee, 180
- probationary period for under-performing employees, 180
- problem manager, 265
- problem reports, 118
- problem solving, 238
- problem-escalation procedure, 259
- problem-solving*, 160, 185, 214
- process, 3, 56, 67, 68, 287
- process-control system, 22
- Prodigy*, 108, 357
- production*, 35, 62, 136, 146
- production code, 47
- production disks, 150
- production spreadsheets, 63
- production staff, 190

production systems, 12, 16, 22, 92, 136, 190
 productivity, 33, 79, 196
 profanity, 332
 professionalism, 157, 332
 professionalism of prospective consultants, 157
professionals, 137, 180, 248
 professorial beagle, 111
 programmer bribed by competitor, 234
 programmers, 92, 301
 programmers duplicate data, 304
 programming, 12, 63, 327
 programming errors, 48
 programming languages, 301
 programming managers, 146
 programming timescales, 179
 progress reports, 259
 Progress Towards Autonomy, 159
 propaganda network, 334
 properties sheet, 51, 126
 property sheets, 113
 proprietary code, 233
 proprietary cryptography, 11
 proprietary formats, 54
 proprietary programs, 47
 proscriptive policies, 294
 prosecution, 23, 76, 135
 prosecution of spammers, 344
 protect intellectual property, 205
 protecting organization's reputation, 357
 protective ducts, 18
 protocol, 367
 provably correct program design, 48
 provably secure, 48
 provisional diagnosis, 280
 proximity devices, 79
 proximity sensors, 13
 proxy privileges, 52
 pseudonym, 69, 371
 psychiatric help, 219
 psychological dangers, 202
 psychological impact, 199
 psychological operations, 311
 psychological stress, 189
 psychologically disturbed adults, 137
 PSYOPS, 311
 public commentary, 332
 public domain, 341
public key, 53, 54, 55, 56, 57, 148
 Public Key Cryptosystem, 45, 53, 148
 Public key infrastructures, 53
 public keys, 56
 public policy, 28
 public relations, 151
 public workstation, 226
 publicity, 30, 86, 203
 public-key infrastructure, 51
 public-relations, 37
 publish research on viruses, 350
 publishing errors, 358
 publishing lies, 358
 publishing rumors, 358
 publishing termination procedures, 202
 publishing virus code, 350
 pump 'n' dump, 86

pumps, 18
 punch cards, 64
 punitive responses to errors, 263
 Putin associate, 312
 pyramid, 4
 pyramid sales fraud, 361

Q

QAnon, 69, 336
 QoS, 107, 261, 264
 quality assurance, 47, 48, 63, 93, 94, 114, 135, 143, 166, 190, 211, 246, 327, 345
 quality assurance failure, 345
 quality assurance truism, 155
 quality control, 64, 141, 211, 263
 quality control supervisor, 173
 quality of service, 261
 quality-assurance, 63, 136
 quality-assurance process, 93
 quantitative estimates using expert opinions, 160
 quantitative risk management, 215
 quantitative risk-management techniques, 216
 quantum computing, 181
 quarterly bottom lines, 231
 quarterly bottom-line, 232
 query program, 306
 question anomalies, 173
 question the candidate closely, 175
 questionnaires, 283
 Quick IP List, 344
 QuickMBA, 205

R

race(s), 75, 158, 176
 racism, 68, 176, 203
 Radikal, 37
 RadLightI, 62
 RAID, 15, 124, 186
 railroad, 9
 raise awareness, 259
 raised floors, 14
 raised printing, 91
 RAND Corporation, 160, 311
 random access, 307
 random punctuation, 342
 random-access reads, 107
 randomized data, 136
 randomly generated subject, 94
 ranges of costs, 216
 rank the estimates, 160
 ransomware, 3, 107, 129, 130, 137, 311
 ransomware protection, 201
 ratio of throughput to cost of ownership, 173
 RDBM, 303
 RDBMS, 303
 realistic examples, 282
 Reality overrides theory, 91, 219
 real-life examples, 281
 real-time access, 160
 real-time backup, 129
 Realtime Blackhole List, 343
 real-time information, 221

