

# **COMPUTER SECURITY HANDBOOK**

# **COMPUTER SECURITY HANDBOOK**

Fifth Edition

Volume 1

**Edited by**

**SEYMOUR BOSWORTH**

**M.E. KABAY**

**ERIC WHYNE**



**WILEY**

**John Wiley & Sons, Inc.**

Copyright © 2009 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, 201-748-6011, fax 201-748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** While the publisher, editors, and the authors have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher, the editors, nor the authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at <http://www.wiley.com>.

***Library of Congress Cataloging-in-Publication Data***

Computer security handbook. – 5th ed. / edited by Seymour Bosworth, M.E. Kabay, Eric Whyne.

p. cm.

Includes index.

ISBN 978-0-471-71652-5 ((paper) (set)) – ISBN 978-0-470-32722-7 ((vol 1)) – ISBN 978-0-470-32723-4 ((vol 2)) 1. Electronic data processing departments—Security measures. I. Bosworth, Seymour. II. Kabay, Michel E. III. Whyne, Eric, 1981–  
HF5548.37.C64 2009  
658.4'78—dc22

2008040626

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

# CONTENTS

**PREFACE**

**ACKNOWLEDGMENTS**

**ABOUT THE EDITORS**

**ABOUT THE CONTRIBUTORS**

**A NOTE TO INSTRUCTORS**

## **PART I FOUNDATIONS OF COMPUTER SECURITY**

- 1. Brief History and Mission of Information System Security**  
Seymour Bosworth and Robert V. Jacobson
- 2. History of Computer Crime**  
M. E. Kabay
- 3. Toward a New Framework for Information Security**  
Donn B. Parker
- 4. Hardware Elements of Security**  
Seymour Bosworth and Stephen Cobb
- 5. Data Communications and Information Security**  
Raymond Panko
- 6. Network Topologies, Protocols, and Design**  
Gary C. Kessler and N. Todd Pritsky
- 7. Encryption**  
Stephen Cobb and Corinne Lefrançois
- 8. Using a Common Language for Computer Security Incident Information**  
John D. Howard
- 9. Mathematical Models of Computer Security**  
Matt Bishop

**vi CONTENTS**

- 10. Understanding Studies and Surveys of Computer Crime**  
M. E. Kabay

- 11. Fundamentals of Intellectual Property Law**  
William A. Zucker and Scott J. Nathan

**PART II THREATS AND VULNERABILITIES**

- 12. The Psychology of Computer Criminals**  
Q. Campbell and David M. Kennedy

- 13. The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns**  
Jerrold M. Post

- 14. Information Warfare**  
Seymour Bosworth

- 15. Penetrating Computer Systems and Networks**  
Chey Cobb, Stephen Cobb, and M. E. Kabay

- 16. Malicious Code**  
Robert Guess and Eric Salveggio

- 17. Mobile Code**  
Robert Gezelter

- 18. Denial-of-Service Attacks**  
Gary C. Kessler and Diane E. Levine

- 19. Social Engineering and Low-Tech Attacks**  
Karthik Raman, Susan Baumes, Kevin Beets, and Carl Ness

- 20. Spam, Phishing, and Trojans: Attacks Meant To Fool**  
Stephen Cobb

- 21. Web-Based Vulnerabilities**  
Anup K. Ghosh, Kurt Baumgarten, Jennifer Hadley, and Steven Lovaas

- 22. Physical Threats to the Information Infrastructure**  
Franklin Platt

**PART III PREVENTION: TECHNICAL DEFENSES**

- 23. Protecting the Information Infrastructure**  
Franklin Platt

- 24. Operating System Security**  
William Stallings

- 25. Local Area Networks**  
Gary C. Kessler and N. Todd Pritsky
- 26. Gateway Security Devices**  
David Brussin and Justin Opatrny
- 27. Intrusion Detection and Intrusion Prevention Devices**  
Rebecca Gurley Bace
- 28. Identification and Authentication**  
Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs
- 29. Biometric Authentication**  
David R. Lease, Robert Guess, Steven Lovaas, and Eric Salveggio
- 30. E-Commerce and Web Server Safeguards**  
Robert Gezelter
- 31. Web Monitoring and Content Filtering**  
Steven Lovaas
- 32. Virtual Private Networks and Secure Remote Access**  
Justin Opatrny
- 33. 802.11 Wireless LAN Security**  
Gary L. Tagg
- 34. Securing VoIP**  
Christopher Dantos and John Mason
- 35. Securing P2P, IM, SMS, and Collaboration Tools**  
Carl Ness
- 36. Securing Stored Data**  
David J. Johnson, Nicholas Takacs, and Jennifer Hadley
- 37. PKI and Certificate Authorities**  
Santosh Chokhani, Padgett Peterson, and Steven Lovaas
- 38. Writing Secure Code**  
Lester E. Nichols, M. E. Kabay, and Timothy Braithwaite
- 39. Software Development and Quality Assurance**  
John Mason, Jennifer Hadley, and Diane E. Levine
- 40. Managing Software Patches and Vulnerabilities**  
Peter Mell and Karen Kent

**viii CONTENTS**

- 41. Antivirus Technology**  
Chey Cobb and Allysa Myers
- 42. Protecting Digital Rights: Technical Approaches**  
Robert Guess, Jennifer Hadley, Steven Lovaas, and Diane E. Levine

**PART IV PREVENTION: HUMAN FACTORS**

- 43. Ethical Decision Making and High Technology**  
James Landon Linderman
- 44. Security Policy Guidelines**  
M. E. Kabay and Bridgitt Robertson
- 45. Employment Practices and Policies**  
M. E. Kabay and Bridgitt Robertson
- 46. Vulnerability Assessment**  
Rebecca Gurley Bace
- 47. Operations Security and Production Controls**  
M. E. Kabay, Don Holden, and Myles Walsh
- 48. E-Mail and Internet Use Policies**  
M. E. Kabay and Nicholas Takacs
- 49. Implementing a Security Awareness Program**  
K. Rudolph
- 50. Using Social Psychology to Implement Security Policies**  
M. E. Kabay, Bridgitt Robertson, Mani Akella, and D. T. Lang
- 51. Security Standards for Products**  
Paul J. Brusil and Noel Zakin

**PART V DETECTING SECURITY BREACHES**

- 52. Application Controls**  
Myles Walsh
- 53. Monitoring and Control Systems**  
Caleb S. Coggins and Diane E. Levine
- 54. Security Audits, Standards, and Inspections**  
Donald Glass, Chris Davis, John Mason, David Gursky, James Thomas, Wendy Carr, and Diane Levine
- 55. Cyber Investigation**  
Peter Stephenson

**PART VI RESPONSE AND REMEDIATION**

- 56. Computer Security Incident Response Teams**  
Michael Miora, M. E. Kabay, and Bernie Cowens
- 57. Data Backups and Archives**  
M. E. Kabay and Don Holden
- 58. Business Continuity Planning**  
Michael Miora
- 59. Disaster Recovery**  
Michael Miora
- 60. Insurance Relief**  
Robert A. Parisi Jr., Chaim Haas, and Nancy Callahan
- 61. Working with Law Enforcement**  
David A. Land

**PART VII MANAGEMENT'S ROLE IN SECURITY**

- 62. Risk Assessment and Risk Management**  
Robert V. Jacobson
- 63. Management Responsibilities and Liabilities**  
Carl Hallberg, M. E. Kabay, Bridgitt Robertson, and Arthur E. Hutt
- 64. U.S. Legal and Regulatory Security Issues**  
Timothy Virtue
- 65. The Role of the CISO**  
Karen F. Worstell
- 66. Developing Security Policies**  
M. E. Kabay and Sean Kelley
- 67. Developing Classification Policies for Data**  
Karthik Raman and Kevin Beets
- 68. Outsourcing and Security**  
Kip Boyle, Michael Buglewicz, and Steven Lovaas

**PART VIII PUBLIC POLICY AND OTHER CONSIDERATIONS**

- 69. Privacy in Cyberspace: U.S. and European Perspectives**  
Marc Rotenberg



**x CONTENTS**

- 70. Anonymity and Identity in Cyberspace**  
M. E. Kabay, Eric Salveggio, and Robert Guess
- 71. Medical Records Protection**  
Paul J. Brusil
- 72. Legal and Policy Issues of Censorship and Content Filtering**  
Lee Tien, Seth Finkelstein, and Steven Lovaas
- 73. Expert Witnesses and the *Daubert* Challenge**  
Chey Cobb
- 74. Professional Certification and Training in Information Assurance**  
Christopher Christian, M. E. Kabay, Kevin Henry, and Sondra Schneider
- 75. Undergraduate and Graduate Education in Information Assurance**  
Vic Maconachy, John Orlando, and Seymour Bosworth
- 76. European Graduate Work in Information Assurance and the Bologna Declaration**  
Urs E. Gattiker
- 77. The Future of Information Assurance**  
Peter G. Neumann

**INDEX**

# PREFACE

Computers are an integral part of our economic, social, professional, governmental, and military infrastructures. They have become necessities in virtually every area of modern life, but their vulnerability is of increasing concern. Computer-based systems are constantly under threats of inadvertent error and acts of nature as well as those attributable to unethical, immoral, and criminal activities. It is the purpose of this *Computer Security Handbook* to provide guidance in recognizing these threats, eliminating them where possible and, if not, then to lessen any losses attributable to them.

This *Handbook* will be most valuable to those directly responsible for computer, network, or information security as well as those who must design, install, and maintain secure systems. It will be equally important to those managers whose operating functions can be affected by breaches in security and to those executives who are responsible for protecting the assets that have been entrusted to them.

With the advent of desktop, laptop, and handheld computers, and with the vast international networks that interconnect them, the nature and extent of threats to computer security have grown almost beyond measure. In order to encompass this unprecedented expansion, the *Computer Security Handbook* has grown apace.

When the first edition of the *Handbook* was published, its entire focus was on mainframe computers, the only type then in widespread use. The second edition recognized the advent of small computers, while the third edition placed increased emphasis on PCs and networks.

<b>Edition</b>	<b>Publication Date</b>	<b>Chapters</b>	<b>Text Pages</b>
First	1973	12	162
Second	1988	19	383
Third	1995	23	571
Fourth	2002	54	1,184
Fifth	2009	77	2,040

The fourth edition of the *Computer Security Handbook* gave almost equal attention to mainframes and microcomputers.

This fifth edition has been as great a step forward as the fourth. With 77 chapters and the work of 86 authors, we have increased coverage in both breadth and depth. We now cover all 10 domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>:

1. Security Management Practices: Chapters 10, 12, 13, 14, 15, 19, 31, 43, 44, 45, 46, 47, 48, 49, 50, 51, 54, 55, 62, 63, 64, 65, 66, 67, 68, 74, 75, 76

## xii PREFACE

2. Security Architecture and Models: Chapters 1, 2, 3, 8, 9, 24, 26, 27, 51
3. Access Control Systems and Methodology: Chapters 15, 19, 28, 29, 32
4. Application Development Security: Chapters 13, 19, 21, 30, 38, 39, 52, 53
5. Operations Security: Chapters 13, 14, 15, 19, 21, 24, 36, 40, 47, 53, 57
6. Physical Security: Chapters 4, 13, 15, 19, 22, 23, 28, 29
7. Cryptography: Chapters 7, 32, 37, 42
8. Telecomm, Networks, and Internet Security: Chapters 4, 5, 6, 13, 14, 15, 16, 17, 18, 20, 21, 24, 25, 26, 27, 30, 31, 32, 33, 34, 35, 41, 48
9. Business Continuity Planning: Chapters 22, 23, 56, 57, 58, 59, 60
10. Law, Investigations, and Ethics: Chapters 11, 12, 13, 31, 42, 61, 63, 64, 69, 70, 71, 72, 73

In addition to updating every chapter of the fourth edition, we have added chapters on:

- History of Computer Crime
- Hardware Elements of Security
- Data Communications and Information Security
- Network Topologies, Protocols, and Design
- Encryption
- Mathematical Models of Information Security
- The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns
- Social Engineering and Low-Tech Attacks
- Spam, Phishing, and Trojans: Attacks Meant to Fool
- Biometric Authentication
- Web Monitoring and Content Filtering
- Virtual Private Networks and Secure Remote Access
- 802.11 Wireless LAN Security
- Securing VoIP
- Securing P2P, IM, SMS, and Collaboration Tools
- Securing Stored Data
- Writing Secure Code
- Managing Software Patches and Vulnerabilities
- U.S. Legal and Regulatory Security Issues
- The Role of the CISO
- Developing Classification Policies for Data
- Outsourcing and Security
- Expert Witnesses and the *Daubert* Challenge
- Professional Certification and Training in Information Assurance
- Undergraduate and Graduate Education in Information Assurance
- European Graduate Work in Information Assurance and the Bologna Declaration

We have continued our practice from the fourth edition of inviting a security luminary to write the final chapter, “The Future of Information Assurance.” We are pleased to include a stellar contribution from Dr. Peter G. Neumann in this edition.

SEYMOUR BOSWORTH  
Senior Editor  
January 2009

# ACKNOWLEDGMENTS

**Seymour Bosworth**, Senior Editor I would like to give grateful recognition to Arthur Hutt and Douglas Hoyt, my coeditors of the first, second, and third editions of this *Handbook*. Although both Art and Doug are deceased, their commitment and their competence remain as constant reminders that nothing less than excellence is acceptable. Mich Kabay, my coeditor from the fourth edition, and Eric Whyne, our new third editor, continue in that tradition. I would not have wanted to undertake this project without them.

We mark with sadness the passing of our friend and colleague Robert Jacobson, who contributed to Chapter 1 (Brief History and Mission of Information System Security) and wrote Chapter 62 (Risk Assessment and Risk Management). Bob was a significant and valued contributor to the development of our field, and we miss his cheerful intelligence. We also miss Diane Levine, who contributed so much to both the third and fourth editions. She wrote four chapters in the third edition and six in the fourth. We are honored to continue to list her as a coauthor on five updated chapters in the fifth edition.

Thanks are also due to our colleagues at John Wiley & Sons: Tim Burgard as Acquisitions Editor, Stacey Rympha as Development Editor, Natasha Andrews-Noel as Senior Production Editor, and Debra Manette as Copyeditor and Joe Ruddick as Proofreader. All have performed their duties in an exemplary manner and with unfailing kindness, courtesy, and professionalism.

**M. E. Kabay**, Technical Editor The contributions from my faculty colleagues and from our alumni in the Master of Science in Information Assurance (MSIA) program at Norwich University are noteworthy. Many of the *Handbook's* authors are graduates of the MSIA program, instructors in the program, or both.

I am immeasurably grateful to Sy for his leadership in this project. In addition to the inherent value of his decades of experience in the field of information security, his insightful editorial comments and queries have forced everyone on the project to strive for excellence in all aspects of our work. He is also fun to work with!

Our coeditor Eric Whyne has loyally persevered in his editorial tasks despite ducking bullets in the war in Iraq, where he has served honorably throughout most of the project. Our thanks to him for his service to the nation and to this project.

Our authors deserve enormous credit for the professional way in which they responded to our requests, outlines, suggestions, corrections, and nagging. I want to express my personal gratitude and appreciation for their courteous, collaborative, and responsive interactions with us.

Finally, as always, I want to thank my beloved wife, Deborah Black, light of my life, for her support and understanding over the years that this project has taken away from our time together.

## **xiv ACKNOWLEDGMENTS**

**Eric Whyne**, Associate Editor There is an enormous amount of work put into a text of this size. The diligent and gifted authors who have contributed their time are some of the brightest and most experienced professionals in their fields. They did so not for compensation but because they love the subjects which they have put so much effort into mastering. The *Computer Security Handbook* will continue its tradition of being a collection point for these labors so long as there are great minds in love with the challenging problems of computer security and willing to devote their time to sharing solutions.

At the time I started on the project, I was a Marine Officer working in the data communications field in Ramadi, Iraq. I worked the night shift and spent my afternoons perched in a folding chair, under the relatively cool Iraq winter sun, writing correspondence and doing first-past edits of the chapters of the *Handbook*. Upon my return to the United States, my spare evenings along the North Carolina coast were dedicated to the *Handbook* as I worked my day job as the Marine Corps Anti-Terrorism Battalion Communications Officer. Since then I have deployed once more to Iraq as an advisor to the Iraqi Army. Everywhere I have gone, and with every job I have held, I have been able to apply and refine the principles covered in this *Handbook* and in previous versions. From the most high-tech cutting-edge, multiplexed satellite communications system used in military operations in Iraq, to the relatively mundane desktop computer networks of offices in the United States, to the ancient weathered computers the Iraqi Army totes around with them and ties into the power grid at any opportunity, computer security is critical to the accomplishment of the most basic tasks these systems are used for.

Unarguably, the exchange of information and ideas has been the largest factor in the shaping and betterment of our world throughout history. Having spent the last year of my life living as a local in a third-world country, that fact is fresh on my mind. In that spirit, computers are recognized as the most powerful and universally applicable tool ever devised. This book's purpose is to help you ensure that your computers remain powerful and successfully applied to the tasks for which you intend them to be used.

I am grateful to Sy Bosworth and Mich Kabay for their faith in bringing me into this project, and for their guidance and leadership along the way. They are both great people, and it has been an honor and a joy to work with them.

## ABOUT THE EDITORS

**Seymour Bosworth, MS, CDP** (e-mail: [sybosworth55@gmail.com](mailto:sybosworth55@gmail.com)) is president of S. Bosworth & Associates, Plainview, New York, a management consulting firm specializing in computing applications for banking, commerce, and industry. Since 1972, he has been a contributing editor of all five editions of the *Computer Security Handbook*, and he has written many articles and lectured extensively about computer security and other technical and managerial subjects. He has been responsible for design and manufacture, systems analysis, programming, and operations, of both digital and analog computers. For his technical contributions, including an error-computing calibrator, a programming aid, and an analog-to-digital converter, he has been granted a number of patents, and is working on several others.

Bosworth is a former president and CEO of Computer Corporation of America, manufacturers of computers for scientific and engineering applications; president of Abbey Electronics Corporation, manufacturers of precision electronic instruments and digital devices; and president of Alpha Data Processing Corporation, a general-purpose computer service bureau. As a vice president at Bankers Trust company, he had overall responsibility for computer operations, including security concerns.

For more than 20 years, Bosworth was an Adjunct Associate Professor of Management at the Information Technologies Institute of New York University, where he lectured on computer security and related disciplines. He has conducted many seminars and training sessions for the Battelle Institute, New York University, the Negotiation Institute, the American Management Association, and other prestigious organizations. For many years he served as Arbitrator, Chief Arbitrator, and Panelist for the American Arbitration Association. He holds a Master's degree from the Graduate School of Business of Columbia University and the Certificate in Data Processing of the Data Processing Management Association.

**M. E. Kabay, PhD, CISSP-ISSMP** (e-mail: [mekabay@gmail.com](mailto:mekabay@gmail.com)) has been programming since 1966. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. After joining a compiler and relational database team in 1979, he worked for Hewlett Packard (Canada) Ltd. from 1980 through 1983 as an HP3000 operating system performance specialist and then ran operations at a large service bureau in Montréal in the mid-1980s before founding his own operations management consultancy. From 1986 to 1996, he was an adjunct instructor in the John Abbott College professional programs in Programming and in Technical Support. He was Director of Education for the National Computer Security Association from 1991 to the end of 1999 and was Security Leader for the INFOSEC Group of AtomicTangerine, Inc., from January 2000 to June 2001. In July 2001, he joined the faculty at Norwich University as Associate Professor of Computer Information Systems in the

## **xvi ABOUT THE EDITORS**

School of Business and Management. In January 2002, he took on additional duties as the director of the graduate program in information assurance in the School of Graduate Studies at Norwich, where he is also Chief Technical Officer.

Kabay was inducted into the Information Systems Security Association Hall of Fame in 2004. He has published over 950 articles in operations management and security in several trade journals. He currently writes two columns a week for *Network World Security Strategies*; archives are at [www.networkworld.com/newsletters/secl](http://www.networkworld.com/newsletters/secl). He has a Web site with freely available teaching materials and papers at [www2.norwich.edu/mkabay/index.htm](http://www2.norwich.edu/mkabay/index.htm).

**Eric Whyne** (e-mail: [ericwhyne@gmail.com](mailto:ericwhyne@gmail.com)) is a Captain in the United States Marine Corps. He joined the Marine Corps in the Signals Intelligence field and received two meritorious promotions before being selected for an officer candidate program and finally commissioning into the communications occupational specialty. His billets have included commanding a data communications platoon, managing large-scale communications networks, advising the Iraqi Army, and serving as the senior communications officer for the Marine Corps Anti-Terrorism unit. Whyne holds a BS in Computer Science from Norwich University as well as minor degrees in Mathematics, Information Assurance, and Engineering. He has presented about communications security and other technology topics at many forums and worked as a researcher for the National Center for Counter-Terrorism and Cyber Crime Research. After nine honorable years of service and two tours to Iraq totaling 18 months, Whyne is transitioning out of the military and pursuing a career in the civilian industry in order to more effectively and freely apply his skills and abilities to cutting-edge technological trends and problems.

## ABOUT THE CONTRIBUTORS

**Mani Akella**, Director (Technology), has been actively working with information security architectures and identity protection for Consultantgurus and its clients. An industry professional for 20 years, Akella has worked with hardware, software, networking, and all the associated technologies that service information in all of its incarnations and aspects. Over the years, he has developed a particular affinity for international data law and understanding people and why they do what they do (or do not). He firmly believes that the best law and policy is that which understands and accounts for cross-cultural differences, and works with an understanding of culture and societal influences. To that end, he has been actively working with all his clients and business acquaintances to improve security policies and make them more people-friendly: His experience has been that the best policy is that which works with, instead of being antagonistic to, the end user.

**Rebecca Gurley Bace** is the President/CEO of Infidel, Inc., a strategic consulting practice headquartered in Scotts Valley, California. She is also a venture consultant for Palo Alto-based Trident Capital, where she is credited with building Trident's investment portfolio of security product and service firms. Her areas of expertise include intrusion detection and prevention, vulnerability analysis and mitigation, and the technical transfer of information security research results to the commercial product realm. Prior to transitioning to the commercial world, Bace worked in the public sector, first at the National Security Agency, where she led the Intrusion Detection research program, then at the Computing Division of the Los Alamos National Laboratory, where she served as Deputy Security Officer. Bace's publishing credits include two books, an NIST Special Publication on intrusion detection and prevention, and numerous articles on information security technology topics.

**Susan Baumes, MS, CISSP**, is an information security professional working in the financial services industry. In her current role, Ms. Baumes works across the enterprise to develop information security awareness and is responsible for application security. Her role also extends to policy development, compliance and audit. She has 11 years experience in application development, systems and network administration, database management, and information security. Previously, Ms. Baumes worked in a number of different sectors including government (federal and state), academia and retail.