- Real-Time Notes, 160
- real-time record, 215
- reasonable hypotheses, 246
- reasonable ranges of probabilities, 216
- reasoned exchange of views, 157
- reboot, 98
- rebooted, 118
- rebuild morale, 232
- rebuilding software configuration, 130
- reCaptcha, 92
- recipients, 36, 45, 50, 81, 86
- recommendations, 15, 144, 341
- record, 63, 86, 88
- record layouts, 307
- record of suggested improvements, 153
- record-level locking, 302
- recording, 90, 158
- records, 3, 22, 64, 148
- records management, 108
- records or rows or tuples, 306
- records, relations, rows, tuples, 307
- recounts, 46, 47
- recover attorney's fees and costs, 361
- recover data from *AES* diskettes, 108
- recovery scams, 310
- recovery strategies, 303
- recycling bins, 113
- Reddit, 69
- Redesi* worm, 94
- redirect script, 97
- redirection, 110
- Redscan, 248
- reduction in pay, 232
- redundancy, 186
- redundancy a requirement for managing personnel, 186
- redundancy at every level, 234
- redundancy rule, 263
- Redundant Arrays of Independent Disks, 15
- referential integrity constraints, 308
- reformat hard drives, 95
- refund*, 27, 45
- refund scam, 45
- refund scams, 100, 310
- refusing cookies, 195
- regulatory-framework review, 29
- rehire this employee, 174
- reinforcement, 142
- re-initialize temporary storage, 302
- rejecting *legitimate* traffic, 223
- rejecting the null hypothesis, 246
- relational database management system, 303
- relational database model, 303
- relational model, 305
- relations, 306
- relationships or links, 306
- relative humidity, 20
- religion, 65, 68, 158, 176
- reload the operating system, 258
- remote-access server, 22
- remote-access software, 27
- replace outmoded policies, 296
- replacement personnel, 199
- REPLY ALL, 368
- report at the same level, 143
- report directly to the CEO, 143
- report failures, 261
- report spam, 100
- reporting the dishonest agent, 264
- reports, 62, 74, 162, 305, 315
- reports on progress, 159
- reprimands, 286
- Republicans, 67, 69
- repudiate, 53, 57
- repudiate forged versions, 327
- reputation, 39, 86, 157, 177, 194, 197
- reputation of trademarks, 339
- Request for Proposal, 156
- Requests for Comments, 380
- require polygraph tests, 174
- research reports, 314
- resentment, 205
- reset password, 223
- residual magnetic fields, 230
- resignation(s), 198, 199, 200, 202, 204, 205
- resist anti-security bias, 286
- resistance to progress, 178
- resisting social-engineering, 153
- resource limitations and dependencies, 154
- resource-usage optimization, 238
- resources for tracking cyberattacks, 309
- resources from the SEI, 249
- respirators, 18
- respond intelligently, 151
- respond to a DDoS attack, 114
- responded constructively, 349
- responding, 77, 249
- responding to Chinese industrial spam, 318
- responding to false alarm, 225
- responding to termination of employment, 200
- response to complaints, 196
- response-time statistics, 241
- responsibilities, 164
- Responsibilities to the Client, 158
- responsibility*, 25, 30, 57, 112, 113, 135
- restricting email, 377
- restricting illegal downloads, 337
- retinal patterns, 74
- retract, 30
- Reva Networks, 59
- revanetworks.com, 59
- revenge, 151
- revenge attacks, 224
- revenge plot, 201
- Revere, 110
- reverse IP-block lookup, 62
- revise estimates, 161
- revocation, 54, 57
- revocation management, 57
- reward rather than punishment, 283
- rewards and punishments important motivators, 283
- RFCs, 380
- RFP, 156
- Rich Text Format, 51, 297
- right to privacy, 330
- Rights and Protections under the Employee Polygraph Protection Act of 1988, 183
- rising temperature, 20
- risk analysis, 220