**Kurt Baumgarten, CISA** (e-mail: [kurtb@peritussecurity.com](mailto:kurtb@peritussecurity.com)) is Vice President of Information Security and a partner at Peritus Security Partners, LLC, a leader in providing compliance-driven information security solutions. He is also a lecturer, consultant, and the developer of the DDIPS intrusion prevention technology as well as a pioneer in



## **xviii ABOUT THE CONTRIBUTORS**

using best practices frameworks for the improvement of information technology security programs and management systems. Baumgarten has authored multiple articles about the business benefits of sound information technology and information assurance practices, and assists businesses and government agencies in defining strategic plans that enhance IT and IA as positive value chain modifiers. He holds both a Master's of Science in Information Assurance and an MBA with a concentration in E-Commerce, and serves as an Adjunct Professor of Information Assurance. He has more than 20 years of experience in IT infrastructure and Information Security and is an active member of ISSA, ISACA, ISSSP, and the MIT Enterprise Forum. Baumgarten periodically acts as an interim Director within external organizations in order to facilitate strategic operational changes in IT and Information Security.

**Kevin Beets** has been a Research Scientist with McAfee for the past five years. His work has concentrated on vulnerability and malware research and documentation with the Foundstone R&D and Avert Labs teams. Prior to working at McAfee, he architected private LANs as well as built, monitored, and supported CheckPoint and PIX firewalls and RealSecure IDS systems.

**Matt Bishop** is a Professor in the Department of Computer Science at the University of California at Davis and a Codirector of the Computer Security Laboratory. His main research area is the analysis of vulnerabilities in computer systems, especially their origin, detection, and remediation. He also studies network security, policy modeling, and electronic voting. His textbook, *Computer Security: Art and Science*, is widely used in advanced undergraduate and graduate courses. He received his PhD in computer science from Purdue University, where he specialized in computer security, in 1984.

**Kip Boyle** is the Chief Information Security Officer of PEMCO Insurance, a \$350 million property, casualty, and life insurance company serving the Pacific Northwest. Prior to joining PEMCO Insurance, he held such positions as Chief Security Officer for a \$50 million national credit card transaction processor and technology service provider; Authentication and Encryption Product Manager for Cable & Wireless America; Senior Security Architect for Digital Island, Inc.; and a Senior Consultant in the Information Security Group at Stanford Research Institute (SRI) Consulting. He has also held director-level positions in information systems and network security for the U.S. Air Force. Boyle is a Certified Information System Security Professional and Certified Information Security Manager. He holds a Bachelor's of Science in Computer Information Systems from the University of Tampa (where he was an Air Force ROTC Distinguished Graduate) and a Master's of Science in Management from Troy State University.

**Timothy Braithwaite** has more than 30 years of hands-on experience in all aspects of automated information processing and communications. He is currently Deputy Director of Strategic Programs at the Center for Information Assurance of Titan Corporation. Before joining Titan, he managed most aspects of information technology, including data and communications centers, software development projects, strategic planning and budget organizations, system security programs, and quality improvement initiatives. His pioneering work in computer systems and communications security while with the Department of Defense resulted in his selection to be the first Systems Security Officer for the Social Security Administration (SSA) in 1980. After developing security policy and establishing a nationwide network of regional security officers,

Braithwaite directed the risk assessment of all payment systems for the agency. In 1982, he assumed the duties of Deputy Director, Systems Planning and Control of the SSA, where he performed substantive reviews of all major acquisitions for the Associate Commissioner for Systems and, through a facilitation process, personally led the development of the first Strategic Systems Plan for the administration. In 1984, he became Director of Information and Communication Services for the Bureau of Alcohol, Tobacco, and Firearms at the Department of Treasury. In the private sector, he worked in senior technical and business development positions for SAGE Federal Systems, a software development company; Validity Corporation, a testing and independent validation and verification company; and J.G. Van Dyke & Associates, where he was Director, Y2K Testing Services. He was recruited to join Titan Corporation in December 1999 to assist in establishing and growing the company's Information Assurance practice.

**Paul J. Brusil, PhD** (e-mail: [brusil@post.harvard.edu](mailto:brusil@post.harvard.edu)) founded Strategic Management Directions, a security and enterprise management consultancy in Beverly, Massachusetts. He has been working with various industry and government sectors including healthcare, telecommunications, and middleware to improve the specification, implementation, and use of trustworthy, quality, security-related products and systems. He supported strategic planning that led to the National Information Assurance Partnership and other industry forums created to understand, promote, and use the Common Criteria to develop security and assurance requirements and to evaluate products. Brusil has organized, convened, and chaired several national workshops, conferences, and international symposia pertinent to management and security. Through these and other efforts to stimulate awareness and cooperation among competing market forces, he spearheaded industry's development of the initial open, secure, convergent, standards-based network and enterprise management solutions. While at the MITRE Corp, Brusil led research and development critical to the commercialization of the world's first LAN solutions. Earlier, at Harvard, he pioneered research leading to noninvasive diagnosis of cardiopulmonary dysfunction. He is a Senior Member of the IEEE, a member of the Editorial Advisory Board of the *Journal of Network and Systems Management (JNSM)*, has been Senior Technical Editor for *JNSM*, is the Guest Editor for all *JNSM*'s Special Issues on Security and Management, and is a Lead Instructor for the Adjunct Faculty supporting the Master's of Science in Information Assurance degree program at Norwich University. He has authored over 100 papers and book chapters. He graduated from Harvard University with a joint degree in Engineering and Medicine.

**David Brussin** is Founder and CEO of Monetate, Inc. Monetate powers Intelligent Personal Promotions™ for online retailers. Brussin is a serial entrepreneur recognized as a leading information security and technology expert, and was honored by MIT's *Technology Review* as one of the world's 100 top young innovators. In January 2004, Brussin cofounded TurnTide, Inc. around the antispam router technology he had invented. As Chief Technology Officer, he also managed engineering and technical operations. TurnTide was acquired by Symantec six months later. Previously, Brussin cofounded and served as Chief Technology Officer for ePrivacy Group, Inc., which created the Trusted Sender program and Trusted Email Open Standard to protect and grow the e-mail marketing channel. Brussin created products to help e-mail marketers increase response and conversion by protecting their trusted relationship with consumers. In 1996, he cofounded and served as Vice President of Technology for InfoSec Labs,

## **xx ABOUT THE CONTRIBUTORS**

an information security company dedicated to helping Fortune 1000 companies safely transition their businesses into the online world. Partnering with his clients, Brussin balanced security with the emerging technical challenges of doing business online and helped many established bricks-and-mortar businesses become multichannel. InfoSec Labs was acquired by Rainbow Technologies, now part of SafeNet, in 1999. Brussin is a frequent speaker and writer on entrepreneurship and technology. He also serves on the Board of Directors of Invite Media, Inc., a stealth-mode start-up working to analyze and optimize online display advertising.

**Michael Buglewicz** spent approximately 10 years in law enforcement carrying out a variety of duties, from front-line patrol work through complex investigations. After concluding his law enforcement career, Buglewicz brought his experiences to technology and held a variety of roles within First Data Corporation, including Internet banking and online payment systems. Buglewicz has worked for Microsoft Corporation since 1996 in a variety of roles and has taught in Norwich University's Information Assurance program. Buglewicz holds an undergraduate degree in Fine Arts from the University of Nebraska at Omaha and graduate degrees from Illinois State University as well as a Master's degree in Information Assurance from Norwich University. His current interests focus on corporate risk management.

**Nancy Callahan** is Vice President, AIG Executive Liability, Financial Institutions Division. AIG is the world's leading international insurance and financial services organization, with operations in approximately 130 countries and jurisdictions. AIG member companies serve commercial, institutional, and individual customers through the most extensive worldwide property-casualty and life insurance networks of any insurer. An expert on privacy and identity theft, Callahan is a frequent speaker at industry conferences throughout the United States and is a much-sought-after media resource, having been quoted in the *Wall Street Journal* and Associated Press. Callahan joined AIG in 2001. Prior to AIG, Callahan worked in e-commerce and financial services. She spent 13 years at Reuters, where her final position was Executive Vice President, Money Transaction Systems. Callahan is a Chartered Property and Casualty Underwriter and Certified Information Privacy Professional. She has a Master's of Business Administration and a BS in Systems Engineering from the University of Virginia.

**Q. Campbell** (e-mail: [qcampbell@hushmail.com](mailto:qcampbell@hushmail.com)) has worked in the information security field for over six years. He specializes in information technology threat analysis and education.

**Wendy Carr, CISSP** (e-mail: [wendylcarr@gmail.com](mailto:wendylcarr@gmail.com)) is a Senior Consultant with Booz, Allen & Hamilton on a client-site in New England. Her focus on addressing security concerns related to the implementation of products and applications includes concentrations in the areas of Certification and Accreditation (Commercial/DITSCAP/DIACAP), risk analysis, compliance testing and vulnerability assessment, forensic examination, incident response, disaster recovery, authentication, and encryption for both physical and wireless environments in the fields of Military, Government and Banking. She holds an MS in Information Assurance from Norwich University and is a member of (ISC)<sup>2</sup>, InfraGard, and the Norwich University *Journal of Information Assurance* Editorial Review Board as well as several organizations dedicated to the advancement of information security.

**Santosh Chokhani** (e-mail: *schokhani@cygnacom.com*) is the Founder and President of CygnaCom Solutions, Inc., an Entrust company specializing in PKI. He has made numerous contributions to PKI technology and related standards, including trust models, security, and policy and revocation processing. He is the inventor of the PKI Certificate Policy and Certification Practices Statement Framework. His pioneering work in this area led to the Internet RFC that is used as the standard for CP and CPS by governments and industry throughout the world. Before starting CygnaCom, he worked for The MITRE Corporation from 1978 to 1994. At MITRE, he was senior technical manager and managed a variety of technology research, development, and engineering projects in the areas of PKI, computer security, expert systems, image processing, and computer graphics. Chokhani obtained his Master's (1971) and PhD (1975) in Electrical Engineering/Computer Science from Rutgers University, where he was a Louis Bevier Fellow from 1971 to 1973.

**Christopher Christian** is an aviator in the United States Army. He received a Bachelor's degree in Computer Information Systems at Norwich University class of 2005. His primary focus of study was Information Assurance and Security. He worked as an intern for an engineering consulting company for three years. He developed cost/analysis worksheets and floor-plan layouts to maximize workspace efficiency for companies in various industries. Christian graduated flight school at Fort Rucker, Alabama, there he trained on the H-60 Blackhawk. He serves as a Flight Platoon Leader in an Air Assault Battalion. First Lieutenant Christian is currently serving in Iraq in support of Operation Iraqi Freedom 08–09.

**Chey Cobb, CISSP** (e-mail: *cheycobb@gmail.com*) began her career in information security while at the National Computer Security Association (now known as TruSecure/ICSA Labs). During her tenure as the NCSA award-winning Webmaster, she realized that Web servers often created security holes in networks and became an outspoken advocate of systems security. Later, while developing secure networks for the Air Force in Florida, her work captured the attention of the U.S. intelligence agencies. Cobb moved to Virginia and began working for the government as the Senior Technical Security Advisor on highly classified projects. Ultimately, she went on to manage the security program at an overseas site. Cobb, who is now semiretired, writes books and articles on computer security and is a frequent speaker at security conferences.

**Stephen Cobb, CISSP** (e-mail: *sc@cobbassociates.com*) is an independent information security consultant and an Adjunct Professor of Information Assurance at Norwich University, Vermont. A graduate of the University of Leeds, Cobb's areas of expertise include risk assessment, computer fraud, data privacy, business continuity management, and security awareness and education. A frequent speaker and seminar leader at industry conferences around the world, Cobb is the author of numerous books on security and privacy as well as hundreds of articles. Cobb cofounded several security companies whose products expanded the range of security solutions available to enterprises and government agencies. As a consultant, he has advised some of the world's largest companies on how to maximize the benefits of information technology by minimizing IT risks.

**Caleb S. Coggins, MSIA, CISSP**, is a Corporate Auditor for Bridgestone Americas. His areas of interest include vulnerability management, network security, and information assurance. Prior to Bridgestone, Coggins served as the Information Manager

## **xxii ABOUT THE CONTRIBUTORS**

for a private company as well as an information security consultant to business clients. He holds a BA from Willamette University and an MS in Information Assurance from Norwich University.

**Bernie Cowens, CISSP, CISA** (e-mail: *bcowens@usa.com*) is Chief Information Security Officer at a Fortune 500 company in the financial services industry. He is an information risk, privacy, and security expert with more than 20 years experience in industries including defense, high technology, healthcare, financial, and Big Four professional services. Cowens has created, trained, and led a number of computer emergency, forensic investigation, and incident response teams over the years. He has real-world experience responding to attacks, disasters, and failures resulting from a variety of sources, including malicious attackers, criminals, and foreign governments. He has served as an advisor to and a member of national-level panels charged with analyzing cyber-system threats to critical infrastructures, assessing associated risks, and recommending both technical and nontechnical mitigation policies and procedures. Cowens holds a Master's degree in Management Information Systems along with undergraduate degrees and certificates in systems management and information processing.

**Christopher Dantos** is a Senior Architectural Specialist with Computer Science Corporation's Global Security Solutions Group. His areas of expertise include 802.11, VoIP, and Web application security. Prior to joining CSC, he spent 10 years as a Security Architect with Motorola Inc., including 5 years in the Motorola Labs Wireless Access Research Center of Excellence. He holds a Master's of Science degree in Information Assurance from Norwich University and a Bachelor's of Science degree in Marine Engineering from the Maine Maritime Academy.

**Chris Davis, CISA, CISSP**, has trained and presented in information security, advanced computer forensic analysis, hardware security design, auditing, and certification curriculum for government, corporate, and university requirements. He was part of the teams responsible for Hacking Exposed Computer Forensics, IT Auditing: Using Controls to Protect Information Assets, and the Anti-Hacker Toolkit. His contributions include projects and presentations for SANS, Gartner, Harvard, BlackHat, CEIC, and 3GSM. He has enjoyed positions at ForeScout, Texas Instruments, Microsoft Technology Center, and Cisco Systems. He holds a Bachelor's degree in Nuclear Engineering Technologies from Thomas Edison, and a Master's in Business from the University of Texas at Austin.

**Seth Finkelstein** (e-mail: *sethf@sethf.com*) is a professional programmer with degrees in Mathematics and in Physics from MIT. He cofounded the Censorware Project, an anti-censorware advocacy group. In 1998, his efforts evaluating the sites blocked by the library's Internet policy in Loudoun County, Virginia, helped the American Civil Liberties Union win a federal lawsuit challenging the policy. In 2001, he received a Pioneer of the Electronic Frontier Award from the Electronic Frontier Foundation for his groundbreaking work in analyzing content-blocking software. In 2003, he was primarily responsible for winning a temporary exemption in the Digital Millennium Copyright Act allowing for the analysis of censorware.

**Urs E. Gattiker** is an internationally-renowned security and risk technologist, both a Founder and the Chief Technology Officer of CyTRAP Labs GmbH. CyTRAP Labs

provides corporate governance and social media services to organizations worldwide. Using sophisticated analysis and correlation tools, CyTRAP Labs' expert Internet Analysts monitor suspicious internal and external activities, user and community behavior, business goals, and web technology to craft and deliver long term successful web and corporate risk management programs for companies.

Urs is the inventor of the ComMetrics benchmark battery of tools. One of these, the FT/ComMetrics corporate blog index, empowers the FT Global 500 companies to compare the value of their blogging activities against to that target information security prevention and safety, with other enterprises. He is the author and co-author of several books on computer viruses, technology and risk management. Gattiker holds a PhD in business focusing on computing/informatics and an MBA (international marketing) both from Claremont Graduate University (Claremont Colleges) and a BS in public administration/informatics from the HWV Zurich.

**Robert Gezelter, CDP**, has over 33 years of experience in computing, starting with programming scientific/technical problems. Shortly thereafter, his focus shifted to operating systems, networks, security, and related matters, where he has 32 years of experience in systems architecture, programming, and management. He has worked extensively in systems architecture, security, internals, and networks, ranging from high-level strategic issues to the low-level specification, design, and implementation of device protocols and embedded firmware.

Gezelter is an alumnus of the IEEE Computer Society's Distinguished Visitor Program for North America, having been appointed to a three-year term in 2004. His appointment included numerous presentations at Computer Society chapters throughout North America.

He has published numerous articles, appearing in *Hardcopy*, *Computer Purchasing Update*, *Network Computing*, *Open Systems Today*, *Digital Systems Journal*, and *Network World*. He is a frequent presenter at conference sessions on operating systems, languages, security, networks, and related topics at local, regional, national, and international conferences, speaking for DECUS, Encompass, IEEE, ISSA, ISACA, and others. He previously authored the mobile code and Internet-related chapters for the 4th edition of this *Handbook* (2002) as well as the "Internet Security" chapters of the 3rd edition (1995) and its supplement (1997).

He is a graduate of New York University with BA (1981) and MS (1983) degrees in Computer Science. Gezelter founded his consulting practice in 1978, working with clients both locally and internationally. He maintains his offices in Flushing, New York. He may be contacted via his firm's www site at [www.rlgsc.com](http://www.rlgsc.com).

**Anup K. Ghosh** is President and Chief Executive of Secure Command, LLC, a security software start-up developing next-generation Internet security products for corporate networks. Ghosh also holds a position as Research Professor at George Mason University. Ghosh was previously Senior Scientist and Program Manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency (DARPA), where he managed an extensive portfolio of information assurance and information operations programs. Ghosh previously served in executive management as Vice President of Research at Cigital, Inc. He has served as principal investigator on contracts from DARPA, NSA, and NIST's Advanced Technology Program and has written more than 40 peer-reviewed conference and journal articles. Ghosh is also author of three books on computer network defense and serves on the editorial board of *IEEE Security and Privacy Magazine* and has been guest editor for *IEEE Software* and *IEEE Journal*

## **xxiv ABOUT THE CONTRIBUTORS**

*on Selected Areas in Communications.* Ghosh is a Senior Member of the IEEE. For his contributions to the Department of Defense's information assurance, Ghosh was awarded the Frank B. Rowlett Trophy for Individual Contributions by the National Security Agency in November 2005, a federal government-wide award. He was also awarded the Office of the Secretary of Defense Medal for Exceptional Public Service for his contributions while at DARPA. In 2005, Worcester Polytechnic Institute awarded Ghosh its Hobart Newell Award for Outstanding Contributions to the Electrical and Computer Engineering Profession. Ghosh has previously been awarded the IEEE's Millennium Medal for Outstanding Contributions to E-Commerce Security. Ghosh completed his PhD and Master of Science in Electrical Engineering at the University of Virginia and his Bachelor of Science in Electrical Engineering at Worcester Polytechnic Institute.

**Donald Glass, CISA, CISSP** (e-mail: [donald@donaldglass.com](mailto:donald@donaldglass.com)) has over 15 years of experience in the IT Auditing and Information Security fields. He's the current Director of IT Audit for Kerzner International. Author of several information security and IT audit articles, Donald is recognized as a leader in the IT audit field and information security.

**Robert Guess** is a Senior Security Engineer at a Fortune 500 firm and an Associate Professor of Information Systems Technology. Guess possesses a Master's of Science in Information Assurance from Norwich University and has over a dozen industry certifications, including the National Security Agency INFOSEC Assessment Methodology, National Security Agency INFOSEC Evaluation Methodology, and Certified Information Systems Security Practitioner. His professional efforts include work in the defense sector, serving as primary subject matter expert on a National Science Foundation Cybersecurity Education Grant, and the development of Department of Defense workforce certification standards for information assurance professionals. Guess's work in recent years has focused on security assessment, penetration testing, incident response, and the forensic analysis of digital evidence.

**David Gursky** is an Information Assurance manager and researcher at Raytheon Integrated Defense Systems working in Crystal City, Virginia. He is principal investigator for behavior-based intrusion detection systems, attribute-based access control, and resource-efficient authentication techniques. He held several senior positions as a Department of Defense Contractor supporting Information Assurance programs and has over 30 years' experience in information technology and information security. He has conducted numerous security audits for PriceWaterhouse and Coopers. Gursky has Bachelor's of Science degree in Business Management from Southern New Hampshire University, a Master's of Science degree from Norwich University, and an MBA from Northeastern University. In addition, he holds a CISA, CISM and CISSP certifications. He lives in Northern Virginia and is an active member of (ISC)<sup>2</sup> and ISACA.

**Jennifer Hadley** (e-mail: [hadley.jennifer@gmail.com](mailto:hadley.jennifer@gmail.com)) is a member of the first Master of Science in Information Assurance graduating class at Norwich University. She is the primary Systems and Security Consultant for Indiana Networking in Lafayette, Indiana, and has served as both a network and systems administrator in higher education and private consulting. She has almost 10 years' experience as a programmer and instructor of Web technologies with additional interests in data backup, virtualization,

authentication/identification, monitoring, desktop and server deployment, and incident response. At present Hadley serves as a Technology Consultant for Axcell Technologies, Inc. Previously she worked as a tester for quality and performance projects for Google, Inc., and as a collegiate adjunct instructor in computer technologies. Hadley received a Bachelor's of Science degree in Industrial and Computer Technology from Purdue University.

**Carl Hallberg, CISSP**, has been a Unix Systems Administrator for years as well as an Information Security Consultant. He has also written training courses for subjects including firewalls, VPNs, and home network security. He has a Bachelor's degree in Psychology. Currently he is a senior member of an incident response team for a major U.S. financial institution.

**Kevin Henry** has been involved in computers since 1976, when he was an operator on the largest minicomputer system in Canada. He has since worked in many areas of information technology, including computer programming, systems analysis, and information technology audit. Henry was asked to become Director of Security based on the evidence of his audits and involvement in promoting secure IT operations. Following 20 years in the telecommunications field, Henry moved to a Senior Auditor position with the State of Oregon, where he was a member of the Governor's IT Security Subcommittee and performed audits on courts and court-related IT systems.

Henry has extensive experience in Risk Management and Business Continuity and Disaster Recovery Planning. He frequently presents papers at industry events and conferences and is on the preferred speakers list for nearly every major security conference. Since joining (ISC)<sup>2</sup> as their first full-time Program Manager in 2002, Henry has been responsible for research and development of new certifications, courseware, and development of educational programs and instructors. He has also been providing support services and consulting for organizations that require in-depth risk analysis and assistance with specific security-related challenges. This has led to numerous consulting engagements in the Middle East and Asia for large telecommunications firms, government departments, and commercial enterprises.