risk assessment, 5
 RISKS Digest, 36, 309
 RISKS DIGEST, 110, 345
 Risks Forum, 140, 251
 RISKS Forum Digest, 63
 road access, 9
 robot, 257
 rock-climbing, 14
 Rockstar Video, 337
 Rocky & Bullwinkle & Friends, 111
 Rocky and His Friends cartoon, 111
 rogue software, 6
 rogue webpage, 59
 role models, 233
 role-playing, 153, 258, 259, 281
 role-playing games, 147
 roles, 249
 roles of social engineer, 147
 rollover problem, 117
 Roman Empire, 311
 root access, 35
 root certificate authority, 56
 root of insecurity, 177
 root passwords in a safe, 190
 root user, 223
 rotate personnel, 191
 rotating staff, 192
 Rounds, 39
 routers, 22, 54, 114, 115
 routing tables updated, 374
 Royal Canadian Mounted Police wiretaps, 115
 RTF, 51
 Rubens, 114
 RUNOFF, 109
 Russian, 45
 Russian alphabet, 96
 Russian Blue kitten, 82
 Russian government, 312
 Russian hackers, 312
 Russian Internet Research Agency, 312
 Russian military intelligence, 312
 Russian PSYOP, 312
 Rwanda, 12

S

sabotage, 38, 189
 safe, 11, 15, 144
 safe hex, 288
 safeguards on file contents, 304
 safety, 10, 87, 145
 safety glass, 13
 safety regulations, 12
 Saliency, 255
 sample anonymized reports, 157
 sanctions, 286
 sandbox, 301
 Sandia National Laboratories, 316, 317
 SANS NewsBites, 250
 SANS newsletters, 250
 SANS@Risk, 250
 SATAN, 27
 saturating communications channels, 379
 scalability, 57

Scalability, 55, 57
 scam, 4, 31, 81, 84, 85, 86
 scams, 45, 89
 scandal, 112
 scanning, 28, 50, 74, 342
 SCAP, 149
 scavenging, 32, 112, 173, 302
 schema, 277, 281
 schemas, 253, 254, 277, 281
 schemas can be challenged, 282
 Schiller, 369
 Schneier, 145, 146, 251
 Scholarship for Service, 181
 Schwartz, 94, 309
 Schwartz, 27
 Science, 148
 SCIF, 90
 scratch tapes, 173
 scream obscenities, 159
 screen icons, 128
 screenshot(s), 45, 51, 52
 scribe, 160, 264
 script, 39
 script kiddie, 348
 scripting language(s), 137
 scumware, 58, 59, 60, 61, 62
 Scumware, 45
 Seagal, 224
 sealed envelope, 190
 sealing passwords into opaque envelopes, 187
 search, 61, 84, 309
 search engine(s), 92, 97, 99, 110, 197
 searchable PDF, 247
 SEC, 111, 361
 SEC Criminal Investigation Division, 112
 second law of thermodynamics, 16
 secondary UPSs, 220
 second-hand information, 244
 second-order abstraction, 305
 secret key, 53, 148
 secret operations, 188
 Secrets and Lies, 145
 Secure Electronic Transactions, 56
 secure perimeter, 12
 secure screen savers, 232
 secure shredding, 112
 Secure Sockets Layer, 150
 secure wiping, 229
 Securities and Exchange Commission, 111, 112, 361
 security analysis, 160
 security architecture, 148
 security auditor, 10
 security awareness, 282, 290
 security best practices, 301
 security by obscurity, 5
 security checklist, 149
 Security Content Automation Protocol, 149
 security drills, 146
 security evaluation, 18
 security is a process, 146, 166
 security management, 77
 security policies, 24
 Security Procedures, 294
 security through obscurity, 11

- security-awareness posters, 296
- security-awareness programs, 142
- security-awareness training, 135
- sedition, 330
- see what we wanted, 155
- SEI, 248
- selecting candidates, 176
- self-explanatory, 31
- self-flagellation, 153
- Self-Handicapping, 255
- Self-Serving Bias, 255
- sell information about consumers, 361
- sell prospects' names for profit, 195
- selling customer data, 151
- send delay, 368
- send essential personnel away, 234
- sense of discomfort, 153
- sense of involvement, 294
- sensitive compartmented information facilities, 90
- sensitive systems, 290
- sensitivity analysis, 216
- sensor, 225
- sentenced, 27
- separation of duties, 35, 135, 190, 191
- sequence numbers, 47, 115
- Serif MonsterCD, 125
- server, 11, 37, 79, 136
- server firewall, 317
- service bureau, 150, 190
- service contract, 17
- service providers, 197
- service-level agreement, 107
- Service-Level Agreement, 141
- servicemark, 197
- SET, 56
- settlement, 52
- sex trafficking, 69
- sexism, 176, 203
- sexual harassment, 52
- sexual orientation, 158
- sexually explicit conduct, 323
- sexually suggestive images, 158
- SFS, 181
- SGS, 116
- Shared Peripheral On Line, 16
- shared spreadsheet, 161
- Shared/Simultaneous Peripheral Operation On Line, 304
- shares, 67, 86
- shareware, 61
- Shelat, 229
- Sherman, 111
- shift the normative values, 286
- shifting blame, 225
- shills, 360
- Shipley, 27
- shoddy treatment of employees, 202
- shoot children, 359
- Short Message Service, 89
- shortcut to creating new message, 370
- short-term goals, 242
- short-term perspective, 232
- short-term profit, 231
- shoulder-surf, 89
- shoulder-surfing, 227
- Shred Nations, 112
- shredding, 111, 112
- side channels, 90
- Sidewalk, 38
- SIGINT, 314
- signals intelligence, 314
- signature-based antivirus, 342
- signing key, 56
- signing keys, 56
- SIGs, 262
- Silberman, 184
- Simon, 48
- Simple Mail Transfer Protocol, 99
- simulate distress, 146
- simulate initial logon dialogue, 226
- simulate logoff message, 226
- simulation, 146
- Singapore Telecom, 27
- Singer, 230
- SIRCAM, 376
- Skype, 90, 381
- SLA, 107, 141
- slab-to-slab walls, 14
- slander, 333
- slave programs, 28
- sleep, 19
- sliding doors, 13
- slow scans, 76
- Smart Tags, 58
- smash-and-grab, 10
- smoke, 9, 18, 19, 21
- smoke sensors, 14
- SMS, 89, 90, 135
- SMTP, 99
- Sneakers, 283
- snipers, 13
- SNOPES*, 66, 366
- Snuffle, 350
- social cognition, 253
- social engineering, 32, 140, 146, 147, 153
- social engineering attacks, 232
- social media, 3, 67, 68, 70, 75, 360
- social psychologist, 253
- social psychology, 253, 276, 288
- Social Psychology and INFOSEC, 276
- social responsibility, 114, 137
- Social Security Number, 148
- Social Security Number(s), 148, 310
- Social Styles Series, 255
- social-engineering techniques, 153
- social-engineering training, 147
- socio-economic profile, 9
- sociopaths, 156
- soft-drink delivery man, 277
- Software Engineering Institute, 248
- software engineering, 48
- software for tracking incidents, 240
- Software Publishers' Association, 284
- Software Status Bulletin, 118
- software testing, 24
- software upgrade, 108
- software-acquisition lead times, 179
- software-update process, 24