**Don Holden** is a Principal Consultant with Concordant specializing in information security. He has more than 20 years of management experience in information systems, security, encryption, business continuity, and disaster recovery planning in both industry and government. Previously he was a Technology Leader for RedSiren Technologies (formerly SRI Consulting). Holden's achievements include leading a cyber-insurance joint venture project, developing privacy and encryption policies for major financial institutions, and recommending standards-based information technology security policies for a federal financial regulator. Holden is an Adjunct Professor for the Norwich University's Master's of Science in Information Assurance. He received an MBA from Wharton and is a Certified Information System Security Professional and Information System Security Management Professional.

**John D. Howard** is a former Air Force engineer and test pilot who currently works in the Security and Networking Research Group at the Sandia National Laboratories, Livermore, California. His projects include development of the SecureLink software for automatic encryption of network connections. He has extensive experience in systems development, including an aircraft-ground collision avoidance system for which he



## **xxvi ABOUT THE CONTRIBUTORS**

holds a patent. He is a graduate of the Air Force Academy, has Master's degrees in both Aeronautical Engineering and Political Science, and has a PhD in Engineering and Public Policy from Carnegie Mellon University.

**Arthur E. Hutt, CCEP.** The late Arthur E. Hutt was an information systems consultant with extensive experience in banking, industry, and government. He served as a contributing editor to the 1st, 2nd, and 3rd Editions of the Computer Security Handbook. He was a principal of PAGE Assured Systems, Inc., a consulting group specializing in security and control of information systems and contingency/disaster recovery planning. He was a senior information systems executive for several major banks active in domestic and international banking. His innovative and pioneering development of online banking systems received international recognition. He was also noted for his contributions to computer security and to information systems planning for municipal government. He was on the faculty of the City University of New York and served as a consultant to CUNY on curriculum and on data processing management. He also served on the mayor's technical advisory panel for the City of New York. Hutt was active in development of national and international technical standards, via ANSI and ISO, for the banking industry.

**Robert V. Jacobson, CPP, CISSP,** deceased was the President of International Security Technology, Inc., a New York City-based risk management consulting firm. Jacobson founded IST in 1978 to develop and apply superior risk management systems. Current and past government and industry clients are located in the United States, Europe, Africa, Asia, and the Middle East. Jacobson pioneered many of the basic computer security concepts now in general use. He served as the first Information System Security Officer at Chemical Bank, now known as J P Morgan Chase. He was a frequent lecturer and had written numerous technical articles. Mr. Jacobson held BS and MS degrees from Yale University, and was a Certified Information Systems Security Professional. He was also a Certified Protection Professional of the American Society for Industrial Security. He was a member of the National Fire Protection Association and the Information Systems Security Association. In 1991, he received the Fitzgerald Memorial Award for Excellence in Security from the New York Chapter of the ISSA.

**David J. Johnson** is an information security analyst for a Fortune 1000 financial services company where he focuses primarily on information security policy and standard creation and maintenance. Additionally, he also performs analysis of information technology projects, as well as IT and business processes, for security and business continuity impact and system vulnerability management. Johnson's prior work includes nine years designing, building, and maintaining an electronic commerce (EC/EDI) infrastructure and data transfers for a national financial service company. He holds a Bachelor's of Science in Business Administration from Oregon State University and a Master's of Science in Information Assurance from Norwich University.

**Sean Kelley** is an Adjunct Professor in Information Assurance (IA) for Norwich and Troy University. He also teaches IA and management conferences for the SANS Institute. His information security career is diversified and has taken him to high-level organizations in Washington, DC, including the Attending Physician's Office to Congress, U.S. Capitol, where he was responsible for the development of policy and controls for the secure handling of electronic health records for 535 members of Congress, Supreme Court Justices, and officials. Kelley is a Certified Information

Systems Security Professional and PMP and also holds several NSA certificates. Kelley also holds a Master's degree from Webster University in Computer Resources and Information Management and a second Master's degree from the Naval Postgraduate School in Information Technology, where he concentrated on computer and network security by taking classes through the NPS Center for INFOSEC Studies and Research.

**David M. Kennedy, CISSP** (e-mail: [david.kennedy@acm.org](mailto:david.kennedy@acm.org)) is TruSecure Corporation's Chief of Research. He directs the Research Group to provide expert services to TruSecure Corporation members, clients, and staff. He supervises the Information Security Reconnaissance (IS/R) team, which collects security-relevant information, both above- and underground in TruSecure Corporation's IS/R data collection. IS/R provides biweekly and special topic reports to IS/R subscribers. Kennedy is a retired U.S. Army Military Police officer. In his last tour of duty, he was responsible for enterprise security of five LANs with Internet access and over 3,000 personal computers and workstations. He holds a BS in Forensic Science.

**Gary C. Kessler** is an Associate Professor of Computer and Digital Forensics and Coordination of Information Assurance Education at Champlain College in Burlington, Vermont, where he is also the Director of the Champlain College Center for Digital Investigation. Kessler is a technical consultant to the Vermont Internet Crimes Task Force and a member of the High Technology Crime Investigation Association and High Tech Crime Consortium; he is also a Certified Information Systems Security Professional and Certified Computer Examiner. Kessler is a frequent speaker at industry conferences, has written two books and over 70 articles on a variety of technology topics, and is an Associate Editor of the *Journal of Digital Forensic Practice* and serves on the editorial board of the *Journal of Digital Forensics, Security, and Law*. He holds a BA in Mathematics, an MS in Computer Science, an EdS in Computing Technology in Education, and is pursuing a doctorate degree.

**David A. Land.** In the U.S. Army as a Counterintelligence Special Agent, Land and David Christie developed and hosted the first Department of Defense Computer Crimes Conference. Since then Land has investigated espionage cases for both the Army and the Department of Energy. He serves as the Information Technology Coordinator for Anniston City Schools in Alabama and as an Adjunct Professor for Norwich University, his alma mater.

**D. T. Lang** served in the United States Air Force, retiring as a Special Agent in Charge. As a Special Agent he worked in the areas of antiterrorism, executive and force protection, counterintelligence and counterespionage. Lang is a combat veteran of Operation Desert Storm and was charged with the Joint Force Protection Team for the United Nations Implementation Forces in Zagreb, Croatia. In the 1990s, he held diplomatic status as a U.S. Arms Control Treaty Inspector. In 2003, he was selected by the United Nations to be a UN weapons of mass destruction inspector in Iraq. Lang currently provides consulting support to the U.S. Intelligence Community and served as a senior instructor in the Master's of Science in Information Assurance Program at Norwich University from 2005 to 2008. Lang is a past commander of Civil Air Patrol's Wyoming Wing and a recipient of the Civil Air Patrol Distinguished Service Medal.

**David R. Lease, PhD** is the Chief Solution Architect at Computer Sciences Corporation. He has over 30 years of technical and management experience in the information

## xxviii ABOUT THE CONTRIBUTORS

technology, security, telecommunications, and consulting industries. Lease's recent projects include a \$2 billion security architecture redesign for a federal law enforcement agency and the design and implementation of a secure financial management system for an organization operating in 85 countries. Lease is a writer and frequent speaker at conferences for organizations in the intelligence community, Department of Defense, civilian federal agencies, as well as commercial and academic organizations. He is also a peer reviewer of technical research for the IEEE Computer Society. Additionally, Lease is on the faculty of Norwich University and the University of Fairfax, where he teaches graduate-level information assurance courses and supervises doctoral-level research.

**Corinne Lefrançois** is an Information Assurance Analyst at the National Security Agency. She graduated from Norwich University with a Bachelor of Science in Business Administration and Accounting in 2004 and is a current student in Norwich University's Master of Science in Information Assurance program.

**Diane ("Dione") E. Levine, CISSP, CFE, FBCI, CPS**, deceased, was the President/CEO of Strategic Systems Management, Ltd., and one of the developers of the Certification for Information Systems Security Professionals. She had a notable career in information security as both a developer and implementer of enterprise security systems. Levine held a series of high-level risk management and security positions in major financial institutions, spent many years as an Adjunct Professor at New York University, and was widely published in both the trade and academic press. She contributed numerous chapters to the Third and Fourth Editions of the *Computer Security Handbook*. Ms. Levine split her time between security and business continuity consulting, writing, and teaching worldwide. She was a frequent public speaker and a member of technical panels and regularly contributed articles and columns to *Information Week*, *Information Security*, *Internet Week*, *Planet IT*, *ST&D*, *internet.com* and *Smart Computing*. Levine was Active in the Information Systems Security Association (ISSA), the Association of Certified Fraud Examiners (ASFE), the Business Continuity Institute (BCI), the Contingency Planning Exchange (CPE), and the Information Security Auditing and Control Association (ISACA) and had devoted many years serving on the Board of Directors of these organizations.

**James Landon Linderman, PhD** (e-mail: [jlinderman@aol.com](mailto:jlinderman@aol.com)) is an Associate Professor in the Computer Information Systems department at Bentley College, Waltham, Massachusetts, where he has taught for 30 years. He is a Research Fellow at Bentley's Center for Business Ethics, and past Vice-Chair of the Faculty Senate. A resident of Fitzwilliam, New Hampshire, Linderman is a Permanent Deacon in the Roman Catholic Diocese of Worcester, Massachusetts, and a consultant in the area of computer-assisted academic scheduling and timetable construction.

**Steven Lovaas, MSIA, CISSP**, is the Information Technology Security Manager for Colorado State University. His areas of expertise include IT security policy and architecture, communication and teaching of complex technical concepts, and security issues in both K-12 and higher education. He has taught for the MS program in Information Assurance at Norwich University, and is pursuing a PhD in Public Communications and Technology at Colorado State University. Lovaas currently holds the position of Editor in Chief for the Norwich University *Journal of Information Assurance*. As part of his

volunteer commitment to educating the next generation of scientists and engineers, he coaches, judges, and writes exams for the Science Olympiad program in Colorado.

**Vic Maconachy, PhD**, assumed the position of Vice President for Academic Affairs/Chief Academic Officer at Capitol College, Laurel, Maryland, in October 2007. Maconachy is charged with sustaining and enhancing the academic quality of programs of study ranging from Business Administration through Engineering, Computer Science, and Information Assurance. He also oversees the operations of the Library and the Space Operations Institute. Maconachy holds the rank of Professor and teaches graduate and undergraduate research courses in information assurance.

Prior to joining Capitol College, Maconachy served at the National Security Agency in several leadership positions. He was appointed by the Director of the NSA as the Deputy Senior Computer Science Authority, where he built a development program for a new generation of Cryptologic Computer Scientists. Prior to this position, Maconachy served as the Director of the National Information Assurance Education and Training Program ([www.nsa.gov/ia/academia/acade00001.cfm](http://www.nsa.gov/ia/academia/acade00001.cfm)). He was responsible for implementing a multidimensional, interagency program, providing direct support and guidance to the services, major Department of Defense components, federal agencies, and the greater national information infrastructure community. This program fosters the development and implementation of information assurance training programs as well as graduate and undergraduate education curricula. In this capacity, he served on several national-level government working groups as well as in an advisory capacity to several universities. Maconachy was the principal architect for several national INFOSEC training standards in the national security systems community. During his time at the NSA, he held many different positions, including work as an INFOSEC Operations Officer, INFOSEC Analyst and a Senior INFOSEC Education and Training Officer.

Prior to joining the NSA, Maconachy worked for the Department of Navy. He developed and implemented INFOSEC training programs for users and system maintainers of sophisticated cryptographic equipment. He also served as the Officer in Charge of several INFOSEC-related operations for the Department of Navy, earning him the Department of Navy Distinguished Civilian Service medal. Maconachy holds a PhD from the University of Maryland. He has numerous publications and awards related to information assurance and is the recipient of the prestigious National Cryptologic Meritorious Service Medal.

**John Mason** is a Manager for SingerLewak's Enterprise Risk Management Group. He has over 20 years of combined experience in internal audit, regulatory compliance, information security, investigations, and process reengineering. He has held senior positions, such as Chief Internal Auditor and Vice President of Audit and Compliance in a variety of companies. While at two multibillion-dollar institutions, he was the Chief Information Security Officer and helped establish information risk management programs as well as designed risk-based audit programs several years before Sarbanes-Oxley. Mason has routinely authored, reviewed, and researched finance control policies and procedures. He has performed audits for governmental agencies and managed a full spectrum of financial, operational, SOX compliance, and data processing audits. He possesses an MBA and numerous certificates, including a CISM, CISA, CFE, CBA, CFSA, and CFSSP and is an Adjunct Professor in Norwich University's Master's of Science in Information Assurance program.

## xxx ABOUT THE CONTRIBUTORS

**Peter Mell** is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology. He is the Program Manager for the National Vulnerability Database as well as the Security Content Automation Protocol validation program. These programs are widely adopted within the U.S. government and used for standardizing and automating vulnerability and configuration management, measurement, and policy compliance checking. He has written the NIST publications on patching, malware, intrusion detection, common vulnerability scoring system, and the common vulnerabilities and exposures standard. Mell's research experience includes the areas of intrusion detection systems, vulnerability scoring, and vulnerability databases.

**Michael Miora** has designed and assessed secure, survivable, highly robust systems for Industry and government over the past 30 years. Miora, one of the original professionals granted the Certified Information Systems Security Professional in the 1990s and the ISSMP in 2004, was accepted as a Fellow of the Business Continuity Institute in 2005. Miora founded and currently serves as President of ContingenZ Corporation. Michael Miora was educated at the University of California, Los Angeles and Berkeley, earning Bachelor's and Master's in Mathematics. He is an Adjunct Professor at Norwich University in the MS Information Assurance program and serves on the editorial boards of the Norwich University *Journal of Information Assurance* and the *Business Continuity Journal*.

**Allysa Myers** is the Director of Research for West Coast Labs. Her primary responsibilities are researching and analyzing technology and security threat trends as well as reviewing and developing test methodologies. Prior to joining West Coast Labs, Myers spent 10 years working in the Avert group at McAfee Security, Inc. While there, she wrote for the Avert blog and *Sage* magazine, plus several external publications. She also provided training demonstrations to new researchers within McAfee along with other groups such as the Department of Defense and McAfee Technical Support and Anti-Spyware teams. Myers has been a member of various security industry groups, such as the Wildlist and the Drone Armies mailing list.

**Scott J. Nathan, Esq.** (e-mail: [snathan@mindspring.com](mailto:snathan@mindspring.com)) is an attorney whose practice includes litigation concerning intellectual property and technology matters, computer fraud and abuse, and environmental and insurance coverage matters involving the exchange of millions of pages of documents. In addition, he advises clients about, among other things, Internet-related risks and risk avoidance, proprietary and open source software licensing, service-level agreements, and insurance coverage. Nathan has written and spoken extensively about such issues as online privacy, cyberspace jurisdiction, and the legal issues surrounding the use of open source software. He is admitted to practice before the United States Supreme Court, the United States Court of Appeals for the First Circuit, the Federal District Court for the District of Massachusetts, and the Courts of the Commonwealth of Massachusetts. Nathan is a member of the American Bar Association's Litigation and Computer Litigation Committees.

**Carl Ness, MS, CISSP**, is a Senior Security Analyst for the University of Iowa. Ness has more than 10 years' experience in the information technology and information security fields, mainly in the academic and healthcare sector. He is a speaker, author, and educator on information assurance, including security in the academic environment, messaging security, disaster recovery and business continuity, safe home

## ABOUT THE CONTRIBUTORS xxxi

computing, and information technology operations. Ness previously served as a systems administrator, network administrator, information technology director, and information security officer. He also provides consulting to several security software development organizations.

**Peter G. Neumann** has doctorates from Harvard and Darmstadt. He has been in SRI International's Computer Science Lab since September 1971, after spending 10 years at Bell Labs in Murray Hill, New Jersey. His work is concerned with computer systems and networks, trustworthiness and high assurance, security, reliability, survivability, safety, and many risk-related issues, such as voting-system integrity, crypto policy, social implications, and human needs including privacy. He moderates the ACM Risks Forum ([risks.org](http://risks.org)) and created ACM SIGSOFT's Software Engineering Notes in 1976. He has participated in four studies for the National Academies of Science. His 1995 book, *Computer-Related Risks*, is still timely. He is a Fellow of the ACM, IEEE, and AAAS.

**Lester E. Nichols** earned a BS degree from the University of Phoenix and an MS degree in Information Assurance from Norwich University. He is currently working on his doctoral degree in Information Security at Capella University. He holds the CISSP, MCSA, MCP, and Security+ certifications. Nichols has over 10 years' experience in computer technology in the medical, nonprofit, financial, and local and federal government sectors, in a variety of roles, including application development, network engineering, and information security. Nichols is currently with Knowledge Consulting Group as a Senior Security Engineer, providing security oversight as well as security justification for network and system design implementations, while working with network engineering to integrate security mind-sets to the design stage of projects. Prior to this, he was employed with Prolific Solutions, LLC as a Senior Information Assurance Manager.

**Justin Opatrny** is currently an information systems manager for a Fortune 500 company, with previous roles specializing in network infrastructure and security. He earned a Master's degree in Information Assurance from Norwich University; holds industry certifications including CISSP, GCFA, and GSNA; and is an active member of ISSA and InfraGard. Opatrny also works as an independent consultant providing technology and information assurance expertise and guidance.

**John Orlando, PhD**, is the Program Director for the Master of Science in Business Continuity Management at Norwich University. He received his PhD from the University of Wisconsin, and has published articles in a variety of applied ethics fields, including information ethics, business ethics, and medical ethics. He has also published a number of articles on business continuity management and consults with universities on business continuity programs. Orlando helped develop online programs at the University of Vermont and Norwich University, and was the Associate Program Director for the Master of Science in Information Assurance at Norwich University.

**Raymond Panko, PhD** (e-mail: [Ray@Panko.com](mailto:Ray@Panko.com)) is a Professor of Information Technology Management in the Shidler College of Business at the University of Hawaii. His interest in security began during lunches with Donn Parker in the 1970s at SRI International and has grown ever since. His textbook on IT security, *Corporate Computer and Network Security*, is published by Prentice-Hall. His current research focuses are

## xxxii ABOUT THE CONTRIBUTORS

security for end user applications (especially spreadsheets), how to deal with fraud, and human and organizational controls. His main teaching focus, however, remains networking. In his networking classes and textbook, he emphasizes security throughput, pointing out the security implications of network protocols and practices.

**Robert A. Parisi, Jr.**, is the Senior Vice-President and National Technology, Network Risk and Telecommunications Practice Leader for the FINPRO unit of Marsh USA. Parisi has spoken at various businesses, technology, legal, and insurance forums throughout the world and has written on issues affecting professional liability, privacy, technology, telecommunications, media, intellectual property, computer security, and insurance. In 2002, Parisi was honored by *Business Insurance* magazine as one of the Rising Stars of Insurance.

Immediately prior to joining Marsh, Parisi was the Senior Vice-President and Chief Underwriting Officer of eBusiness Risk Solutions (a unit of the property and casualty companies of American International Group, Inc.). Parisi joined the AIG group of companies in 1998 as legal counsel for its Professional Liability group and held several executive and legal positions within AIG, including the position of Chief Underwriting Officer for Professional Liability and Technology. While at AIG, Parisi oversaw the creation and drafting of underwriting guidelines and policies for all lines of professional liability. Prior to joining AIG, Parisi had been in private practice, principally as legal counsel to various Lloyds of London syndicates handling a variety of professional liability lines.

Parisi graduated cum laude from Fordham College with a B.A. in Economics and received his law degree from Fordham University School of Law. He is admitted to practice in New York and the U.S. District Courts for the Eastern and Southern Districts of New York.

**Donn B. Parker, CISSP**, Fellow of the Association for Computing Machinery (e-mail: [donnlorna@aol.com](mailto:donnlorna@aol.com)) is a retired (1997) senior management consultant who has specialized in information security and computer crime research for 35 of his 50 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty based on interviews with over 200 computer criminals and reviews of the security of many large corporations. He received the 1992 Award for Outstanding Individual Achievement from the Information Systems Security Association, the 1994 National Computer System Security Award from the U.S. NIST/NCSC, the Aerospace Computer Security Associates 1994 Distinguished Lecturer award, and The MIS Training Institute *Infosecurity News* 1996 Lifetime Achievement Award. *Information Security Magazine* identified him as one of the five top Infosecurity Pioneers (1998).

**Padgett Peterson, P.E., CISSP, IAM/IEM**, has been involved with computer security and encryption for over 40 years. Since 1979 he has been employed by different elements of a major aerospace contractor. Peterson is also an Adjunct Professor in the Master's of Science in Information Assurance program at Norwich University.

**Franklin Platt** (e-mail: [Fnplatt@aol.com](mailto:Fnplatt@aol.com) or telephone: 603 449-2211) is Founder and President of Office Planning Services, a Wall Street consultancy for 20 years headquartered in Stark, New Hampshire since 1990. He has worked extensively in security planning, management, and preparedness in both the private and public sectors. His academic background includes business administration and electrical engineering.

## ABOUT THE CONTRIBUTORS xxxiii

He has received extensive government training in emergency management, including terrorism and weapons of mass destruction, much of which is not available to the public. He holds many security certifications and is currently vetted by the FBI and by several states. Platt's areas of expertise include: security risk management; compliance with the latest Homeland Security procedures and other federal regulations that affect the private sector; risk identification and assessment; vulnerability analysis; cost-value studies; response planning; site security surveys and compliance auditing; briefing and training; second opinion; and due diligence.

**Jerrold M. Post, PhD**, is Professor of Psychiatry, Political Psychology, and International Affairs and Director of the Political Psychology Program at George Washington University. He has devoted his entire career to the field of political psychology. Post came to George Washington after a 21-year career with the Central Intelligence Agency, where he was the Founding Director of the Center for the Analysis of Personality and Political Behavior. He played the lead role in developing the Camp David profiles of Menachem Begin and Anwar Sadat for President Jimmy Carter and initiated the U.S. government program in understanding the psychology of terrorism. He is a widely published author, whose most recent book is *The Mind of the Terrorist: The Psychology of Terrorists from the IRA to al-Qaeda*. Post is also a frequent commentator on national and international media.

**N. Todd Pritsky** is the Director of E-learning Courseware at Hill Associates, a telecommunications training company in Colchester, Vermont. He is a Senior Member of the Technical Staff and an instructor of online, lecture, and hands-on classes. His teaching and writing specialties include e-commerce, network security, TCP/IP, and the Internet, and he also leads courses on fast packet and network access technologies. He enjoys writing articles on network security and is a contributing author of *Telecommunications: A Beginner's Guide* (McGraw-Hill/Osborne). Previously he managed a computer center and created multimedia training programs. He holds a BA in Philosophy and Russian/Soviet Studies from Colby College.

**Karthik Raman** (e-mail: [ramankmail@gmail.com](mailto:ramankmail@gmail.com)) is a Research Scientist at McAfee Avert Labs, an internationally renowned research group for fighting malicious software. His work at McAfee focuses on vulnerability research, malware analysis, and security-research automation. His interests include the application of computer and social sciences to computer-security problems and developing security tools. Karthik graduated with BS degrees in Computer Science and Computer Security from Norwich University in 2006, where he studied under Dr. Mich Kabay.

**Bridgitt Robertson** has been teaching business and technology courses for over six years. Her multidisciplinary approach to security awareness analyzes threats in the global enterprise and investigates how an educated workforce can mitigate risks and enhance corporate competitiveness. Prior to teaching, Robertson worked for global companies in the areas of project management, business analysis, and consulting. She is looking forward to obtaining her doctorate in 2009. She is a member of InfraGard.

**Marc Rotenberg** is Executive Director of the Electronic Privacy Information Center in Washington, DC. He teaches information privacy law at Georgetown University Law Center. He has published many articles in legal and scientific journals. He is the coauthor of several books, including *Information Privacy Law, Privacy and Human Rights, The*



## xxxiv ABOUT THE CONTRIBUTORS

*Privacy Law Sourcebook*, and *Litigation under the Federal Open Government Laws*. He frequently testifies before the U.S. Congress and the European Parliament on emerging privacy issues. He is a Fellow of the American Bar Foundation and the recipient of several awards, including the World Technology Award in Law.

**K. Rudolph, CISSP**, is President and Chief Inspiration Officer of Native Intelligence, Inc., a Maryland-based consulting firm focused on providing creative and practical information security awareness solutions. Rudolph develops security awareness products including posters, images, 60-second daily security tips, Web-based and computer-based courses designed in accord with adult-learning principles. She facilitates security awareness peer group meetings and is a frequent speaker at security conferences. In 2006, Rudolph was honored by the Federal Information Security Educators' Association as the Security Educator of the Year. Special areas of interest to Rudolph include storytelling in security awareness and behavior-based messages and metrics.

**Eric Salveggio** is an information technology security professional who enjoys teaching online courses in CMIS for Liberty University and Auditing for Norwich University. He works as a trained ISO 17799, NSTISSI 4011 and 4013 consultant for Dynetics Corporation of Huntsville, Alabama, in IT Security and Auditing, and as a Private Consultant in networking, network design, and security (wired and wireless) with 10 years experience. He previously worked as the IT Director for the Birmingham, Alabama, campus of Virginia College, where he opened two start-up campuses—on ground and online—and created three accredited programs (two undergrad, one graduate level) at state and federal levels in Network and Cyber Security. While in this position, he was chosen as a nominee for the 2006 Information Security Executive Award, and enjoyed being the only educational facility recognized. He was personally awarded a plaque of recognition by the Stonesoft Corporation for the same. He is a published author and photographer, and enjoys working at times as a Technical Editor for Pearson Education and Thomson Publishing on cyber forensics, cyber security, and operating systems.

**Ravi Sandhu** is Cofounder and Chief Scientist of SingleSignOn.Net in Reston, Virginia, and Professor of Information Technology and Engineering at George Mason University in Fairfax, Virginia. An ACM and an IEEE Fellow, he is the founding Editor in Chief of *ACM's Transactions on Information and System Security*, Chairman of ACM's Special Interest Group on Security, Audit and Control, and Security Editor for *IEEE Internet Computing*. Sandhu has published over 140 technical papers on information security. He is a popular teacher and has lectured all over the world. He has provided high-level consulting services to numerous private and government organizations.

**Sondra Schneider** is CEO and Founder of Security University, an Information Security and Information Assurance Training and Certification company. She and SU have challenged security professionals for the past 10 years, delivering hands-on tactical security classes and certifications around the world.

Starting in 2008, SU set up an exam server to meet the demand for tactical security certifications. In 2005, SU refreshed the preexisting AIS security training program to the new "SU Qualified Programs," which meet and exceed security professionals requirements for hands-on tactical security "skills" training. SU delivers the Qualified/Information Security Professional and Qualified/Information Assurance Professional

certifications, which are the first of their kind that measure a candidate's tactical hands-on security skills.

In 2004, Schneider was awarded Entrepreneur of the Year for the First Annual Women of Innovation Award from the Connecticut Technology Council. In 2007, she was Tech Editor for the popular 2007 CEH V5 Study Guide, and a multiple chapter author for the 2007 CHFI Study Guide. She sits on three advisory boards for computer security (start-up) technology companies and is a frequent speaker at computer security and wireless industry events. She is a founding member of the NYC HTCIA and IETF chapters, works closely with (ISC)<sup>2</sup>, ISSA, and ISACA chapters, and the security and wireless vendor community. She specializes in information security, intrusion detection, information assurance (PKI), wireless security and security awareness training.

**William Stallings, PhD** (e-mail: [ws@shore.net](mailto:ws@shore.net)) is a consultant, lecturer, and author of over a dozen professional reference books and textbooks on data communications and computer networking. His clients have included major corporations and government agencies in the United States and Europe. He has received numerous awards for the Best Computer Science Textbook of the Year from the Text and Academic Authors Association. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. Stallings created and maintains the Computer Science Student Resource Site at <http://WilliamStallings.com/StudentSupport.html>.

**Peter Stephenson, PhD**, is a writer, researcher and lecturer on information assurance and risk, information warfare and counterterrorism, and digital investigation and forensics on large-scale computer networks. He has lectured extensively on digital investigation and security and has written or contributed to 14 books and several hundred articles in major national and international trade, technical and scientific publications.

He is the Associate Program Director in the Master's of Science in Information Assurance program at the Norwich University School of Graduate Studies, where he teaches information assurance, cyber crime and cyber law, and digital investigation on both the graduate and undergraduate levels. He is Senior Research Scientist at the Norwich University Applied Research Institutes, Chair of the Department of Computing, and the Chief Information Security Officer for the university.

He has lectured or delivered consulting engagements for the past 23 years in 11 countries plus the United States and has been a technologist for over 40 years. He operated a successful consulting practice for over 20 years and has worked for such companies as Siemens, Tektronix, and QinetiQ (UK).

Stephenson obtained his PhD in computer science at Oxford Brookes University, Oxford, England, where his research was in the structured investigation of digital incidents in complex computing environments. He holds a Master's of Arts degree in Diplomacy with a concentration in Terrorism from Norwich University.

He is on the editorial advisory boards of *International Journal of Digital Evidence* and the Norwich University *Journal of Information Assurance* among several others. Stephenson is technology editor for *SC Magazine* and the editor in chief for Norwich University Press.

Stephenson is a Fellow of the Institute for Communications, Arbitration and Forensics in the United Kingdom and is a member of Michigan InfraGard and the International Federation of Information Processing Technical Committee 11, Working Group 11.9, Digital Forensics. He serves on the steering Committee of the Michigan Electronic Crime Task Force. His research is focused on information conflict.

## **xxxvi ABOUT THE CONTRIBUTORS**

**Gary L. Tagg** is a highly experienced information security professional with over 20 years working in the financial and government sectors. The organizations he has worked with include Deutsche Bank, PA Consulting group, Clearstream, Pearl Assurance, and Lloyds TSB. He has performed a wide range of security roles including risk management, consulting, security architecture, policy and standards, project management, development, testing and auditing. Tagg is currently a risk consultant in Deutsche Bank's IT security Governance Group.

**Nicholas Takacs** is an information security professional and Business Systems Director for a long-term care insurance company. He is also an Adjunct Professor of Information Assurance at Norwich University. Takacs has expertise in the areas of security policy management, security awareness, business continuity planning, and execution. Prior to moving into the insurance industry, Takacs spent several years in the public utility industry focusing on the areas of regulatory compliance, disaster recovery, and identity management.

**James Thomas, MSc CISSP**, is a Senior Partner with Norwich Security Associates, a full-spectrum information assurance consultancy headquartered in Scotland. Thomas spends most of his professional time providing policy, process, and governance advice to large banking and financial organizations in the United Kingdom and Europe. He is a 2004 graduate of the Norwich University Master of Science in Information Assurance program. Prior to focusing his efforts in the security space, he had a long career in Information Technology and Broadcast Engineering spanning the United Kingdom and the eastern United States.

**Lee Tien, Esq.**, is a Senior Staff Attorney with the Electronic Frontier Foundation in San Francisco, California. He specializes in free speech and surveillance law and has authored several law review articles. He received his undergraduate degree in psychology from Stanford University and his law degree from Boalt Hall School of Law, UC Berkeley. He is also a former newspaper reporter.

**Timothy Virtue** is an accomplished information assurance leader with a focus in strategic enterprise technology risk management, information security, data privacy, and regulatory compliance. Virtue has extensive experience with publicly traded corporations, privately held businesses, government agencies, and nonprofit organizations of all sizes. Additionally he holds these professional designations: CISSP, CISA, CCE, CFE, and CIPP/G.

**Myles Walsh** is an Adjunct Professor at three colleges in New Jersey: Ramapo College, County College of Morris, and Passaic County Community. For the past 12 years, he has taught courses in Microsoft Office and Web Page Design. He also implements small Office applications and Web sites. From 1966 until 1989, he worked his way up from programmer to director in several positions at CBS, CBS Records, and CBS News. His formal education includes an MBA from the Baruch School of Business and a BBA from St. John's University.

**Karen F. Worstell, CISM**, is Cofounder and Principal of W Risk Group, a consultancy serving clients across multiple sectors to define due diligence to a defensible standard of care for information protection. Her areas of expertise include incident detection and management, compliance, governance, secure data management and risk

## ABOUT THE CONTRIBUTORS xxxvii

management. She is coauthor of *Evaluating the Electronic Discovery Capabilities of Outside Law Firms: A Model Request for Information and Analysis* (BNA, 2006) and is a frequent speaker and contributor in risk management and information security forums internationally. She participates in ISACA, IIA, and the ABA Science and Technology Section, Information Security Committee, and serves as President of the Puget Sound Chapter of the ISSA.

**Noel Zakin** is President of RANCO Consulting LLC. He has been an information technology/telecommunications industry executive for over 45 years. He has held managerial positions at the Gartner Group, AT&T, the American Institute of CPAs, and Unisys. These positions involved strategic planning, market research, competitive analysis, business analysis, and education and training. His consulting assignments have ranged from the Fortune 500 to small start-ups and have involved data security, strategic planning, conference management, market research, and management of corporate operations. He has been active with ACM, IFIP, and AFIPS and currently with ISSA. He holds an MBA from the Wharton School.

**William A. Zucker, Esq.**, is a partner at McCarter & English, LLP's Boston office. Zucker serves as a senior consultant for the Cutter Consortium on legal issues relating to information technology, outsourcing, and risk management, and is a member of the American Arbitration Association's National Technology Panel and a member of the CPR Institute's working group on technology business alliances and conflict management. He has also served on the faculty of Norwich University, where he taught the intellectual property aspects of computer security. Zucker is a trial lawyer whose practice focuses on negotiation/litigation of business transactions, outsourcing/ebusiness and technology/intellectual property. Among his publications are: "The Legal Framework for Protecting Intellectual Property in the Field of Computing and Computer Software," written for the *Computer Security Handbook*, 4th edition, coauthored with Scott Nathan; and "Intellectual Property and Open Source: Copyright, Copyleft and Other Issues for the Community User."



## A NOTE TO INSTRUCTORS

This two-volume text will serve the interests of practitioners and teachers of information assurance. The fourth edition of the *Handbook* was well received in academia; at least one quarter of all copies were bought by university and college bookstores. The design and contents of this fifth edition have been tailored even more closely to meet those needs as well as the needs of other professionals in the field.

University professors looking for texts appropriate for a two-semester sequence of undergraduate courses in information assurance will find the *Handbook* most suitable. In my own work at Norwich University in Vermont, Volume I is the text for our *IS340 Introduction to Information Assurance* and Volume II is the basis for our *IS342 Management of Information Assurance* courses.

The text will also be useful as a resource in graduate courses. In the School of Graduate Studies at Norwich University, we use both volumes as required and supplementary reading for our 18-month, 36-credit Master of Science in Information Assurance program (MSIA).

I will continue to create and post PowerPoint lecture slides based on the chapters of the *Handbook* on my Norwich University Web site for free access by anyone applying them to noncommercial use (e.g., for self-study, for courses in academic institutions, and for unpaid industry training); the materials will be available in the IS340 and IS342 sections:

[www2.norwich.edu/mkabay/courses/academic/norwich/is340](http://www2.norwich.edu/mkabay/courses/academic/norwich/is340)

[www2.norwich.edu/mkabay/courses/academic/norwich/is342](http://www2.norwich.edu/mkabay/courses/academic/norwich/is342)

M. E. KABAY  
Technical Editor  
*January 2009*



## INTRODUCTION TO PART I

# FOUNDATIONS OF COMPUTER SECURITY

The foundations of computer security include answers to the superficially simple question “What is this all about?” Our first part establishes a technological and historical context for information assurance so that readers will have a broad understanding of why information assurance matters in the real world. Chapters focus on principles that will underlie the rest of the text: historical perspective on the development of our field; how to conceptualize the goals of information assurance in a well-ordered schema that can be applied universally to all information systems; computer hardware and network elements underlying technical security; history and modern developments in cryptography; and how to discuss breaches of information security using a common technical language so that information can be shared, accumulated, and analyzed.

Readers also learn or review the basics of commonly used mathematical models of information security concepts and how to interpret survey data and, in particular, the pitfalls of self-selection in sampling about crimes. Finally, the first section of the text introduces elements of law (U.S. and international) applying to information assurance. This legal framework from a layman’s viewpoint, provides a basis for understanding later chapters; in particular, when examining privacy laws and management’s fiduciary responsibilities.

Chapter titles and topics in Part I include:

- 1. Brief History and Mission of Information System Security.** An overview focusing primarily on developments in the second half of the twentieth century and the first decade of the twenty-first
- 2. History of Computer Crime.** A review of key computer crimes and notorious computer criminals from the 1970s to the mid-2000s
- 3. Toward a New Framework for Information Security.** A systematic and thorough conceptual framework and terminology for discussing the nature and goals of securing all aspects of information, not simply the classic triad of confidentiality, integrity, and availability
- 4. Hardware Elements of Security.** A review of computer and network hardware underlying discussions of computer and network security



## **I · 2 FOUNDATIONS OF COMPUTER SECURITY**

- 5. Data Communications and Information Security.** Fundamental principles and terminology of data communications, and their implications for information assurance
- 6. Network Topologies, Protocols, and Design.** Information assurance of the communications infrastructure
- 7. Encryption.** Historical perspectives on cryptography and steganography from ancient times to today as fundamental tools in securing information
- 8. Using a Common Language for Computer Security Incident Information.** An analytic framework for understanding, describing, and discussing security breaches by using a common language of well-defined terms
- 9. Mathematical Models of Computer Security.** A review of the most commonly referenced mathematical models used to describe information security functions
- 10. Understanding Studies and Surveys of Computer Crime.** Scientific and statistical principles for understanding studies and surveys of computer crime
- 11. Fundamentals of Intellectual Property Law.** An introductory review of cyberlaw: laws governing computer-related crime, including contracts, and intellectual property (trade secrets, copyright, patents, open-source-models). Also, violations (piracy, circumvention of technological defenses), computer intrusions, and international frameworks for legal cooperation

# CHAPTER 1

## BRIEF HISTORY AND MISSION OF INFORMATION SYSTEM SECURITY

Seymour Bosworth and Robert V. Jacobson

<b>1.1 INTRODUCTION TO INFORMATION SYSTEM SECURITY</b>	<b>1-1</b>	1.2.14 1980s: Productivity Enhancements	1-9
<b>1.2 EVOLUTION OF INFORMATION SYSTEMS</b>	<b>1-3</b>	1.2.15 Personal Computer	1-9
1.2.1 1950s: Punched-Card Systems	1-4	1.2.16 Local Area Networks	1-10
1.2.2 Large-Scale Computers	1-4	1.2.17 1990s: Total Interconnection	1-11
1.2.3 Medium-Size Computers	1-5	1.2.18 Telecommuting	1-12
1.2.4 1960s: Small-Scale Computers	1-6	1.2.19 Internet and the World Wide Web	1-12
1.2.5 Transistors and Core Memory	1-7	<b>1.3 GOVERNMENT RECOGNITION OF INFORMATION ASSURANCE</b>	<b>1-13</b>
1.2.6 Time Sharing	1-7	1.3.1 IA Standards	1-13
1.2.7 Real-Time, Online Systems	1-7	1.3.2 Computers at Risk	1-13
1.2.8 A Family of Computers	1-7	1.3.3 InfraGard	1-18
1.2.9 1970s: Microprocessors, Networks, and Worms	1-8	<b>1.4 RECENT DEVELOPMENTS</b>	<b>1-18</b>
1.2.10 First Personal Computers	1-8	<b>1.5 ONGOING MISSION FOR INFORMATION SYSTEM SECURITY</b>	<b>1-19</b>
1.2.11 First Network	1-8	<b>1.6 NOTES</b>	<b>1-19</b>
1.2.12 Further Security Considerations	1-9		
1.2.13 First "Worm."	1-9		

**1.1 INTRODUCTION TO INFORMATION SYSTEM SECURITY.** The growth of computers and of information technology has been explosive. Never before has an entirely new technology been propagated around the world with such speed and with so great a penetration of virtually every human activity. Computers have brought vast benefits to fields as diverse as human genome studies, space exploration, artificial intelligence, and a host of applications from the trivial to the most life-enhancing.

Unfortunately, there is also a dark side to computers: They are used to design and build weapons of mass destruction as well as military aircraft, nuclear submarines,

# CHAPTER 2

## HISTORY OF COMPUTER CRIME

M. E. Kabay

<b>2.1 WHY STUDY HISTORICAL RECORDS?</b>	<b>2·2</b>	2.10.2 Scrambler, 12-Tricks and PC Cyborg	2·12
<b>2.2 OVERVIEW</b>	<b>2·2</b>	2.10.3 1994: Datacomp Hardware Trojan	2·12
<b>2.3 1960S AND 1970S: SABOTAGE</b>	<b>2·2</b>	2.10.4 Keylogger Trojans	2·13
2.3.1 Direct Damage to Computer Centers	2·3	2.10.5 Haephtrati Trojan	2·13
2.3.2 1970–1972: Albert the Saboteur	2·4	2.10.6 Hardware Trojans and Information Warfare	2·14
<b>2.4 IMPERSONATION</b>	<b>2·4</b>	<b>2.11 NOTORIOUS WORMS AND VIRUSES</b>	<b>2·14</b>
2.4.1 1970: Jerry Neal Schneider	2·5	2.11.1 1970–1990: Early Malware Outbreaks	2·14
2.4.2 1980–2003: Kevin Mitnick	2·5	2.11.2 December 1987: Christmas Tree Worm	2·15
2.4.3 Credit Card Fraud	2·6	2.11.3 November 2, 1988: Morris Worm	2·15
2.4.4 Identity Theft Rises	2·7	2.11.4 Malware in the 1990s	2·16
<b>2.5 PHONE PHREAKING</b>	<b>2·7</b>	2.11.5 March 1999: Melissa	2·17
2.5.1 2600 Hz	2·7	2.11.6 May 2000: I Love You	2·19
2.5.2 1982–1991: Kevin Poulsen	2·8	<b>2.12 SPAM</b>	<b>2·19</b>
<b>2.6 DATA DIDDLING</b>	<b>2·9</b>	2.12.1 1994: Green Card Lottery Spam	2·19
2.6.1 Equity Funding Fraud (1964–1973)	2·9	2.12.2 Spam Goes Global	2·20
2.6.2 1994: Vladimir Levin and the Citibank Heist	2·10	<b>2.13 DENIAL OF SERVICE</b>	<b>2·20</b>
<b>2.7 SALAMI FRAUD</b>	<b>2·10</b>	2.13.1 1996: Unemailer	2·20
<b>2.8 LOGIC BOMBS</b>	<b>2·10</b>	2.13.2 2000: MafiaBoy	2·21
<b>2.9 EXTORTION</b>	<b>2·11</b>	<b>2.14 HACKER UNDERGROUND OF THE 1980S AND 1990S</b>	<b>2·21</b>
<b>2.10 TROJAN HORSES</b>	<b>2·11</b>	2.14.1 1981: Chaos Computer Club	2·22
2.10.1 1988 Flu-Shot Hoax	2·11	2.14.2 1982: The 414s	2·22
		2.14.3 1984: Cult of the Dead Cow	2·22
		2.14.4 1984: <i>2600: The Hacker Quarterly</i>	2·23
		2.14.5 1984: Legion of Doom	2·23

## 2.2 HISTORY OF COMPUTER CRIME

2.14.6	1985: <i>Phrack</i>	2.24	2.14.11	2004: Shadowcrew	2.26
2.14.7	1989: Masters of Deception	2.24	<b>2.15 CONCLUDING REMARKS</b>		<b>2.26</b>
2.14.8	1990: Operation Sundevil	2.25	<b>2.16 FURTHER READING</b>		<b>2.27</b>
2.14.9	1990: Steve Jackson Games	2.25	<b>2.17 NOTES</b>		<b>2.27</b>
2.14.10	1992: L0pht Heavy Industries	2.26			

**2.1 WHY STUDY HISTORICAL RECORDS?** Every field of study and expertise develops a common body of knowledge that distinguishes professionals from amateurs. One element of that body of knowledge is a shared history of significant events that have shaped the development of the field. Newcomers to the field benefit from learning the names and significant events associated with their field so that they can understand references from more senior people in the profession, and so that they can put new events and patterns into perspective. This chapter provides a brief overview of some of the more famous (or notorious) cases of computer crime (including those targeting computers and those mediated through computers) of the last four decades.<sup>1</sup>

**2.2 OVERVIEW.** This chapter illustrates several general trends from the 1960s through the decade following 2000:

- In the early decades of modern information technology (IT), computer crimes were largely committed by individual disgruntled and dishonest employees.
- Physical damage to computer systems was a prominent threat until the 1980s.
- Criminals often used authorized access to subvert security systems as they modified data for financial gain or destroyed data for revenge.
- Early attacks on telecommunications systems in the 1960s led to subversion of the long-distance phone systems for amusement and for theft of services.
- As telecommunications technology spread throughout the IT world, hobbyists with criminal tendencies learned to penetrate systems and networks.
- Programmers in the 1980s began writing malicious software, including self-replicating programs, to interfere with personal computers.
- As the Internet increased access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for vandalism, political action, and financial gain.
- As the 1990s progressed, financial crime using penetration and subversion of computer systems increased.
- The types of malware shifted during the 1990s, taking advantage of new vulnerabilities and dying out as operating systems were strengthened, only to succumb to new attack vectors.
- Illegitimate applications of e-mail grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent e-mail.

**2.3 1960S AND 1970S: SABOTAGE.** Early computer crimes often involved physical damage to computer systems and subversion of the long-distance telephone networks.