- solid-state drives, 124
- sort by variance, 161
- sort lines of text, 162
- sorted, 63, 213
- source code, 11, 264
- source.xml, 122
- SourceForge, 215
- spam, 3, 36, 52, 59, 79, 80, 91, 92, 318, 342, 344, 361, 375, 377
- spam from industrial companies, 318
- spam-filtering software, 342
- spam-recognition, 343
- spare disk packs, 150
- Special Interest Groups, 262
- Special Operations and Low Intensity Conflict, 313
- speed, 61
- speed access, 306
- spikes, 18
- Spock, 254
- spoof, 65, 117
- spoof originating IP address, 223
- spoofed originator addresses, 114
- SPOOL, 304
- spoolfile(s), 173, 247
- pooling, 16
- spreading knowledge, 186
- spreadsheet, 62, 63, 94, 137, 161
- spreadsheet errors, 62, 63, 94
- spreadsheets, 45, 62, 63
- spurious claims, 340
- spyware, 3, 27, 28, 62
- SQ3R*, 266
- SQL, 305
- SRI International, 251
- SSD, 124
- SSDs, 124
- SSL, 150, 151
- SSL certificate, 151
- SSN, 148
- SSNs, 148
- stairwells, 18
- stalking, 158
- standard operating procedures, 34
- standards of appropriate behavior, 357
- standards of the auditing profession, 143
- standby, 19
- standby power systems, 20
- Stanford University, 110
- state library, 39
- statements, 89
- static electricity, 20
- statistics, 12, 148, 279
- statistics about information security, 134
- steal dinosaur embryos, 234
- stealth, 23
- stealth mode, 24
- stealth-mode software, 23
- steganography, 90
- stereotypes, 255
- sticker, 80, 81
- stimulate group discussion, 369
- sting operation, 186
- stock manipulation, 32, 86
- stonewallers, 30
- storage, 57, 136
- storage area, 14
- storage room, 108
- storage tanks, 9
- store repeated information, 304
- strategic planning, 141
- Strategic Support Force, 316
- Stratus Technologies, 186
- structure, 8
- Structured Query Language, 305
- student interns, 180
- students, 36, 62, 64, 110, 130, 270, 348
- students supervised, 181
- students vetted, 181
- students write malicious code, 348
- stupid rule, 36
- stupidest question, 368
- stupidity, 30
- stupidly published, 30
- style in policy documents, 275
- Subcommittee on Oversight and Investigations, 230
- subject lines, 95, 342
- subject lines of spam, 342
- subpoena, 224
- subset of available information, 254
- succession planning, 216
- succession plans, 216
- sudden unavailability of key people, 216
- sudden wealth, 189
- suggestions for improvement welcomed, 186
- SULFNBK hoax, 64
- Sumerian cuneiform, 247
- summary of countermeasures, 99
- Superman, 6
- supply-chain management, 211, 223
- support from upper management essential, 291
- supporting autocratic movements, 358
- Supreme Court, 68, 323
- Surf and Keep, 58
- surge suppressor, 18
- surge-suppressor, 16
- surveillance, 28, 74, 234, 314
- surveillance software, 27
- surveys on computer crime, 134
- suspend alarms, 222
- suspended ceilings, 18
- Swedish University Network, 38
- switch, 15, 17, 69
- switch roles, 259
- switches, 18
- synchronization, 122, 129, 130
- synchronous* communication, 90
- synonyms for keywords, 342
- sysops, 332
- system documentation, 113
- system failures, 130, 173, 257
- system management, 78, 152
- system manager, 150
- system operators, 332
- system personnel, 150
- system registry, 59
- system testing, 150
- systematic problem-solving, 211, 259
- system-manager capabilities, 190