## TOWARD A NEW FRAMEWORK FOR INFORMATION SECURITY\*

**Donn B. Parker, CISSP**

<b>3.1 PROPOSAL FOR A NEW INFORMATION SECURITY FRAMEWORK</b>	<b>3·1</b>	<b>3.4 COMPREHENSIVE LISTS OF SOURCES AND ACTS CAUSING INFORMATION LOSSES</b>	<b>3·10</b>
<b>3.2 SIX ESSENTIAL SECURITY ELEMENTS</b>	<b>3·3</b>	3.4.1 Complete List of Information Loss Acts	3·11
3.2.1 Loss Scenario 1: Availability	3·4	3.4.2 Examples of Acts and Suggested Controls	3·14
3.2.2 Loss Scenario 2: Utility	3·4	3.4.3 Physical Information and Systems Losses	3·17
3.2.3 Loss Scenario 3: Integrity	3·5	3.4.4 Challenge of Complete Lists	3·18
3.2.4 Loss Scenario 4: Authenticity	3·5	<b>3.5 FUNCTIONS OF INFORMATION SECURITY</b>	<b>3·19</b>
3.2.5 Loss Scenario 5: Confidentiality	3·6	<b>3.6 SELECTING SAFEGUARDS USING A STANDARD OF DUE DILIGENCE</b>	<b>3·22</b>
3.2.6 Loss Scenario 6: Possession	3·7	<b>3.7 THREATS, ASSETS, VULNERABILITIES MODEL</b>	<b>3·22</b>
3.2.7 Conclusions about the Six Elements	3·8	<b>3.8 CONCLUSION</b>	<b>3·22</b>
<b>3.3 WHAT THE DICTIONARIES SAY ABOUT THE WORDS WE USE</b>	<b>3·9</b>		

### 3.1 PROPOSAL FOR A NEW INFORMATION SECURITY FRAMEWORK.

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.

\*This chapter is a revised excerpt from Donn B. Parker, *Fighting Computer Crime* (New York: John Wiley & Sons, 1998), Chapter 10, "A New Framework for Information Security," pp. 229–255.

# CHAPTER 4

## HARDWARE ELEMENTS OF SECURITY

Sy Bosworth and Stephen Cobb

<b>4.1 INTRODUCTION</b>	<b>4·1</b>	4.8.5	Dirt and Dust	4·12
		4.8.6	Radiation	4·12
<b>4.2 BINARY DESIGN</b>	<b>4·2</b>	4.8.7	Downtime	4·13
4.2.1	Pulse Characteristics	4·2		
4.2.2	Circuitry	4·2		
4.2.3	Coding	4·3		
<b>4.3 PARITY</b>	<b>4·4</b>	<b>4.9 DATA COMMUNICATIONS</b>	<b>4·13</b>	
4.3.1	Vertical Redundancy Checks	4.9.1	Terminals	4·13
4.3.2	Longitudinal Redundancy Checks	4.9.2	Wired Facilities	4·14
4.3.3	Cyclical Redundancy Checks	4.9.3	Wireless Communication	4·16
4.3.4	Self-Checking Codes	4·5		
<b>4.4 HARDWARE OPERATIONS</b>	<b>4·6</b>	<b>4.10 CRYPTOGRAPHY</b>	<b>4·16</b>	
<b>4.5 INTERRUPTS</b>	<b>4·7</b>	<b>4.11 BACKUP</b>	<b>4·17</b>	
4.5.1	Types of Interrupts	4.11.1	Personnel	4·18
4.5.2	Trapping	4.11.2	Hardware	4·18
		4.11.3	Power	4·19
<b>4.6 MEMORY AND DATA STORAGE</b>	<b>4·8</b>	4.11.4	Testing	4·20
4.6.1	Main Memory	4·8		
4.6.2	Read-Only Memory	4·8		
4.6.3	Secondary Storage	4·9		
<b>4.7 TIME</b>	<b>4·10</b>	<b>4.12 RECOVERY PROCEDURES</b>	<b>4·20</b>	
4.7.1	Synchronous	4·10		
4.7.2	Asynchronous	4·11		
<b>4.8 NATURAL DANGERS</b>	<b>4·11</b>	<b>4.13 MICROCOMPUTER CONSIDERATIONS</b>	<b>4·20</b>	
4.8.1	Power Failure	4.13.1	Accessibility	4·21
4.8.2	Heat	4.13.2	Knowledge	4·21
4.8.3	Humidity	4.13.3	Motivation	4·21
4.8.4	Water	4.13.4	Opportunity	4·21
		4.13.5	Threats to Microcomputers	4·21
		4.13.6	Maintenance and Repair	4·24
		<b>4.14 CONCLUSION</b>	<b>4·25</b>	
		<b>4.15 HARDWARE SECURITY CHECKLIST</b>	<b>4·25</b>	
		<b>4.16 FURTHER READING</b>	<b>4·27</b>	

**4.1 INTRODUCTION.** Computer hardware has always played a major role in computer security. Over the years, that role has increased dramatically, due to both the

# CHAPTER 5

## DATA COMMUNICATIONS AND INFORMATION SECURITY

Raymond Panko

<b>5.1</b>	<b>INTRODUCTION</b>	<b>5-2</b>	5.6.6 Window Field	5-20	
<b>5.2</b>	<b>SAMPLING OF NETWORKS</b>	<b>5-2</b>	5.6.7 Options	5-20	
5.2.1	Simple Home Network	5-2	5.6.8 Port Numbers	5-20	
5.2.2	Building LAN	5-4	5.6.9 TCP Security	5-22	
5.2.3	Firm's Wide Area Networks (WANs)	5-5	<b>5.7</b>	<b>USER DATAGRAM PROTOCOL</b>	<b>5-22</b>
5.2.4	Internet	5-6	<b>5.8</b>	<b>TCP/IP SUPERVISORY STANDARDS</b>	<b>5-23</b>
5.2.5	Applications	5-8	5.8.1	Internet Control Message Protocol (ICMP)	5-23
<b>5.3</b>	<b>NETWORK PROTOCOLS AND VULNERABILITIES</b>	<b>5-9</b>	5.8.2	Domain Name System (DNS)	5-24
<b>5.4</b>	<b>STANDARDS</b>	<b>5-9</b>	5.8.3	Dynamic Host Configuration Protocol (DHCP)	5-25
5.4.1	Core Layers	5-9	5.8.4	Dynamic Routing Protocols	5-26
5.4.2	Layered Standards Architectures	5-10	5.8.5	Simple Network Management Protocol (SNMP)	5-26
5.4.3	Single-Network Standards	5-11	<b>5.9</b>	<b>APPLICATION STANDARDS</b>	<b>5-26</b>
5.4.4	Internetworking Standards	5-13	5.9.1	HTTP and HTML	5-27
<b>5.5</b>	<b>INTERNET PROTOCOL (IP)</b>	<b>5-13</b>	5.9.2	E-Mail	5-27
5.5.1	IP Version 4 Packet	5-13	5.9.3	Telnet, FTP, and SSH	5-27
5.5.2	IP Version 6	5-15	5.9.4	Other Application Standards	5-27
5.5.3	IPsec	5-16	<b>5.10</b>	<b>CONCLUDING REMARKS</b>	<b>5-28</b>
<b>5.6</b>	<b>TRANSMISSION CONTROL PROTOCOL (TCP)</b>	<b>5-17</b>	<b>5.11</b>	<b>FURTHER READING</b>	<b>5-28</b>
5.6.1	Connection-Oriented and Reliable Protocol	5-17	<b>5.12</b>	<b>NOTES</b>	<b>5-28</b>
5.6.2	Reliability	5-19			
5.6.3	Flag Fields	5-19			
5.6.4	Octets and Sequence Number	5-19			
5.6.5	Acknowledgment Numbers	5-20			

# CHAPTER 6

## NETWORK TOPOLOGIES, PROTOCOLS, AND DESIGN

Gary C. Kessler and N. Todd Pritsky

<b>6.1 OVERVIEW</b>	<b>6-2</b>	6.5.1 OSI Model versus LAN Model Architectures	6-14
6.1.1 LAN Characteristics	6-2	6.5.2 IEEE 802 Standards	6-16
6.1.2 LAN Components	6-2	6.5.3 IEEE 802.3 CSMA/CD Standard	6-18
6.1.3 LAN Technology Parameters	6-3	6.5.4 Ethernet II	6-19
6.1.4 Summary	6-3	6.5.5 IEEE 802.5 Token-Ring Standard	6-20
<b>6.2 LAN TOPOLOGY</b>	<b>6-3</b>	6.5.6 IEEE 802.2 LLC Standard	6-22
6.2.1 Network Control	6-3	6.5.7 Summary	6-23
6.2.2 Star Topology	6-4	<b>6.6 INTERCONNECTION DEVICES</b>	<b>6-23</b>
6.2.3 Ring Topology	6-4	6.6.1 Hubs	6-23
6.2.4 Bus Topology	6-5	6.6.2 Switches	6-24
6.2.5 Physical versus Logical Topology	6-6	6.6.3 Bridges	6-24
<b>6.3 MEDIA</b>	<b>6-8</b>	6.6.4 Routers	6-25
6.3.1 Coaxial Cable	6-8	6.6.5 Summary	6-25
6.3.2 Twisted Pair	6-9	<b>6.7 NETWORK OPERATING SYSTEMS</b>	<b>6-26</b>
6.3.3 Optical Fiber	6-9	<b>6.8 SUMMARY</b>	<b>6-27</b>
6.3.4 Wireless “Media”	6-10	<b>6.9 WEB SITES</b>	<b>6-28</b>
6.3.5 Summary	6-12	<b>6.10 FURTHER READING</b>	<b>6-28</b>
<b>6.4 MEDIA ACCESS CONTROL</b>	<b>6-12</b>	<b>6.11 NOTES</b>	<b>6-28</b>
6.4.1 Contention	6-12		
6.4.2 Distributed Polling	6-13		
<b>6.5 LAN PROTOCOLS AND STANDARDS</b>	<b>6-14</b>		

This chapter provides a broad overview of local area network (LAN) concepts, basic terms, standards, and technologies. These topics are important to give the information security professional a better understanding of the terms that might be used to describe a particular network implementation and its products. The chapter also is written with an eye to what information security professionals need to know; for a more complete



# CHAPTER 7

## ENCRYPTION

Stephen Cobb and Corinne LeFrançois

<b>7.1 INTRODUCTION TO CRYPTOGRAPHY</b>	<b>7·1</b>	7.3.6 DES Weakness	7·20
7.1.1 Terminology	7·2	<b>7.4 PUBLIC KEY ENCRYPTION</b>	<b>7·22</b>
7.1.2 Role of Cryptography	7·3	7.4.1 Key-Exchange Problem	7·22
7.1.3 Limitations	7·6	7.4.2 Public Key Systems	7·23
<b>7.2 BASIC CRYPTOGRAPHY</b>	<b>7·6</b>	7.4.3 Authenticity and Trust	7·25
7.2.1 Early Ciphers	7·6	7.4.4 Limitations and Combinations	7·26
7.2.2 More Cryptic Terminology	7·8	<b>7.5 PRACTICAL ENCRYPTION</b>	<b>7·27</b>
7.2.3 Basic Cryptanalysis	7·8	7.5.1 Communications and Storage	7·27
7.2.4 Brute Force Cryptanalysis	7·9	7.5.2 Securing the Transport Layer	7·28
7.2.5 Monoalphabetical Substitution Ciphers	7·11	7.5.3 X.509v3 Certificate Format	7·31
7.2.6 Polyalphabetical Substitution Ciphers	7·12	<b>7.6 BEYOND RSA AND DES</b>	<b>7·35</b>
7.2.7 The Vigenère Cipher	7·13	7.6.1 Elliptic Curve Cryptography	7·35
7.2.8 Early-Twentieth-Century Cryptanalysis	7·14	7.6.2 RSA Patent Expires	7·36
7.2.9 Adding Up XOR	7·15	7.6.3 DES Superseded	7·37
<b>7.3 DES AND MODERN ENCRYPTION</b>	<b>7·16</b>	7.6.4 Quantum Cryptography	7·38
7.3.1 Real Constraints	7·16	7.6.5 Snake Oil Factor	7·42
7.3.2 One-Time Pad	7·17	<b>7.7 FURTHER READING</b>	<b>7·43</b>
7.3.3 Transposition, Rotors, Products, and Blocks	7·18	<b>7.8 NOTES</b>	<b>7·44</b>
7.3.4 Data Encryption Standard	7·19		
7.3.5 DES Strength	7·20		

**7.1 INTRODUCTION TO CRYPTOGRAPHY.** The ability to transform data so that they are accessible only to authorized persons is just one of the many valuable services performed by the technology commonly referred to as encryption. This technology has appeared in other chapters, but some readers may not be familiar with its principles and origins. The purpose of this chapter is to explain encryption technology in basic terms and to describe its application in areas such as file encryption, message scrambling, authentication, and secure Internet transactions. This is not a theoretical or scientific treatise on encryption, but a practical guide for those who need to employ encryption in a computer security context.

# USING A COMMON LANGUAGE FOR COMPUTER SECURITY INCIDENT INFORMATION

John D. Howard

<b>8.1 INTRODUCTION</b>	<b>8·1</b>	8.4.3 Full Incident Information Taxonomy	8·15
<b>8.2 WHY A COMMON LANGUAGE IS NEEDED</b>	<b>8·2</b>	<b>8.5 ADDITIONAL INCIDENT INFORMATION TERMS</b>	<b>8·17</b>
<b>8.3 DEVELOPMENT OF THE COMMON LANGUAGE</b>	<b>8·3</b>	8.5.1 Success and Failure	8·17
		8.5.2 Site and Site Name	8·17
		8.5.3 Other Incident Terms	8·17
<b>8.4 COMPUTER SECURITY INCIDENT INFORMATION TAXONOMY</b>	<b>8·4</b>	<b>8.6 HOW TO USE THE COMMON LANGUAGE</b>	<b>8·18</b>
8.4.1 Events	8·4	<b>8.7 NOTES</b>	<b>8·20</b>
8.4.2 Attacks	8·12		

**8.1 INTRODUCTION.** A computer security *incident* is some set of events that involves an attack or series of attacks at one or more sites. (See Section 8.4.3 for a more formal definition of the term “incident.”) Dealing with these incidents is inevitable for individuals and organizations at all levels of computer security. A major part of dealing with these incidents is recording and receiving incident information, which almost always is in the form of relatively unstructured text files. Over time, these files can end up containing a large quantity of very valuable information. Unfortunately, the unstructured form of the information often makes incident information difficult to manage and use.

This chapter presents the results of several efforts over the last few years to develop and propose a method to handle these unstructured, computer security incident records. Specifically, this chapter presents a *tool* designed to help individuals and organizations record, understand, and share computer security incident information. We call the tool the *common language for computer security incident information*. This common language contains two parts:

1. A set of “high-level” incident-related terms
2. A method of classifying incident information (a taxonomy)

## MATHEMATICAL MODELS OF COMPUTER SECURITY

**Matt Bishop**

<b>9.1 WHY MODELS ARE IMPORTANT</b>	<b>9·1</b>	9.3.3 Role-Based Access Control Models and Groups	9·7
		9.3.4 Summary	9·9
<b>9.2 MODELS AND SECURITY</b>	<b>9·3</b>	<b>9.4 CLASSIC MODELS</b>	<b>9·9</b>
9.2.1 Access-Control Matrix Model	9·3	9.4.1 Bell-LaPadula Model	9·9
9.2.2 Harrison, Ruzzo, and Ullman and Other Results	9·5	9.4.2 Biba’s Strict Integrity Policy Model	9·12
9.2.3 Typed Access Control Model	9·6	9.4.3 Clark-Wilson Model	9·14
		9.4.4 Chinese Wall Model	9·16
		9.4.5 Summary	9·18
<b>9.3 MODELS AND CONTROLS</b>	<b>9·6</b>	<b>9.5 OTHER MODELS</b>	<b>9·18</b>
9.3.1 Mandatory and Discretionary Access-Control Models	9·6	<b>9.6 CONCLUSION</b>	<b>9·19</b>
9.3.2 Originator-Controlled Access-Control Model and DRM	9·6	<b>9.7 FURTHER READING</b>	<b>9·19</b>
		<b>9.8 NOTES</b>	<b>9·20</b>

**9.1 WHY MODELS ARE IMPORTANT.** When you drive a new car, you look for specific items that will help you control the car: the accelerator, the brake, the shift, and the steering wheel. These exist on all cars and perform the function of speeding the car up, slowing it down, and turning it left and right. This forms a model of the car. With these items properly working, you can make a convincing argument that the model correctly describes what a car must have in order to move and be steered properly.

A model in computer security serves the same purpose. It presents a general description of a computer system (or collection of systems). The model provides a definition of “protect” (e.g., “keep confidential” or “prevent unauthorized change to”) and conditions under which the protection is provided. With mathematical models, the conditions can be shown to provide the stated protection. This provides a high degree of assurance that the data and programs are protected, assuming the model is implemented correctly.

# CHAPTER 10

## UNDERSTANDING STUDIES AND SURVEYS OF COMPUTER CRIME

**M. E. Kabay**

<b>10.1 INTRODUCTION</b>	<b>10·1</b>	10.2.1 Some Fundamentals of Statistical Design and Analysis	10·3
10.1.1 Value of Statistical Knowledge Base	10·1	10.2.2 Research Methods Applicable to Computer Crime	10·9
10.1.2 Limitations on Our Knowledge of Computer Crime	10·1	<b>10.3 SUMMARY</b>	<b>10·11</b>
10.1.3 Limitations on the Applicability of Computer Crime Statistics	10·2	<b>10.4 FURTHER READING</b>	<b>10·11</b>
<b>10.2 BASIC RESEARCH METHODOLOGY</b>	<b>10·3</b>	<b>10.5 NOTES</b>	<b>10·11</b>

**10.1 INTRODUCTION.** This chapter provides guidance for critical reading of research results about computer crime. It will also alert designers of research instruments who may lack formal training in survey design and analysis to the need for professional support in developing questionnaires and analyzing results.

**10.1.1 Value of Statistical Knowledge Base.** Security specialists are often asked about computer crime; for example, customers want to know who is attacking which systems, how often, using what methods. These questions are perceived as important because they bear on the strategies of risk management; in theory, in order to estimate the appropriate level of investment in security, it would be helpful to have a sound grasp of the probability of different levels of damage. Ideally, one would want to evaluate an organization's level of risk by evaluating the experiences of other organizations with similar system and business characteristics. Such comparisons would be useful in competitive analysis and in litigation over standards of due care and diligence in protecting corporate assets.

**10.1.2 Limitations on Our Knowledge of Computer Crime.** Unfortunately, in the current state of information security, no one can give reliable answers to such questions. There are two fundamental difficulties preventing us from

# CHAPTER 11

## FUNDAMENTALS OF INTELLECTUAL PROPERTY LAW

William A. Zucker and Scott J. Nathan

<b>11.1</b>	<b>INTRODUCTION</b>	<b>11·2</b>	11.4.3	First Sale Limitation	11·9
<b>11.2</b>	<b>THE MOST FUNDAMENTAL BUSINESS TOOL FOR PROTECTION OF TECHNOLOGY IS THE CONTRACT</b>	<b>11·3</b>	11.4.4	Fair Use Exception	11·10
11.2.1	Prevention Begins at Home—Employee and Fiduciary Duties	11·4	11.4.5	Formulas Cannot be Copyrighted	11·10
11.2.2	Employment Contract, Manual, and Handbook	11·4	11.4.6	Copyright Does Not Protect the “Look and Feel” for Software Products	11·10
11.2.3	Technology Rights and Access in Contracts with Vendors and Users	11·4	11.4.7	Reverse Engineering as a Copyright Exception	11·11
<b>11.3</b>	<b>PROPRIETARY RIGHTS AND TRADE SECRETS</b>	<b>11·5</b>	11.4.8	Interfaces	11·11
11.3.1	Remedies for Trade Secret Misappropriation	11·6	11.4.9	Transformative Uses	11·11
11.3.2	Vigilance Is a Best Practice	11·8	11.4.10	Derivative Works	11·12
<b>11.4</b>	<b>COPYRIGHT LAW AND SOFTWARE</b>	<b>11·8</b>	11.4.11	Semiconductor Chip Protection Act of 1984	11·12
11.4.1	Works for Hire and Copyright Ownership	11·8	11.4.12	Direct, Contributory, or Vicarious Infringement	11·12
11.4.2	Copyright Rights Adhere from the Creation of the Work	11·9	11.4.13	Civil and Criminal Remedies	11·13
<b>11.5</b>	<b>DIGITAL MILLENNIUM COPYRIGHT ACT</b>	<b>11·14</b>			
<b>11.6</b>	<b>CIRCUMVENTING TECHNOLOGY MEASURES</b>	<b>11·14</b>			
11.6.1	Exceptions to the Prohibitions on Technology Circumvention	11·16			

## 11 · 2 FUNDAMENTALS OF INTELLECTUAL PROPERTY LAW

<b>11.7</b>	<b>PATENT PROTECTION</b>	<b>11 · 18</b>	<b>11.10</b>	<b>OPEN SOURCE</b>	<b>11 · 33</b>
11.7.1	Patent Protection Requires Disclosure	11 · 19	11.10.1	Open Source Licenses	11 · 33
11.7.2	Patent Protection in Other Jurisdictions	11 · 19	11.10.2	GPL	11 · 33
11.7.3	Patent Infringement	11 · 19	11.10.3	Other Open Source Licenses	11 · 34
			11.10.4	Business Policies with Respect to Open Source Licenses	11 · 34
<b>11.8</b>	<b>PIRACY AND OTHER INTRUSIONS</b>	<b>11 · 20</b>	<b>11.11</b>	<b>APPLICATION INTERNATIONALLY</b>	<b>11 · 34</b>
11.8.1	Marketplace	11 · 20	11.11.1	Agreement on Trade-Related Aspects of Intellectual Property Rights	11 · 35
11.8.2	Database Protection	11 · 21	11.11.2	TRIPS and Trade Secrets	11 · 36
11.8.3	Applications of Transformative and Fair Use	11 · 21	11.11.3	TRIPS and Copyright	11 · 37
11.8.4	Internet Hosting and File Distribution	11 · 22	11.11.4	TRIPS and Patents	11 · 37
11.8.5	Web Crawlers and Fair Use	11 · 23	11.11.5	TRIPS and Anticompetitive Restrictions	11 · 38
11.8.6	HyperLinking	11 · 23	11.11.6	Remedies and Enforcement Mechanisms	11 · 38
11.8.7	File Sharing	11 · 23	<b>11.12</b>	<b>CONCLUDING REMARKS</b>	<b>11 · 39</b>
<b>11.9</b>	<b>OTHER TOOLS TO PREVENT UNAUTHORIZED INTRUSIONS</b>	<b>11 · 24</b>	<b>11.13</b>	<b>FURTHER READING</b>	<b>11 · 39</b>
11.9.1	Trespass	11 · 24	<b>11.14</b>	<b>NOTES</b>	<b>11 · 39</b>
11.9.2	Terms of Use	11 · 25			
11.9.3	Computer Fraud and Abuse Act	11 · 26			
11.9.4	Electronic Communications and Privacy	11 · 29			
11.9.5	Stored Communications Act	11 · 32			

**11.1 INTRODUCTION.** This chapter is not for lawyers or law students. Rather, it is written for computer professionals who might find it useful to understand how their concerns at work fit into a legal framework, and how that framework shapes strategies that they might employ in their work. It is not intended to be definitive but to help readers spot issues when they arise and to impart an understanding that is the first part of a fully integrated computer security program.

The word “cyberlaw” is really a misnomer. Cyberlaw is a compendium of traditional law that has been updated and applied to new technologies. When gaps have developed or traditional law is inadequate, particular statutes have been enacted. It is a little like the old story of the three blind men and the elephant: One of the blind men touching the elephant’s leg believes he is touching a tree; the other touching its ear believes it is a wing, and the third, touching the tail, thinks it is a snake. Issues of cyberspace, electronic data, networks, global transmissions, and positioning have neither simple unitary solutions nor a simple body of law to consult.

## INTRODUCTION TO PART II

# THREATS AND VULNERABILITIES

What are the practical, technical problems faced by security practitioners? Readers are introduced to what is known about the psychological profiles of computer criminals and employees who commit insider crime. The focus is then widened to look at national security issues involving information assurance—critical infrastructure protection in particular. After a systematic review of how criminals penetrate security perimeters—essential for developing proper defensive mechanisms—readers can study a variety of programmatic attacks (widely used by criminals) and methods of deception, such as social engineering. The section ends with a review of widespread problems such as spam, phishing, Trojans, Web-server security problems, and physical facility vulnerabilities (an important concern for security specialists, but one that is often overlooked by computer-oriented personnel).

The chapter titles and topics in Part II include:

12. **The Psychology of Computer Criminals.** Psychological insights into motivations and behavioral disorders of criminal hackers and virus writers
13. **The Dangerous Technology Insider: Psychological Characteristics and Career Patterns.** Identifying potential risks among employees and other authorized personnel
14. **Information Warfare.** Cyberconflict and protection of national infrastructures
15. **Penetrating Computer Systems and Networks.** Widely used penetration techniques for breaching security perimeters
16. **Malicious Code.** Dangerous computer programs, including viruses and worms
17. **Mobile Code.** Analysis of applets, controls, scripts and other small programs, including those written in activeX, Java, and Javascript
18. **Denial-of-Service Attacks.** Resource saturation and outright sabotage that brings down availability of systems
19. **Social Engineering and Low-Tech Attacks.** Lying, cheating, impersonation, intimidation—and countermeasures to strengthen organizations against such attacks

## **II · 2 THREATS AND VULNERABILITIES**

- 20. Spam, Phishing, and Trojans: Attacks Meant to Fool.** Fighting spam, phishing, and Trojans
- 21. Web-Based Vulnerabilities.** Web servers, and how to strengthen their defenses
- 22. Physical Threats to the Information Infrastructure.** Attacks against the information infrastructure, including buildings and network media



# CHAPTER 12

## THE PSYCHOLOGY OF COMPUTER CRIMINALS

Q. Campbell and David M. Kennedy

<b>12.1 INTRODUCTION</b>	<b>12·1</b>	12.5.2 Five-Factor Model of Personality and Computer Criminals	12·9
<b>12.2 SELF-REPORTED MOTIVATIONS</b>	<b>12·3</b>	12.5.3 Asperger Syndrome and Computer Criminals	12·10
<b>12.3 PSYCHOLOGICAL PERSPECTIVES ON COMPUTER CRIME</b>	<b>12·3</b>	12.5.4 Computer Addiction and Computer Crime	12·11
<b>12.4 SOCIAL DISTANCE, ANONYMITY, AGGRESSION, AND COMPUTER CRIME</b>	<b>12·4</b>	<b>12.6 ETHICS AND COMPUTER CRIME</b>	<b>12·12</b>
12.4.1 Social Presence and Computer Crime	12·5	<b>12.7 CLASSIFICATIONS OF COMPUTER CRIMINALS</b>	<b>12·15</b>
12.4.2 Deindividuation and Computer Crime	12·6	12.7.1 Early Classification Theories of Computer Criminals	12·16
12.4.3 Social Identity Theory and Computer Crime	12·6	12.7.2 Rogers's New Taxonomy of Computer Criminals	12·18
12.4.4 Social Learning Theory of Computer Crime	12·7	12.7.3 Virus Creators	12·19
<b>12.5 INDIVIDUAL DIFFERENCES AND COMPUTER CRIMINALS</b>	<b>12·8</b>	<b>12.8 SUMMARY AND CONCLUSIONS</b>	<b>12·21</b>
12.5.1 Narcissistic Personalities and Computer Criminals	12·9	<b>12.9 NOTES</b>	<b>12·22</b>

**12.1 INTRODUCTION.** In modern society, it is virtually impossible to go through the day without using computers to assist us in our various tasks and roles. We use computers extensively in both our professional and personal lives. We rely on them to interact with coworkers and associates, to regulate the climate in our homes, to operate our automobiles, to update our finances, and even to monitor and protect our loved ones. However, this ever-increasing reliance on technology comes at a cost. As we become more dependent on information technology, we are also becoming increasingly vulnerable to attacks and exploitation by computer criminals.

# CHAPTER 13

## THE DANGEROUS INFORMATION TECHNOLOGY INSIDER: PSYCHOLOGICAL CHARACTERISTICS AND CAREER PATTERNS<sup>1</sup>

**Jerrold M. Post**

<b>13.1</b>	<b>COMPUTER INFORMATION TECHNOLOGY INSIDERS</b>	<b>13-1</b>	<b>13.4</b>	<b>ESCALATING PATHWAY TO MAJOR COMPUTER CRIME</b>	<b>13-3</b>
<b>13.2</b>	<b>PSYCHOLOGICAL CHARACTERISTICS OF INFORMATION TECHNOLOGY SPECIALISTS</b>	<b>13-2</b>	<b>13.5</b>	<b>STRESS AND ATTACKS ON COMPUTER SYSTEMS</b>	<b>13-5</b>
<b>13.3</b>	<b>CHARACTERISTICS OF THE DANGEROUS COMPUTER INFORMATION TECHNOLOGY INSIDER (CITI)</b>	<b>13-2</b>	<b>13.6</b>	<b>TYPOLGY OF COMPUTER CRIME PERPETRATORS</b>	<b>13-6</b>
			<b>13.7</b>	<b>CONCLUSION AND IMPLICATIONS</b>	<b>13-8</b>
			<b>13.8</b>	<b>NOTE</b>	<b>13-9</b>

**13.1 COMPUTER INFORMATION TECHNOLOGY INSIDERS.** In the complex world of information technology, it is people who create the systems and it is people with authorized access, the computer information technology insiders (CITIs), who represent the greatest threat to these systems.

Computer security experts have developed ever more sophisticated technological solutions to protect sensitive information and combat computer fraud. But no matter how sensitive the computer intrusion detection devices, no matter how impenetrable the firewalls, they will be of no avail in countering the malicious insider.

In considering the population of authorized insiders, it is clear just how broad and variegated this category is and that the line between insiders and outsiders is often blurred.

CITIs include:

- Staff employees
- Contractors and consultants
- Partners and customers

# CHAPTER 14

## INFORMATION WARFARE

**Seymour Bosworth**

<b>14.1 INTRODUCTION</b>	<b>14·2</b>	14.4.5 Criminals	14·17
		14.4.6 Hobbyists	14·17
<b>14.2 VULNERABILITIES</b>	<b>14·2</b>	<b>14.5 WEAPONS OF CYBERWAR</b>	<b>14·17</b>
14.2.1 Critical Infrastructure	14·2	14.5.1 Denial of Service and Distributed Denial of Service	14·18
14.2.2 Off-the-Shelf Software	14·3	14.5.2 Malicious Code	14·18
14.2.3 Dissenting Views	14·3	14.5.3 Cryptography	14·19
14.2.4 Rebuttal	14·4	14.5.4 Psychological Operations	14·19
<b>14.3 GOALS AND OBJECTIVES</b>	<b>14·4</b>	14.5.5 Physical Attacks	14·20
14.3.1 Infrastructure	14·4	14.5.6 Biological and Chemical Weapons and Weapons of Mass Destruction	14·21
14.3.2 Military	14·4	14.5.7 Weapons Inadvertently Provided	14·21
14.3.3 Government	14·7	<b>14.6 DEFENSES</b>	<b>14·21</b>
14.3.4 Transportation	14·8	14.6.1 Legal Defenses	14·21
14.3.5 Commerce	14·9	14.6.2 Forceful Defenses	14·22
14.3.6 Financial Disruptions	14·10	14.6.3 Technical Defenses	14·23
14.3.7 Medical Security	14·11	14.6.4 In-Kind Counterattacks	14·23
14.3.8 Law Enforcement	14·11	14.6.5 Cooperative Efforts	14·23
14.3.9 International and Corporate Espionage	14·12	14.6.6 Summary	14·23
14.3.10 Communications	14·13	<b>14.7 FURTHER READING</b>	<b>14·24</b>
14.3.11 Destabilization of Economic Infrastructure	14·13	<b>14.8 NOTES</b>	<b>14·25</b>
<b>14.4 SOURCES OF THREATS AND ATTACKS</b>	<b>14·13</b>		
14.4.1 Nation-States	14·13		
14.4.2 Cyberterrorists	14·15		
14.4.3 Corporations	14·16		
14.4.4 Activists	14·17		

*Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries.*

—Dr. Ivan Goldberg, Institute for Advanced Study of Information Warfare

# CHAPTER 15

## PENETRATING COMPUTER SYSTEMS AND NETWORKS

**Chey Cobb, Stephen Cobb, and M. E. Kabay**

<b>15.1 MULTIPLE FACTORS INVOLVED IN SYSTEM PENETRATION</b>	<b>15·1</b>	15.3.4 Spying	15·19
15.1.1 System Security: More than a Technical Issue	15·1	15.3.5 Penetration Testing, Toolkits, and Techniques	15·19
15.1.2 Organizational Culture	15·2	15.3.6 Penetration via Web Sites	15·25
15.1.3 Chapter Organization	15·3	15.3.7 Role of Malware and Botnets	15·29
<b>15.2 NONTECHNICAL PENETRATION TECHNIQUES</b>	<b>15·3</b>	<b>15.4 POLITICAL AND LEGAL ISSUES</b>	<b>15·30</b>
15.2.1 Misrepresentation (Social Engineering)	15·3	15.4.1 Exchange of System Penetration Information	15·31
15.2.2 Incremental Information Leveraging	15·6	15.4.2 Full Disclosure	15·31
<b>15.3 TECHNICAL PENETRATION TECHNIQUES</b>	<b>15·7</b>	15.4.3 Sources	15·32
15.3.1 Data Leakage: A Fundamental Problem	15·7	15.4.4 Future of Penetration	15·34
15.3.2 Intercepting Communications	15·8	<b>15.5 SUMMARY</b>	<b>15·34</b>
15.3.3 Breaching Access Controls	15·14	<b>15.6 FURTHER READING</b>	<b>15·35</b>
		<b>15.7 NOTES</b>	<b>15·36</b>

**15.1 MULTIPLE FACTORS INVOLVED IN SYSTEM PENETRATION.** Although penetrating computer systems and networks may sound like a technical challenge, most information security professionals are aware that systems security has both technical and nontechnical aspects. Both aspects come into play when people attempt to penetrate systems. Both aspects are addressed in this chapter, which is not a handbook on how to penetrate systems but rather a review of the methods and means by which systems penetrations are accomplished.

**15.1.1 System Security: More than a Technical Issue.** The primary nontechnical factor in system security and resistance to system penetration is human

# CHAPTER 16

## MALICIOUS CODE

Robert Guess and Eric Salvaggio

<b>16.1 INTRODUCTION</b>	<b>16·1</b>	16.4.1 Signature-Based Malicious Code Detection	16·8
<b>16.2 MALICIOUS CODE THREAT MODEL</b>	<b>16·2</b>	16.4.2 Network-Based Malicious Code Detection	16·8
16.2.1 Self-Replicating Code	16·2	16.4.3 Behavioral Malicious Code Detection	16·9
16.2.2 Actors: Origin of Malicious Code Threats	16·2	16.4.4 Heuristic Malicious Code Detection	16·9
16.2.3 Actors: Structured Threats	16·2	<b>16.5 PREVENTION OF MALICIOUS CODE ATTACKS</b>	<b>16·9</b>
16.2.4 Actors: Unstructured Threats	16·3	16.5.1 Defense in Depth	16·9
16.2.5 Access versus Action: Vector versus Payload	16·3	16.5.2 Operational Controls for Malicious Code	16·9
<b>16.3 SURVEY OF MALICIOUS CODE</b>	<b>16·3</b>	16.5.3 Human Controls for Malicious Code	16·9
16.3.1 Viruses	16·3	16.5.4 Technical Controls for Malicious Code	16·10
16.3.2 Worms	16·5	<b>16.6 CONCLUSION</b>	<b>16·11</b>
16.3.3 Trojans	16·6	<b>16.7 FURTHER READING</b>	<b>16·11</b>
16.3.4 Spyware	16·6	<b>16.8 NOTES</b>	<b>16·11</b>
16.3.5 Rootkits	16·7		
16.3.6 IRC Bots	16·7		
16.3.7 Malicious Mobile Code	16·8		
<b>16.4 DETECTION OF MALICIOUS CODE</b>	<b>16·8</b>		

**16.1 INTRODUCTION.** Malicious logic (or code) is “hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose.”<sup>1</sup> In this chapter, we enumerate the common types of malicious code, sources of malicious code, methods of malicious code replication, and methods of malicious code detection.

Common types of malicious code include viruses, worms, Trojan horses, spyware, rootkits, and bots. Emerging malicious code threats include kleptographic code, cryptoviruses, and hardware-based rootkits. Present-day malicious code threats do not always fit into neat categories, resulting in confusion when discussing the topic. It is not possible to classify all code as being *good* code or *malicious* code. Absent the *mens rea*, or criminal intent of the author or user, code is neither good nor bad. Authors develop code to achieve some goal or fulfill some purpose just as users run code to

# CHAPTER 17

## MOBILE CODE

Robert Gezelter

<b>17.1 INTRODUCTION</b>	<b>17·1</b>	17.3.1 Java	17·9
17.1.1 Mobile Code from the World Wide Web	17·2	<b>17.4 DISCUSSION</b>	<b>17·10</b>
17.1.2 Motivations and Goals	17·3	17.4.1 Asymmetric, and Transitive or Derivative, Trust	17·10
17.1.3 Design and Implementation Errors	17·4	17.4.2 Misappropriation and Subversion	17·11
<b>17.2 SIGNED CODE</b>	<b>17·4</b>	17.4.3 Multidimensional Threat	17·11
17.2.1 Authenticode	17·5	17.4.4 Client Responsibilities	17·11
17.2.2 Fundamental Limitations of Signed Code	17·5	17.4.5 Server Responsibilities	17·12
17.2.3 Specific Problems with the ActiveX Security Model	17·6	<b>17.5 SUMMARY</b>	<b>17·13</b>
17.2.4 Case Studies	17·6	<b>17.6 FURTHER READING</b>	<b>17·13</b>
<b>17.3 RESTRICTED OPERATING ENVIRONMENTS</b>	<b>17·8</b>	<b>17.7 NOTES</b>	<b>17·14</b>

**17.1 INTRODUCTION.** At its most basic, mobile code is a set of instructions that are delivered to a remote computer for dynamic execution. The problems with mobile code stem from its ability to do more than just display characters on the remote display.

It is this dynamic nature of mobile code that causes policy and implementation difficulties. A blanket prohibition on mobile code is secure, but that prohibition would prevent users of the dynamic Web from performing their tasks. It is this tension between integrity and dynamism that is at the heart of the issue.

The ongoing development of computer-based devices, particularly personal digital assistants (PDAs) and mobile phones, has broadened the spectrum of devices that use mobile code, and therefore are vulnerable to related exploits. The advent of the Apple iPhone in 2007 highlighted this hazard.<sup>1</sup>

Several definitions, as used by United States military forces but applicable to all, are useful in considering the content of this chapter:

**Enclave.** An information system environment that is end to end under the control of a single authority and has a uniform security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave.

# CHAPTER 18

## DENIAL-OF-SERVICE ATTACKS

Gary C. Kessler and Diane E. Levine

<b>18.1 INTRODUCTION</b>	<b>18·1</b>	<b>18.3 DISTRIBUTED DENIAL-OF-SERVICE ATTACKS</b>	<b>18·13</b>
<b>18.2 DENIAL-OF-SERVICE ATTACKS</b>	<b>18·2</b>	18.3.1 Short History of Distributed Denial of Service	18·13
18.2.1 History of Denial-of-Service Attacks	18·2	18.3.2 Distributed Denial-of-Service Terminology and Overview	18·14
18.2.2 Costs of Denial-of-Service Attacks	18·4	18.3.3 Distributed Denial-of-Service Tool Descriptions	18·16
18.2.3 Types of Denial-of-Service Attacks	18·5	18.3.4 Defenses against Distributed Denials of Service	18·22
18.2.4 Specific Denial-of-Service Attacks	18·5	<b>18.4 MANAGEMENT ISSUES</b>	<b>18·27</b>
18.2.5 Preventing and Responding to Denial-of-Service Attacks	18·12	<b>18.5 FURTHER READING</b>	<b>18·28</b>
		<b>18.6 NOTE</b>	<b>18·28</b>

**18.1 INTRODUCTION.** This chapter discusses denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. These attacks seek to render target systems and networks unusable or inaccessible by saturating resources or causing catastrophic errors that halt processes or entire systems. Furthermore, they are increasingly easy for even *script kiddies* (persons who follow explicit attack instructions or execute attack programs) to launch. Successful defense against these attacks will come only when there is widespread cooperation among all Internet service providers (ISPs) and other Internet-connected systems worldwide.

Working in a variety of ways, the DoS attacker selects an intended target system and launches a concentrated attack against it. Although initially deemed to be primarily a “nuisance,” DoS attacks can incapacitate an entire network, especially those with hosts that rely on Transmission Control Protocol/Internet Protocol (TCP/IP). DoS attacks on corporate networks and ISPs have resulted in significant damage to productivity and revenues. DoS attacks can be launched against any hardware or operating system

# CHAPTER 19

## SOCIAL ENGINEERING AND LOW-TECH ATTACKS

**Karthik Raman, Susan Baumes,  
Kevin Beets, and Carl Ness**

<b>19.1</b>	<b>INTRODUCTION</b>	<b>19·2</b>	19.5.1	Consequences	19·12	
<b>19.2</b>	<b>BACKGROUND AND HISTORY</b>	<b>19·2</b>	19.5.2	Case Study Examples from Business	19·13	
	19.2.1	Frank Abagnale	19·2	19.5.3	Success Rate	19·14
	19.2.2	Kevin Mitnick and the Media	19·3	19.5.4	Small Businesses versus Large Organizations	19·14
	19.2.3	Frequency of Use	19·3	19.5.5	Trends	19·15
	19.2.4	Social Engineering as a Portion of an Attack	19·3	<b>19.6</b>	<b>DETECTION</b>	<b>19·15</b>
<b>19.3</b>	<b>SOCIAL ENGINEERING METHODS</b>	<b>19·4</b>	19.6.1	People	19·15	
	19.3.1	Impersonation	19·4	19.6.2	Audit Controls	19·16
	19.3.2	Seduction	19·5	19.6.3	Technology for Detection	19·16
	19.3.3	Low-Tech Attacks	19·6	<b>19.7</b>	<b>RESPONSE</b>	<b>19·16</b>
	19.3.4	Network and Voice Methods	19·8	<b>19.8</b>	<b>DEFENSE AND MITIGATION</b>	<b>19·16</b>
	19.3.5	Reverse Social Engineering	19·10	19.8.1	Training and Awareness	19·17
<b>19.4</b>	<b>PSYCHOLOGY AND SOCIAL PSYCHOLOGY OF SOCIAL ENGINEERING</b>	<b>19·10</b>	19.8.2	Technology for Prevention	19·17	
	19.4.1	Psychology	19·10	19.8.3	Physical Security	19·18
	19.4.2	Social Psychology	19·11	<b>19.9</b>	<b>CONCLUSION</b>	<b>19·18</b>
	19.4.3	Social Engineer Profile	19·12	<b>19.10</b>	<b>FURTHER READING</b>	<b>19·19</b>
<b>19.5</b>	<b>DANGERS OF SOCIAL ENGINEERING AND ITS IMPACT ON BUSINESSES</b>	<b>19·12</b>	<b>19.11</b>	<b>NOTES</b>	<b>19·20</b>	



# CHAPTER 20

## SPAM, PHISHING, AND TROJANS: ATTACKS MEANT TO FOOL

Stephen Cobb

<b>20.1 UNWANTED E-MAIL AND OTHER PESTS: A SECURITY ISSUE</b>	<b>20·1</b>	20.4.5 Spam Filters	20·20
20.1.1 Common Elements	20·2	20.4.6 Network Devices	20·23
20.1.2 Chapter Organization	20·3	20.4.7 E-mail Authentication	20·24
		20.4.8 Industry Initiatives	20·25
		20.4.9 Legal Remedies	20·25
<b>20.2 E-MAIL: AN ANATOMY LESSON</b>	<b>20·3</b>	<b>20.5 PHISHING</b>	<b>20·26</b>
20.2.1 Simple Mail Transport Protocol	20·3	20.5.1 What Phish Look Like	20·26
20.2.2 Heads-Up	20·5	20.5.2 Growth and Extent of Phishing	20·28
<b>20.3 SPAM DEFINED</b>	<b>20·6</b>	20.5.3 Where Is the Threat?	20·28
20.3.1 Origins and Meaning of Spam (not SPAM™)	20·7	20.5.4 Phish Fighting	20·29
20.3.2 Digging into Spam	20·8	<b>20.6 TROJAN CODE</b>	<b>20·29</b>
20.3.3 Spam's Two-Sided Threat	20·12	20.6.1 Classic Trojans	20·30
<b>20.4 FIGHTING SPAM</b>	<b>20·17</b>	20.6.2 Basic Anti-Trojan Tactics	20·31
20.4.1 Enter the Spam Fighters	20·17	20.6.3 Lockdown and Quarantine	20·32
20.4.2 A Good Reputation?	20·17	<b>20.7 CONCLUDING REMARKS</b>	<b>20·33</b>
20.4.3 Relaying Trouble	20·19	<b>20.8 FURTHER READING</b>	<b>20·33</b>
20.4.4 Black Holes and Block Lists	20·19	<b>20.9 NOTES</b>	<b>20·34</b>

### 20.1 UNWANTED E-MAIL AND OTHER PESTS: A SECURITY ISSUE.

Three oddly named threats to computer security are addressed in this chapter: spam, phishing, and Trojan code. Spam is unsolicited commercial e-mail. Phishing is the use of deceptive unsolicited e-mail to obtain—to fish electronically for—confidential information. Trojan code, a term derived from the Trojan horse, is software designed to achieve unauthorized access to systems by posing as legitimate applications. In this

# CHAPTER 21

## WEB-BASED VULNERABILITIES

**Anup K. Ghosh, Kurt Baumgarten, Jennifer Hadley, and Steven Lovaas**

<b>21.1 INTRODUCTION</b>	<b>21·1</b>	21.6.1 Client-Side Risks	21·8
<b>21.2 BREAKING E-COMMERCE SYSTEMS</b>	<b>21·1</b>	21.6.2 Network Protocol Risks	21·10
<b>21.3 CASE STUDY OF BREAKING AN E-BUSINESS</b>	<b>21·2</b>	21.6.3 Business Application Logic	21·12
<b>21.4 WEB APPLICATION SYSTEM SECURITY</b>	<b>21·5</b>	21.6.4 CGI Script Vulnerabilities	21·14
<b>21.5 PROTECTING WEB APPLICATIONS</b>	<b>21·6</b>	21.6.5 Application Subversion	21·15
<b>21.6 COMPONENTS AND VULNERABILITIES IN E-COMMERCE SYSTEMS</b>	<b>21·8</b>	21.6.6 Web Server Exploits	21·16
		21.6.7 Database Security	21·19
		21.6.8 Platform Security	21·20
		<b>21.7 SUMMARY</b>	<b>21·21</b>
		<b>21.8 FURTHER READING</b>	<b>21·21</b>
		<b>21.9 NOTES</b>	<b>21·22</b>

**21.1 INTRODUCTION.** This chapter systematically reviews the primary software components that make up Web applications, with a primary focus on e-commerce, and provides an overview of the risks to each of these components.<sup>1</sup> The goal of this chapter is to point out that every system will have risks to its security and privacy that need to be systematically analyzed and ultimately addressed.