Systems Status Bulletin, 347
systems-engineering manager, 141

T

tables, 306
tactical warning, 311
take responsibility, 259
talking loudly, 32
tampering, 18, 47, 49, 53, 81
Tandem, 186
TANSTAAFL, 239
tape backups, 20
tapes, 108, 145
target, 58, 62
target categories for cyberattacks, 137
Task Force on Outreach and Education, 110
TCB, 92
TCP address, 62
TCP/IP, 53, 136
teacher management, 211
teacher variables, 269
technical support, 36, 76, 213, 238, 240
technical-support group, 293
TEITNO, 240
telecommunications-network expansion, 238
telecommunications-network monitoring, 238
telephone calls, 152
telephone game, 64, 244
telephone numbers, 27, 126
temperature sensor, 20
temperatures, 21
templates, 127, 157
term paper, 130, 131
Terminal Compromise, 94
terminate sessions remotely, 142
terminating employment, 199
termination, 25, 74, 199, 201
termination of access, 78
termination policies, 202
termination style, 202
terroristic threat, 359
test, 27, 62, 75, 91, 190, 315
test address, 197
test assumptions, 37
test challenges the system, 155
test coverage, 93, 136
test our assumptions, 91
test perceptions, 157
test security, 146
test the updated system, 150
test version, 242
testing operational resilience, 188
testing software before production, 155
testing their own creation, 155
textbook on elementary statistics, 242
The Hacker News, 309
The Piranha Brothers, 117
The Polygraph and Lie Detection, 182
The Register, 317
theft of identity, 87
theft of services, 137
themes, 162
themes sorted by category, 163
theory for organizing data, 304
there ain't no such thing as a free lunch, 239
thermal contractions and expansions, 19
thermal disruption of magnetic domains, 108
thermostat, 20
thief, 73, 89, 131
thiefware, 58
think independently, 157
third-world country, 145
thorough preparation, 146
threat, 8, 33, 66, 92, 140
threat models, 49
threat of physical harm, 158
threat to kill, 159
threaten dismissal, 204
threatening email, 87
threats, 75, 156, 249, 336
threat-scoring, 28
Ticketmaster, 38
TIFF, 108
tiles, 21
TIME Magazine, 316
time to first answer by helpdesk, 241
time-limit for level of support, 259
time-management, 258
time-sensitivity, 261
timeout(s), 78, 131
timeout doubles, 76
timestamps, 47
timing, 191
timing in employee relations, 203
timing unannounced, 146
Tips of the Month, 252
TITAN RAIN, 316
tokens, 22, 74, 77, 78, 135
tool for capturing keystrokes, 226
toolbar(s), 22
top 30 vulnerabilities, 150
top-down hierarchical structure, 56
top-down hierarchy, 56
TopText, 59
TotalNews, 97
touch-sensitive, 46
tower computer, 129
toxic waste dumps, 9
tracking incidents, 238
tracking incidents by CSIRTs, 240
trade secrets, 175
trademark, 197
trademark infringement, 337, 338
trademarks, 73, 79, 99
trail, 23, 131
training, 6, 126, 286
training and awareness exercise, 147
training replacements, 200
training tech-support staff, 238
training tools, 262
transformation of corporate culture, 293
transgender rights, 364
transient over voltage, 18
transsexuality, 39
transvestism, 364
transvestite, 39
Traynor, 224

Trend Micro, 343
 tricking employees, 146
 Trojan, 48, 124, 348
 Trojans, 136
 trolls, 312, 334
 Tropical Storm Irene, 10
 trouble catching one's own errors, 155
 Trumpist lies, 335
 TruSecure, 343
 trust, 49, 53, 54, 66, 81, 87
 Trusted Computing Base, 92
 trustworthiness, 47, 137
 trustworthy soft-drink delivery man, 277
 trying to do in operational terms, 243
 tunneling, 374
 two-factor authentication, 22
 typing errors, 59