**21.2 BREAKING E-COMMERCE SYSTEMS.** To make a system more secure, it may be advisable to break it. Finding the vulnerabilities in a system is necessary in order to strengthen it, but breaking an e-commerce system requires a different mind-set from that of the programmers who developed it. Instead of thinking about developing within a specification, a criminal or hacker looks outside the specifications.

Hackers believe that rules exist only to be broken, and they always use a system in unexpected ways. In doing so, they usually follow the path of least resistance. Those areas perceived to provide the strongest security, or the most resistance to hacking, will likely be ignored. For example, if a system uses Secure Sockets Layer (SSL) to encrypt Web sessions between Web clients and the Web server, a hacker will not try to

# CHAPTER 22

## PHYSICAL THREATS TO THE INFORMATION INFRASTRUCTURE

Franklin Platt

<b>22.1</b>	<b>INTRODUCTION</b>	<b>22·2</b>		
<b>22.2</b>	<b>BACKGROUND AND PERSPECTIVE</b>	<b>22·2</b>		
22.2.1	Today's Risks Are Greater	22·3		
22.2.2	Likely Targets	22·4		
22.2.3	Productivity Issues	22·4		
22.2.4	Terrorism and Violence Are Now Serious Threats	22·6		
22.2.5	Costs of a Threat Happening	22·6		
22.2.6	Who Must Be Involved	22·7		
22.2.7	Liability Issues	22·8		
22.2.8	Definitions and Terms	22·8		
22.2.9	Uniform, Comprehensive Planning Process	22·9		
<b>22.3</b>	<b>THREAT ASSESSMENT PROCESS</b>	<b>22·10</b>		
22.3.1	Set Up a Steering Committee	22·11	22.3.6	Costs of Cascading Events 22·14
22.3.2	Identify All Possible Threats	22·11	22.3.7	Determine the Vulnerability to Each Threat 22·14
22.3.3	Sources of Information and Assistance	22·12	22.3.8	Completing the Threat Assessment Report 22·15
22.3.4	Determine the Likelihood of Each Threat	22·13	<b>22.4</b>	<b>GENERAL THREATS 22·15</b>
22.3.5	Approximate the Impact Costs	22·13	22.4.1	Natural Hazards 22·16
			22.4.2	Other Natural Hazards 22·17
			22.4.3	Health Threats 22·17
			22.4.4	Man-Made Threats 22·17
			22.4.5	Wiretaps 22·19
			22.4.6	High-Energy Radio-Frequency Threats 22·21
			<b>22.5</b>	<b>WORKPLACE VIOLENCE AND TERRORISM 22·22</b>
			<b>22.6</b>	<b>OTHER THREAT SITUATIONS 22·23</b>
			22.6.1	Leaks, Temperature, and Humidity 22·23
			22.6.2	Off-Hour Visitors 22·23
			22.6.3	Cleaning and Maintenance Threats 22·24
			22.6.4	Storage-Room Threats 22·24
			22.6.5	Medical Emergencies 22·25
			22.6.6	Illicit Workstation 22·25

## INTRODUCTION TO PART III

# PREVENTION: TECHNICAL DEFENSES

The threats and vulnerabilities described in Part II can be met in part by effective use of technical countermeasures.

The chapter titles and topics in this part include:

- 23. Protecting the Information Infrastructure.** Facilities security and emergency management
- 24. Operating System Security.** Fundamentals of operating-systems security, including security kernels, privilege levels, access control lists, and memory partitions
- 25. Local Area Networks.** Security for local area networks, including principles and platform-specific tools
- 26. Gateway Security Devices.** Effective recommendations for implementing firewalls and proxy servers
- 27. Intrusion Detection and Intrusion Prevention Devices.** Critical elements of security management for measuring attack frequencies outside and inside the perimeter and for reducing successful penetrations
- 28. Identification and Authentication.** What one knows, what one has, what one is, and what one does
- 29. Biometric Authentication.** Special focus on who one is and what one does as markers of identity
- 30. E-Commerce and Web Server Safeguards.** Technological and legal measures underlying secure e-commerce and a systematic approach to developing and implementing security services
- 31. Web Monitoring and Content Filtering.** Tools for security management within the perimeter
- 32. Virtual Private Networks and Secure Remote Access.** Encrypted channels (virtual private networks) for secure communication, and approaches for safe remote access
- 33. 802.11 Wireless LAN Security.** Protecting increasingly pervasive wireless networks

### III · 2 PREVENTION: TECHNICAL DEFENSES

34. **Securing VoIP.** Security measures for Voice over IP telephony
35. **Securing P2P, IM, SMS, and Collaboration Tools.** Securing collaboration tools such as peer-to-peer networks, instant messaging, text messaging services, and other mechanisms to reduce physical travel, and to facilitate communications
36. **Securing Stored Data.** Managing encryption and efficient storage of stored data
37. **PKI and Certificate Authorities.** Concepts, terminology, and applications of the Public Key Infrastructure for asymmetric encryption
38. **Writing Secure Code.** Guidelines for writing robust program code that includes few bugs, and that can successfully resist deliberate attacks
39. **Software Development and Quality Assurance.** Using quality assurance and testing to underpin security in the development phase of programs
40. **Managing Software Patches and Vulnerabilities.** Rational deployment of software patches
41. **Antivirus Technology.** Methods for fighting malicious code
42. **Protecting Digital Rights: Technical Approaches.** Methods for safeguarding intellectual property such as programs, music, and video that must by its nature be shared to be useful

# CHAPTER 23

## PROTECTING THE INFORMATION INFRASTRUCTURE

Franklin Platt

<b>23.1</b>	<b>INTRODUCTION</b>	<b>23·2</b>			
<b>23.2</b>	<b>SECURITY PLANNING AND MANAGEMENT</b>	<b>23·3</b>			
23.2.1	National Incident Management System Compliance	23·3	23.4.1	Segmented Secrets	23·11
23.2.2	National Response Plan	23·4	23.4.2	Confidential Design Details	23·12
23.2.3	National Infrastructure Protection Plan	23·5	23.4.3	Difficulties in Protecting the Infrastructure	23·13
23.2.4	Other Presidential Directives	23·6	23.4.4	Appearance of Good Security	23·13
23.2.5	Security-Related Laws and Regulations	23·6	23.4.5	Proper Labeling	23·14
23.2.6	Some Other Regulatory Requirements	23·6	23.4.6	Reliability and Redundancy	23·14
23.2.7	Security Auditing Standards	23·7	23.4.7	Proper Installation and Maintenance	23·15
<b>23.3</b>	<b>STRATEGIC PLANNING PROCESS</b>	<b>23·7</b>	<b>23.5</b>	<b>OTHER CONSIDERATIONS</b>	<b>23·16</b>
23.3.1	Attractive Targets	23·8	23.5.1	Threats from Smoke and Fire	23·16
23.3.2	Defensive Strategies	23·8	23.5.2	Equipment Cabinets	23·17
23.3.3	Who Is Responsible?	23·9	23.5.3	Good Housekeeping Practices	23·18
23.3.4	One Process, One Language	23·9	23.5.4	Overt, Covert, and Deceptive Protections	23·18
23.3.5	Federal Guidelines	23·10	<b>23.6</b>	<b>ACCESS CONTROL</b>	<b>23·19</b>
<b>23.4</b>	<b>ELEMENTS OF GOOD PROTECTION</b>	<b>23·11</b>	23.6.1	Locks and Hardware	23·20
			23.6.2	Card Entry Systems	23·21
			23.6.3	Proximity and Touch Cards	23·22
			23.6.4	Authentication	23·23
			23.6.5	Integrated Card Access Systems	23·25
			23.6.6	Portal Machines	23·25

## 23.2 PROTECTING THE INFORMATION INFRASTRUCTURE

23.6.7	Bypass Key	23.26	23.9.2	Remote Spying Devices	23.49
23.6.8	Intrusion Alarms	23.26	23.9.3	Bombs, Threats, Violence, and Attacks	23.49
23.6.9	Other Important Alarms	23.27	23.9.4	Medical Emergencies	23.50
<b>23.7</b>	<b>SURVEILLANCE SYSTEMS</b>	<b>23.28</b>	<b>23.10</b>	<b>INFORMATION NOT PUBLICLY AVAILABLE</b>	<b>23.51</b>
23.7.1	Surveillance Cameras	23.28	<b>23.11</b>	<b>COMPLETING THE SECURITY PLANNING PROCESS</b>	<b>23.52</b>
23.7.2	Camera Locations and Mounts	23.29	23.11.1	All-Hazard Mitigation Plan	23.52
23.7.3	Recording Systems	23.30	23.11.2	Cost-Benefit Analysis	23.53
23.7.4	Camera Control Systems	23.30	23.11.3	Security Response Plan	23.53
23.7.5	Broadband Connections	23.30	23.11.4	Implementation, Accountability, and Follow-Up	23.54
<b>23.8</b>	<b>OTHER DESIGN CONSIDERATIONS</b>	<b>23.31</b>	<b>23.12</b>	<b>SUMMARY AND CONCLUSIONS</b>	<b>23.55</b>
23.8.1	Choosing Safe Sites	23.31	23.12.1	Federal Guidelines and Instructions Are Still Deficient	23.55
23.8.2	Physical Access	23.32	23.12.2	Good Risk Management Is the Answer	23.56
23.8.3	Protective Construction	23.33	<b>23.13</b>	<b>FURTHER READING</b>	<b>23.56</b>
23.8.4	Using Existing Premises Alarms	23.35	<b>23.14</b>	<b>NOTES</b>	<b>23.56</b>
23.8.5	Clean Electrical Power	23.36			
23.8.6	Emergency Power	23.38			
23.8.7	Environmental Control	23.44			
23.8.8	Smoke and Fire Protection	23.46			
<b>23.9</b>	<b>MITIGATING SPECIFIC THREATS</b>	<b>23.48</b>			
23.9.1	Preventing Wiretaps and Bugs	23.48			

**23.1 INTRODUCTION.** There are three steps necessary to protect the information infrastructure properly. The first step is to establish uniform and comprehensive policies and procedures for security planning, implementation, and management. The second step is to review the facilities design factors and security defenses needed to protect the information infrastructure as well as the people who use it. The third step is a cost-benefit analysis to determine which of the security defenses derived from steps 1 and 2 will be the most cost effective. Once all possible threat situations have been identified and assessed as described in Chapter 22, this chapter covers the remaining steps necessary to implement good security protection.

A uniform and comprehensive process for good security planning and management is no longer optional or accidental. Today, anything less than good security is likely to cost any organization dearly. And even more important today is that good security now requires compliance with many new federal laws, regulations, and directives, if only to ensure good risk management and to circumvent unnecessary and potentially costly allegations of negligence. Once insurance was enough to cover most threat situations.

# CHAPTER 24

## OPERATING SYSTEM SECURITY

William Stallings

<b>24.1 INFORMATION PROTECTION AND SECURITY</b>	<b>24·1</b>	<b>24.4 FILE SHARING</b>	<b>24·10</b>
		24.4.1 Access Rights	24·10
		24.4.2 Simultaneous Access	24·11
<b>24.2 REQUIREMENTS FOR OPERATING SYSTEM SECURITY</b>	<b>24·2</b>	<b>24.5 TRUSTED SYSTEMS</b>	<b>24·11</b>
24.2.1 Requirements	24·2	24.5.1 Trojan Horse Defense	24·13
24.2.2 Computer System Assets	24·3		
24.2.3 Design Principles	24·4	<b>24.6 WINDOWS 2000 SECURITY</b>	<b>24·14</b>
<b>24.3 PROTECTION MECHANISMS</b>	<b>24·4</b>	24.6.1 Access-Control Scheme	24·14
24.3.1 Protection of Memory	24·5	24.6.2 Access Token	24·15
24.3.2 User-Oriented Access Control	24·6	24.6.3 Security Descriptors	24·16
24.3.3 Data-Oriented Access Control	24·7	<b>24.7 FURTHER READING</b>	<b>24·19</b>
24.3.4 Protection Based on an Operating System Mode	24·9	<b>24.8 NOTES</b>	<b>24·19</b>

**24.1 INFORMATION PROTECTION AND SECURITY.** This chapter reviews the principles of security in operating systems. Some general-purpose tools can be built into computers and operating systems (OSs) that support a variety of protection and security mechanisms. In general, the concern is with the problem of controlling access to computer systems and the information stored in them. Four types of overall protection policies, of increasing order of difficulty, have been identified:

- 1. No sharing.** In this case, processes are completely isolated from each other, and each process has exclusive control over the resources statically or dynamically assigned to it. With this policy, processes often “share” a program or data file by making a copy of it and transferring the copy into their own virtual memory.
- 2. Sharing originals of program or data files.** With the use of reentrant code, a single physical realization of a program can appear in multiple virtual address spaces, as can read-only data files. Special locking mechanisms are required for



# CHAPTER 25

## LOCAL AREA NETWORKS

Gary C. Kessler and N. Todd Pritsky

<b>25.1 INTRODUCTION</b>	<b>25 · 1</b>	25.4.4 Wireless LAN Issues	25 · 6
<b>25.2 POLICY AND PROCEDURE ISSUES</b>	<b>25 · 1</b>	<b>25.5 NETWORK OPERATING SYSTEM ISSUES</b>	<b>25 · 8</b>
<b>25.3 PHYSICAL SITE SECURITY</b>	<b>25 · 3</b>	25.5.1 Windows 9x	25 · 9
<b>25.4 PHYSICAL LAYER ISSUES</b>	<b>25 · 3</b>	25.5.2 NT/2000, XP Vista	25 · 10
25.4.1 Sniffers and Broadcast LANs	25 · 3	25.5.3 UNIX	25 · 13
25.4.2 Attacks on the Physical Plant	25 · 4	25.5.4 MacOS	25 · 14
25.4.3 Modems, Dial-up Servers, and Telephone Lines	25 · 5	<b>25.6 CONCLUSION</b>	<b>25 · 15</b>
		<b>25.7 FURTHER READING</b>	<b>25 · 16</b>
		<b>25.8 NOTES</b>	<b>25 · 17</b>

**25.1 INTRODUCTION.** This chapter discusses generic issues surrounding local area network (LAN) security. Securing the LAN is essential to securing the Internet because LANs are where most of the attackers, victims, clients, servers, firewalls, routers, and other devices reside. Compromised LAN systems on the Internet open other nodes on that local network to attack and put other systems at risk on the Internet as a whole. Many of the general issues mentioned herein are described in more specific terms in other chapters of this *Handbook*, such as Chapters 15, 22, 23, and 47 in particular.

**25.2 POLICY AND PROCEDURE ISSUES.** Twenty years ago, all users had accounts on a shared mainframe or minicomputer. A single system manager was responsible for security, backup, disaster recovery, account management, policies, and all other related issues. Today all users are system managers, and, in many cases, individuals have responsibility for several systems. Since the vulnerability of a single computer can compromise the entire LAN, it is imperative that there be rules in place so that everyone can work together for mutual efficiency and defense. But where policies and procedures can be centralized, they should be, because most users do not take the security procedures seriously enough.

The next list, modified from the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2196, is a rough outline of LAN-related security policies and procedures that should at least be considered.<sup>1</sup>

# CHAPTER 26

## GATEWAY SECURITY DEVICES

David Brussin and Justin Opatrny

<b>26.1 INTRODUCTION</b>	<b>26·1</b>	26.4.2 Gateway Protection Device Positioning	26·18
26.1.1 Changing Security Landscape	26·2	26.4.3 Management and Monitoring Strategies	26·19
26.1.2 Rise of the Gateway Security Device	26·3		
26.1.3 Application Firewall: Beyond the Proxy	26·4	<b>26.5 NETWORK SECURITY DEVICE EVALUATION</b>	<b>26·23</b>
<b>26.2 HISTORY AND BACKGROUND</b>	<b>26·4</b>	26.5.1 Current Infrastructure Limitations	26·24
26.2.1 Changing Network Models	26·4	26.5.2 New Infrastructure Requirements	26·24
26.2.2 Firewall Architectures	26·5	26.5.3 Performance	26·24
26.2.3 Firewall Platforms	26·8	26.5.4 Management	26·25
<b>26.3 NETWORK SECURITY MECHANISMS</b>	<b>26·10</b>	26.5.5 Usability	26·28
26.3.1 Basic Roles	26·10	26.5.6 Price	26·29
26.3.2 Personal and Desktop Agents	26·13	26.5.7 Vendor Considerations	26·30
26.3.3 Additional Roles	26·14	26.5.8 Managed Security Service Providers	26·32
<b>26.4 DEPLOYMENT</b>	<b>26·17</b>	<b>26.6 CONCLUDING REMARKS</b>	<b>26·32</b>
26.4.1 Screened Subnet Firewall Architectures	26·17	<b>26.7 FURTHER READING</b>	<b>26·33</b>

**26.1 INTRODUCTION.** The firewall has come to represent both the concept and the realization of network and Internet security protections. Due to its rapid acceptance and evolution, the firewall has become the most visible of security technology throughout the enterprise chain of command. In distinct contrast with virtually any other single piece of technology, there is not likely to be a chief executive officer in this country who cannot say a word or two about how firewalls are used to protect enterprise systems and data.