U

U.S. Army Space and Strategic Defense, 316
U.S. Code Chapter 41, 323
U.S. Code Title 35, 340
 U.S. Court of Appeals for the Ninth Circuit, 337
 U.S. Cybersecurity & Infrastructure Security Agency, 28
 U.S. Identity Theft: The Stark Reality, 87
 U.S. Postal Service, 339
 U.S. Senate Intelligence Committee, 312
 UCLA School of Law, 67
 UK National Cyber Security Centre, 150
 unannounced drills, 146
 unauthorized access, 21
 unauthorized disclosure, 140, 151
 unauthorized link, 38
 unauthorized penetration, 224, 325
 unauthorized penetrations, 221
 unauthorized release of data, 151
 unauthorized software, 24
 unauthorized software on public terminals, 226
 unbiased questionnaires, 289
 uncontrolled environment, 26
 under-floor area, 14
 undesirable materials on official systems, 377
 undocumented code, 47, 92, 93, 94
 undocumented system is time bomb, 233
 unexpected attachment, 376
 unexpected errors, 155
 unexpectedly angry, 188
 unexpectedly cheerful, 188
 unexpectedly depressed, 188
 unexpectedly friendly, 188
 unexpectedly happy, 188
 unexpectedly hostile, 188
 unfair competition, 339
 Uniform Code of Military Justice, 332
 Uniform Trade Secrets Act, 175
 uninformed victims, 376
 uninterpretable URL, 89
 uninterruptible power supplies, 16
 unique case identifier, 213
 unique resources cause risk, 186
 United States Postal Inspection Service, 339
 United States v. Alvarez, 68
 universal vulnerability, 250
 Université nationale du Rwanda, 12
 University of Calgary, 348
 University of California San Diego, 49
 University of Chicago, 366
 University of Vermont Medical Center, 107
 Unlawful Access to Stored Communications Act, 224
 unlawfully overheard electronic communication, 323
 unlock a sequence of locks, 302
 unlock code for projectors, 227
 unnoticed breaches of security, 221
 unsecured medical devices, 49
unsend a message, 368
 unsolicited commercial email, 3, 36, 79, 342, 377
 unsolicited faxes, 86
 unstable URLs, 110
 unsubscribe, 101, 194
 unsubscribe link, 198, 343
 untested, 48
 untrained personnel, 113
 unusual activity, 152
 unusual *behavior*, 189, 190
 unusual patterns of system use, 152
 unverified reports, 143
 updating a directory structure, 15
 upgrades, 24
 upload assignments, 381
 UPS, 16, 17, 18
 UPS batteries drained, 220
 UPSs, 16, 17, 220
 URL, 97, 110
 usability, 8, 48
 usage errors, 382
 USB drives, 16
 use and abuse of polygraph testing, 182
 Use of Polygraph Examinations in the Department of Justice, 183
 used disk drives, 229
useful, 23, 58, 64, 74, 78, 111, 158, 252
 useful information on the Web, 346
 useful security tip in a corporate newsletter, 287
usefulness of data, 122
 user ID, 76
 user identifier, 74
 users as *customers*, 260
 user-satisfaction surveys, 241
 uses of fMRI, 184
 USPIS, 339
 USPS Forever stamps, 339
 utility, 107, 309
Utility, 2, 122
 UTSA, 175
 UVM Medical Center, 107

V

vaccination, 67
 vacuum cleaner, 18
 validation and verification, 190
 Valimail, 99
 value-added networks, 357
 Van Damme, 224
 VANs, 357
 variance of the CAC scores, 161
 variant spellings, 99

VAs, 221
 vaults, 10, 11
 vehicle barriers, 5
 vendor(s), 3, 21, 59, 75, 88, 150
 verbal abuse, 202
 verification, 53, 57, 64, 88
 verifying accuracy and appearance of output, 238
 Vermont House Committee on Government Operations
 and Military Affairs, 46
 Vermont State Offices Complex, 10
 version, 36, 63, 129
 version numbers, 126
 vicarious liability, 337
 victim of social engineering, 146
 victim status, 158
 victims, 3, 45, 84, 85, 86, 87, 88, 137
 video tapes, 145
 Vienna Art History Museum, 224
 viewing pornography, 238
 vigilance, 49, 88, 147
 violate corporate policies, 24
 violating Acceptable-Use Policy, 147
 violating netiquette, 358
 violations of privacy, 92
 violations of security policies, 150
 Virginia Supreme Court, 361
 virtual drives, 123
 virtual machine, 301
 virtual private networks, 34
 Virtual Private Networks, 374
 virtual-memory swapping, 124
 virus, 27, 48, 58, 64, 65, 93, 348
 virus in printer, 365
 virus payload, 93
 virus warning, 94
 virus writing illegal, 349
 viruses, 3, 24, 93, 136, 348
 vision panels, 13
 visitor, 35, 39
 visitor control, 5
 voice over IP, 87
 voicemail, 90
 voice-over-IP, 100
 VoIP, 100
 Volokh, 67, 68
 volume, 57, 137
 volume of traffic, 99
 volume testing, 114
 voluntary response, 134
 voting, 47, 48, 49
 voting machines, 46
 VPN, 374
 VPN tunneling, 374
 VPNs, 34, 136
 vulnerability(ies), 1, 8, 27, 28, 29, 114, 136, 146, 149, 150,
 221, 250
 vulnerability analysis, 152
 vulnerability definition, 250
 vulnerability disclosure, 28
 vulnerability disclosure for a fee, 346
 Vulnerability Disclosure Framework, 28
 vulnerability information, 28
 vulnerability management, 28, 29, 149

Vulnerability Notes Database, 149, 249
 vulnerability of users, 137
 vulnerability scans, 27, 316
 vulnerability to electronic warfare, 309
 vulnerability to phishing, 95
 vulnerability trends, 248
 vulnerability-assessment, 221

W

WABAC Machine, 111
 walls, 10, 12
 warning(s), 30, 39, 58, 64, 68, 81, 86, 90, 91, 117, 376
 warning signs, 18, 46
 Washington Post, 74
 water, 136
 water leakage, 14
 water sensors, 14
 waveform deformations, 18
 Wayback Machine, 110
 WayBack Machine, 111
 weaknesses in security configurations, 221
 weather patterns, 8
 Web hijacking, 98
 Web hosting, 197
 Web of trust, 56
 Webmaster, 59
 webpage, 22, 58, 60, 61
 webpage hijacking, 96
 websites, 10, 92, 111, 137, 193, 364
 Weekend Edition, 48
 weekly reports, 181
 Weiner, 254
 Westmount Municipal Pool, 146
 WhatsApp, 27
 white-collar crime investigation, 112
 white-hat hackers, 49
 WHO, 66
who is supposed to do *what*, 265
 WHOIS, 86, 96, 317
 Whole-Language Movement, 381
 Wiegand cards, 79
 Wikipedia, 110
 Will brain imaging be lie detector test of the
 future, 184
 Willis, 13
 Wilson Learning, 255, 257
 Wilson typology, 257, 258
 windows, 12, 13, 225
 Windows, 6, 13, 22, 78, 109, 122, 215, 226
 Windows 9x crash frequency, 117
 Windows 9x crashing, 117
 Windows 9x kernel, 118
 WinZIP, 136
 wiping disks, 229
 wire fraud, 98, 322
 wire transfer, 45
 WIRED, 309
 wiring, 14, 17
 Wizop, 332
 Wolpe, 183
 Wood, 292
 wooden cane, 20

word of mouth, 261
WordPerfect, 51, 108, 109
WordPress, 98
work at home, 204
work with outliers, 289
Worker Adjustment and Retraining Notification Act, 203
working for direct competitors, 205
working memory, 166
workplace safety regulations, 18
workstation, 6, 23, 79, 136
World Health Organization, 66
World Trade Center, 18
World Wide Web, 3, 38, 332
worms, 3, 348
worms using misleading subject fields, 376
WPD, 51
write-access to a website, 98
writing advice, 381
writing secure code, 301
written authorization, 146
wrong target, 224
wrongful dismissal, 204

X

X.500, 54, 55
X.509 version 3, 55
XLS, 62
XLSX, 136
XML, 108
XyLoc, 79

Y

Yahoo, 115, 116, 117

Z

ZDV, 27
zero-day exploits, 152
zero-day vulnerabilities, 27
Zimmerman, 53
zombie, 114
zombie software, 137
ZOOM, 34, 160, 251