The firewall, as originally devised, was intended to allow certain explicitly authorized communications between networks while denying all others. This approach centralizes much of the responsibility for the security of a protected network at the firewall component while distributing some responsibility to the components handling the authorized communications with outside networks. The centralized responsibility

# CHAPTER 27

## INTRUSION DETECTION AND INTRUSION PREVENTION DEVICES

Rebecca Gurley Bace

<b>27.1</b>	<b>SECURITY BEHIND THE FIREWALL</b>	<b>27·2</b>	27.4.5 Issues in Information Sources	27·7
27.1.1	What Is Intrusion Detection?	27·2	<b>27.5 ANALYSIS SCHEMES</b>	<b>27·8</b>
27.1.2	What Is Intrusion Prevention?	27·2	27.5.1 Misuse Detection	27·8
27.1.3	Where Do Intrusion Detection and Intrusion Prevention Fit in Security Management?	27·3	27.5.2 Anomaly Detection	27·8
27.1.4	Brief History of Intrusion Detection	27·4	27.5.3 Hybrid Approaches	27·9
<b>27.2</b>	<b>MAIN CONCEPTS</b>	<b>27·4</b>	27.5.4 Issues in Analysis	27·10
27.2.1	Process Structure	27·4	<b>27.6 RESPONSE</b>	<b>27·10</b>
27.2.2	Monitoring Approach	27·5	27.6.1 Passive Responses	27·10
27.2.3	Intrusion Detection Architecture	27·5	27.6.2 Active Responses: Man-in-the-Loop and Autonomous	27·11
27.2.4	Monitoring Frequency	27·5	27.6.3 Automated Response Goals	27·11
27.2.5	Analysis Strategy	27·6	27.6.4 Investigative Support	27·12
<b>27.3</b>	<b>INTRUSION PREVENTION</b>	<b>27·6</b>	27.6.5 Issues in Responses	27·12
27.3.1	Intrusion Prevention System Architecture	27·6	<b>27.7 NEEDS ASSESSMENT AND PRODUCT SELECTION</b>	<b>27·13</b>
27.3.2	Intrusion Prevention Analysis Strategy	27·6	27.7.1 Matching Needs to Features	27·13
<b>27.4</b>	<b>INFORMATION SOURCES</b>	<b>27·6</b>	27.7.2 Specific Scenarios	27·13
27.4.1	Network Monitoring	27·7	27.7.3 Integrating IDS Products with Your Security Infrastructure	27·14
27.4.2	Operating System Monitoring	27·7	27.7.4 Deployment of IDS Products	27·14
27.4.3	Application Monitoring	27·7	<b>27.8 CONCLUSION</b>	<b>27·16</b>
27.4.4	Other Types of Monitoring	27·7	<b>27.9 FURTHER READING</b>	<b>27·16</b>
			<b>27.10 NOTES</b>	<b>27·17</b>

# CHAPTER 28

## IDENTIFICATION AND AUTHENTICATION

**Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs**

<b>28.1</b>	<b>INTRODUCTION</b>	<b>28·1</b>	28.3.9	Risk of Password Reuse	28·12
<b>28.2</b>	<b>FOUR PRINCIPLES OF AUTHENTICATION</b>	<b>28·2</b>	28.3.10	Authentication Using Recognition of Symbols	28·12
28.2.1	What Only You Know	28·3	<b>28.4</b>	<b>TOKEN-BASED AUTHENTICATION</b>	<b>28·13</b>
28.2.2	What Only You Have	28·3	28.4.1	One-Time Password Generators	28·13
28.2.3	What Only You Are	28·4	28.4.2	Smart Cards and Dongles	28·14
28.2.4	What Only You Do	28·4	28.4.3	Soft Tokens	28·14
<b>28.3</b>	<b>PASSWORD-BASED AUTHENTICATION</b>	<b>28·5</b>	<b>28.5</b>	<b>BIOMETRIC AUTHENTICATION</b>	<b>28·15</b>
28.3.1	Access to User Passwords by System Administrators	28·5	<b>28.6</b>	<b>CROSS-DOMAIN AUTHENTICATION</b>	<b>28·15</b>
28.3.2	Risk of Undetected Theft	28·5	<b>28.7</b>	<b>RELATIVE COSTS OF AUTHENTICATION TECHNOLOGIES</b>	<b>28·16</b>
28.3.3	Risk of Undetected Sharing	28·6	<b>28.8</b>	<b>CONCLUDING REMARKS</b>	<b>28·16</b>
28.3.4	Risk of Weakest Link	28·7	<b>28.9</b>	<b>SUMMARY</b>	<b>28·17</b>
28.3.5	Risk of Online Guessing	28·8	<b>28.10</b>	<b>FURTHER READING</b>	<b>28·17</b>
28.3.6	Risk of Off-Line Dictionary Attacks	28·9	<b>28.11</b>	<b>NOTES</b>	<b>28·18</b>
28.3.7	Risk of Password Replay	28·9			
28.3.8	Risk of Server Spoofing	28·11			

**28.1 INTRODUCTION.** *Authorization* is the allocation of permissions for specific types of access to restricted information. In the real world, authorization is conferred on real human beings; in contrast, information technology normally

# CHAPTER 29

## BIOMETRIC AUTHENTICATION

**David R. Lease, Robert Guess,  
Steven Lovaas, and Eric Salveggio**

<b>29.1 INTRODUCTION</b>	<b>29·2</b>	<b>29.6 DISADVANTAGES AND PROBLEMS</b>	<b>29·16</b>
<b>29.2 IMPORTANCE OF IDENTIFICATION AND VERIFICATION</b>	<b>29·2</b>	29.6.1 General Considerations	29·16
<b>29.3 FUNDAMENTALS AND APPLICATIONS</b>	<b>29·2</b>	29.6.2 Health and Disability Considerations	29·17
29.3.1 Overview and History	29·2	29.6.3 Environmental and Cultural Considerations	29·18
29.3.2 Properties of Biometrics	29·4	29.6.4 Cost Considerations	29·18
29.3.3 Identification, Authentication, and Verification	29·5	29.6.5 Attacks on Biometric Systems	29·18
29.3.4 Application Areas	29·6	29.6.6 Privacy Concerns	29·19
29.3.5 Data Acquisition and Presentation	29·8	<b>29.7 RECENT TRENDS IN BIOMETRIC AUTHENTICATION</b>	<b>29·21</b>
<b>29.4 TYPES OF BIOMETRIC TECHNOLOGIES</b>	<b>29·8</b>	29.7.1 Government Advances in Biometric Authentication	29·21
29.4.1 Finger Scan	29·8	29.7.2 Face Scanning at Airports and Casinos	29·21
29.4.2 Facial Scan/Recognition	29·10	29.7.3 Increased Deployment in the Financial Industry	29·22
29.4.3 Hand Geometry Scan	29·12	29.7.4 Biometrics in the Healthcare Industry	29·22
29.4.4 Iris Scan	29·13	29.7.5 Increased Deployment of Time and Attendance Systems	29·22
29.4.5 Voice Recognition	29·14	<b>29.8 SUMMARY AND RECOMMENDATIONS</b>	<b>29·24</b>
29.4.6 Other Biometric Technologies	29·15	<b>29.9 FURTHER READING</b>	<b>29·25</b>
<b>29.5 TYPES OF ERRORS AND SYSTEM METRICS</b>	<b>29·15</b>	<b>29.10 NOTES</b>	<b>29·25</b>
29.5.1 False Accept	29·15		
29.5.2 False Reject	29·15		
29.5.3 Crossover Error Rate	29·15		
29.5.4 Failure to Enroll	29·16		

# CHAPTER 30

## E-COMMERCE AND WEB SERVER SAFEGUARDS

Robert Gezelter

<b>30.1 INTRODUCTION</b>	<b>30·2</b>	30.3.10 Hold Harmless	30·21
<b>30.2 BUSINESS POLICIES AND STRATEGIES</b>	<b>30·3</b>	<b>30.4 RISK ANALYSIS</b>	<b>30·22</b>
30.2.1 Step 1: Define Information Security Concerns Specific to the Application	30·3	30.4.1 Business Loss	30·22
30.2.2 Step 2: Develop Security Service Options	30·5	30.4.2 PR Image	30·22
30.2.3 Step 3: Select Security Service Options Based on Requirements	30·7	30.4.3 Loss of Customers/Business Interruptions	30·23
30.2.4 Step 4: Ensures the Ongoing Attention to Changes in Technologies and Requirements	30·9	30.4.4 Interruptions	30·23
30.2.5 Using the Security Services Framework	30·9	30.4.5 Proactive versus Reactive Threats	30·24
30.2.6 Framework Conclusion	30·17	30.4.6 Threat and Hazard Assessment	30·24
<b>30.3 RULES OF ENGAGEMENT</b>	<b>30·17</b>	<b>30.5 OPERATIONAL REQUIREMENTS</b>	<b>30·24</b>
30.3.1 Web Site–Specific Measures	30·17	30.5.1 Ubiquitous Internet Protocol Networking	30·25
30.3.2 Defining Attacks	30·18	30.5.2 Internal Partitions	30·25
30.3.3 Defining Protection	30·19	30.5.3 Critical Availability	30·26
30.3.4 Maintaining Privacy	30·19	30.5.4 Accessibility	30·26
30.3.5 Working with Law Enforcement	30·19	30.5.5 Applications Design	30·26
30.3.6 Accepting Losses	30·20	30.5.6 Provisioning	30·27
30.3.7 Avoiding Overreaction	30·20	30.5.7 Restrictions	30·27
30.3.8 Appropriate Responses to Attacks	30·20	30.5.8 Multiple Security Domains	30·28
30.3.9 Counter-Battery	30·21	30.5.9 What Needs to Be Exposed?	30·28
		30.5.10 Access Controls	30·29
		30.5.11 Site Maintenance	30·29
		30.5.12 Maintaining Site Integrity	30·29
		<b>30.6 TECHNICAL ISSUES</b>	<b>30·30</b>
		30.6.1 Inside/Outside	30·30
		30.6.2 Hidden Subnets	30·31
		30.6.3 What Need Be Exposed?	30·31

## 30 · 2 E-COMMERCE AND WEB SERVER SAFEGUARDS

30.6.4	Multiple Security Domains	30·32	30.7.1	Liabilities	30·38
30.6.5	Compartmentalization	30·34	30.7.2	Customer Monitoring, Privacy, and Disclosure	30·39
30.6.6	Need to Access	30·35	30.7.3	Litigation	30·40
30.6.7	Accountability	30·36	30.7.4	Application Service Providers	30·41
30.6.8	Read-Only File Security	30·36			
30.6.9	Going Off-Line	30·37			
30.6.10	Auditing	30·37	<b>30.8</b>	<b>SUMMARY</b>	<b>30·42</b>
30.6.11	Emerging Technologies	30·38	<b>30.9</b>	<b>FURTHER READING</b>	<b>30·42</b>
			<b>30.7</b>	<b>ETHICAL AND LEGAL ISSUES</b>	<b>30·38</b>
			<b>30.10</b>	<b>NOTES</b>	<b>30·45</b>

**30.1 INTRODUCTION.** Today, electronic commerce involves the entire enterprise. While the most obvious e-commerce applications involve business transactions with outside customers on the World Wide Web (WWW or Web), they are merely the proverbial tip of the iceberg. The presence of e-commerce has become far more pervasive, often involving the entire logistical and financial supply chains that are the foundations of modern commerce. Even the smallest organizations now rely on the Web for access to services and information.

The pervasive desire to improve efficiency often causes a convergence between the systems supporting conventional operations with those supporting the organization's online business. It is thus common for internal systems at bricks-and-mortar stores to utilize the same back-office systems as are used by Web customers. It is also common for kiosks and cash registers to use wireless networks to establish connections back to internal systems. These interconnections have the potential to provide intruders with access directly into the heart of the enterprise.

The TJX case, which came to public attention in the beginning of 2007, was one of a series of large-scale compromises of electronically stored information on back-office and e-commerce systems. Most notably, the TJX case appears to have started with an insufficiently secured corporate network and the associated back-office systems, not a Web site penetration. This breach escalated into a security breach of corporate data systems. It has been reported that at least 94 million credit cards were compromised.<sup>1</sup> On November 30, 2007, it was reported that TJX, the parent organization of stores including TJ Maxx and Marshall's, agreed to settle bank claims related to VISA cards for US\$ 40.9M.<sup>2</sup>

E-commerce has now come of age, giving rise to fiduciary risks that are important to senior management and to the board of directors. The security of data networks, both those used by customers and those used internally, now has reached the level where it significantly affects the bottom line. TJX has suffered both monetarily and in public relations, with stories concerning the details of this case appearing in the *Wall Street Journal*, the *New York Times*, *Business Week*, and many industry trade publications. Data security is no longer an abstract issue of concern only to technology personnel. The legal settlements are far in excess of the costs directly associated with curing the technical problem.

Protecting e-commerce information requires a multifaceted approach, involving business policies and strategies as well as the technical issues more familiar to information security professionals.

Throughout the enterprise, people and information are physically safeguarded. Even the smallest organizations have a locked door and a receptionist to keep outsiders from entering the premises. The larger the organization, the more elaborate

# CHAPTER 31

## WEB MONITORING AND CONTENT FILTERING

Steven Lovaas

<b>31.1</b>	<b>INTRODUCTION</b>	<b>31·1</b>	31.5.2 Third-Party Block Lists	31·8
<b>31.2</b>	<b>SOME TERMINOLOGY</b>	<b>31·2</b>	<b>31.6 ENFORCEMENT</b>	<b>31·8</b>
<b>31.3</b>	<b>MOTIVATION</b>	<b>31·2</b>	31.6.1 Proxies	31·8
	31.3.1 Prevention of Dissent	31·3	31.6.2 Firewalls	31·8
	31.3.2 Protection of Children	31·3	31.6.3 Parental Tools	31·9
	31.3.3 Supporting Organizational Human Resources Policy	31·3	<b>31.7 VULNERABILITIES</b>	<b>31·9</b>
	31.3.4 Enforcement of Laws	31·4	31.7.1 Spoofing	31·10
<b>31.4</b>	<b>GENERAL TECHNIQUES</b>	<b>31·4</b>	31.7.2 Tunneling	31·10
	31.4.1 Matching the Request	31·4	31.7.3 Encryption	31·11
	31.4.2 Matching the Host	31·5	31.7.4 Anonymity	31·11
	31.4.3 Matching the Domain	31·6	31.7.5 Translation Sites	31·11
	31.4.4 Matching the Content	31·6	31.7.6 Caching Services	31·12
<b>31.5</b>	<b>IMPLEMENTATION</b>	<b>31·7</b>	<b>31.8 THE FUTURE</b>	<b>31·12</b>
	31.5.1 Manual “Bad URL” Lists	31·7	<b>31.9 SUMMARY</b>	<b>31·13</b>
			<b>31.10 FURTHER READING</b>	<b>31·13</b>
			<b>31.11 NOTES</b>	<b>31·13</b>

**31.1 INTRODUCTION.** The Internet has been called a cesspool, sometimes in reference to the number of virus-infected and hacker-controlled machines, but more often in reference to the amount of objectionable content available at a click of the mouse. This chapter deals with efforts to monitor and control access to some of this content. Applications that perform this kind of activity are controversial: Privacy and free-speech advocates regularly refer to “censorware,” while the writers of such software tend to use the term “content filtering.” This chapter uses “content filtering,” without meaning to take a side in the argument by so doing. For more on the policy and legal issues surrounding Web monitoring and content filtering, see Chapters 48 and 72 in this *Handbook*.

This chapter briefly discusses the possible motivations leading to the decision to filter content, without debating the legitimacy of these motives. Given the variety of



# VIRTUAL PRIVATE NETWORKS AND SECURE REMOTE ACCESS

**Justin Opatrny**

<b>32.1 INTRODUCTION</b>	<b>32·1</b>	32.3.1 Multiprotocol Layer Switching	32·6
32.1.1 Borders Dissolving	32·1	32.3.2 Site-to-Site VPNs	32·6
32.1.2 Secure Remote Access	32·2	32.3.3 Information Assurance Considerations	32·7
32.1.3 Virtual Private Networks	32·2		
32.1.4 VPN Technology Concepts	32·3		
<b>32.2 SECURE CLIENT VPNS</b>	<b>32·3</b>	<b>32.4 EXTRANETS</b>	<b>32·11</b>
32.2.1 IPSec	32·4	32.4.1 Information Assurance Goals	32·11
32.2.2 Transport Layer Security	32·4	32.4.2 Extranet Concepts	32·12
32.2.3 User Authentication Methods	32·5	32.4.3 Types of Extranet Access	32·12
32.2.4 Infrastructure Requirements	32·5	32.4.4 Information Assurance Considerations	32·13
32.2.5 Network Access Requirements	32·5	<b>32.5 CONCLUSION</b>	<b>32·15</b>
<b>32.3 TRUSTED VPNS</b>	<b>32·6</b>	<b>32.6 FURTHER READING</b>	<b>32·15</b>

**32.1 INTRODUCTION.** The rise of the Internet created a new chapter in human civilization. People are no longer tied to static information sources such as libraries. The seemingly exponential growth of people looking to access wide varieties of content also spurred the desire for mobility. If a person can search for information residing halfway around the world from home, why not be able to do the same from the local coffee shop or while sitting at an airport during a business trip? This information revolution offered an opportunity to provide information and services to consumers, businesses, and employees at virtually any point on the globe.

**32.1.1 Borders Dissolving.** Prolific Internet access redefined the dynamics of network and perimeter protections. Previously, companies needed to focus on protecting the internal network as well as systems exposed to the Internet. A perimeter firewall was sufficient to keep the digital predators at bay. The greater challenge then became how to maintain the security of the internal network when employees use mobile technologies from home or while traveling. Further complicating the issue is how to allow other business partners to access the systems and information that require protection.

# CHAPTER 33

## 802.11 WIRELESS LAN SECURITY

Gary L. Tagg

<b>33.1 INTRODUCTION</b>	<b>33·2</b>	33.4.3 Defending against the WEP Vulnerability	33·20
33.1.1 Scope	33·3		
33.1.2 Background and Uses of Wireless LANs	33·3		
<b>33.2 802.11 ARCHITECTURE AND PRODUCT TYPES</b>	<b>33·4</b>	<b>33.5 IEEE 802.11I</b>	<b>33·25</b>
33.2.1 802.11 Components	33·4	33.5.1 Structure of the Robust Security Network	33·25
33.2.2 802.11 Network Architecture	33·6	33.5.2 802.1X Authentication	33·26
33.2.3 802.11 Physical Layer	33·6	33.5.3 Security Association Management	33·27
33.2.4 Wireless LAN Product Types	33·7	33.5.4 RSNA Key Hierarchy and Management	33·30
33.2.5 Benefits of Wireless Switch/Access Controller Architecture	33·8	33.5.5 Temporal Key Integrity Protocol	33·32
33.2.6 Security Benefits of Wireless Switch/Access Controller Architecture	33·9	33.5.6 Counter Mode/CBC-MAC Protocol (CCMP)	33·33
		33.5.7 Remaining Implementation Issues	33·34
		33.5.8 Wi-Fi Alliance's WPA and WPA2 Standards	33·35
<b>33.3 WIRELESS LAN SECURITY THREATS</b>	<b>33·9</b>		
33.3.1 Comparison between Wired and Wireless	33·10	<b>33.6 802.11 SECURITY AUDITING TOOLS</b>	<b>33·36</b>
33.3.2 Specific Threats Enabled by Wireless LANs	33·10	33.6.1 Auditor and BackTrack	33·36
		33.6.2 Kismet	33·36
		33.6.3 Netstumbler	33·36
		33.6.4 Aircrack	33·38
		33.6.5 CoWPAtty and Aircrack	33·38
		33.6.6 Ethereal	33·38
		33.6.7 Wellenreiter	33·38
		33.6.8 Commercial Wireless Auditing Tools	33·39
<b>33.4 ORIGINAL 802.11 SECURITY FUNCTIONALITY</b>	<b>33·14</b>		
33.4.1 Security Functionality Overview	33·14		
33.4.2 Connecting to a Wireless Network and Authentication	33·14		

## 33·2 802.11 WIRELESS LAN SECURITY

<b>33.7 CONCLUSION</b>	<b>33·39</b>		
<b>33.8 APPENDIX 33A—802.11 STANDARDS</b>	<b>33·40</b>		
33.8.1 802.11 and 802.11b: MAC and Physical Layer Specifications	33·40	33.8.14 802.11r: Fast Roaming/Fast BSS Transition	33·42
33.8.2 802.11a: 5GHz High-Speed Physical Layer	33·40	33.8.15 802.11s: ESS Mesh Networking	33·42
33.8.3 802.11d: 802.11 Additional Regulatory Domains	33·41	33.8.16 802.11T: Wireless Performance Prediction (WPP)	33·42
33.8.4 802.11e: MAC Enhancements for Quality of Service	33·41	33.8.17 802.11u: Interworking with External Networks	33·42
33.8.5 802.11F: Inter-Access Point Protocol	33·41	33.8.18 802.11v: Wireless Network Management	33·43
33.8.6 802.11g: Higher-Rate Extension to 802.11b	33·41	33.8.19 802.11w: Protected Management Frames	33·43
33.8.7 802.11h: Spectrum Managed 802.11a	33·41	33.8.20 802.11y: 3650–3700MHz Operation in the United States	33·43
33.8.8 802.11i: MAC Security Enhancements	33·41	33.8.21 802.1x: Port-Based Network Access Control	33·43
33.8.9 802.11j: 4.9GHz–5GHz Operation in Japan	33·41	33.8.22 Wi-Fi Protected Access (WPA) and WPA2	33·43
33.8.10 802.11k: Radio Resource Measurement Enhancements	33·41		
33.8.11 802.11m: Maintenance	33·42	<b>33.9 APPENDIX 33B: ABBREVIATIONS, TERMINOLOGY, AND DEFINITIONS</b>	<b>33·43</b>
33.8.12 802.11n: Enhancements for Higher Throughput	33·42	<b>33.10 FURTHER READING</b>	<b>33·47</b>
33.8.13 802.11p: Wireless Access for the		<b>33.11 NOTES</b>	<b>33·48</b>

**33.1 INTRODUCTION.** Corporations and home users have mass adopted IEEE 802.11 as the protocol for wireless local area networks. These networks have benefits over traditional wired networks, such as mobility, flexibility, rapid deployment, and cost reduction. However, as with any networking technology, it creates new opportunities for unauthorized individuals to access the networks and the information carried over them.

The purpose of this chapter is to introduce wireless LAN technologies, the issues, and ways to address them. Reasons driving the adoption of wireless LANs derive from:

- The 802.11 architecture and product types
- The threats to information presented by wireless LAN technology, and how they compare to other networking threats, such as the Internet
- The security functionality provided by the original 802.11 standard, the security weaknesses, and how to mitigate them
- The security functionality provided by the 802.11i security standard, which was developed to address issues with the original standards

# CHAPTER 34

## SECURING VOIP

Christopher Dantos and John Mason

<b>34.1 INTRODUCTION</b>	<b>34·1</b>		
<b>34.2 REGULATORY COMPLIANCE AND RISK ANALYSIS</b>	<b>34·2</b>		
34.2.1 Key Federal Laws and Regulations	34·2	34.4.2 Application Layer Gateways and Firewalls	34·11
34.2.2 Other U.S. Federal Regulations and Laws	34·3	34.4.3 Logical Separation of Voice and Data	34·11
34.2.3 State Laws and Regulations	34·5	34.4.4 Quality of Service	34·12
34.2.4 International Laws and Considerations	34·5	34.4.5 Network Monitoring Tools	34·12
34.2.5 Liability	34·5	34.4.6 Device Authentication	34·12
34.2.6 Risk Analysis	34·6	34.4.7 User Authentication	34·12
		34.4.8 Network Address Translation and NAT-Traversal	34·12
<b>34.3 TECHNICAL ASPECTS OF VOIP SECURITY</b>	<b>34·8</b>	<b>34.5 ENCRYPTION</b>	<b>34·13</b>
34.3.1 Protocol Basics	34·8	34.5.1 Secure SIP	34·13
34.3.2 VoIP Threats	34·9	34.5.2 Secure Real-Time Protocol	34·13
		34.5.3 Session Border Control	34·14
<b>34.4 PROTECTING THE INFRASTRUCTURE</b>	<b>34·11</b>	<b>34.6 CONCLUDING REMARKS</b>	<b>34·14</b>
34.4.1 Real-Time Antivirus Scanning	34·11	<b>34.7 FURTHER READING</b>	<b>34·14</b>
		<b>34.8 NOTES</b>	<b>34·15</b>

**34.1 INTRODUCTION.** Whether it is referred to as Voice over Internet Protocol (VoIP) or Internet Protocol Telephony (IPT), the digitization of voice messaging has had and will continue to have an impact on society. Voice messaging is part of a shift that some are calling the Unified Messaging System (UMS).<sup>1</sup> The future does not include separate applications for instant messaging, text messaging, voice communications, video conferencing, e-mail, and network presence. These are expected to become one application that will be shared by both the home user and large corporations. New technologies promise to empower users as never before by freeing our communications from geographically stationary limits. For example, users can decide to work from home and have their office telephones ring into their laptops. Aside from convenience and

# CHAPTER 35

## SECURING P2P, IM, SMS, AND COLLABORATION TOOLS

Carl Ness

<b>35.1 INTRODUCTION</b>	<b>35·1</b>	<b>35.5 SECURING SMS</b>	<b>35·12</b>
<b>35.2 GENERAL CONCEPTS AND DEFINITIONS</b>	<b>35·1</b>	35.5.1 Dangers to the Business	35·12
35.2.1 Peer to Peer	35·2	35.5.2 Prevention and Mitigation	35·13
35.2.2 Instant Messaging	35·2	35.5.3 Reaction and Response	35·16
35.2.3 Short Message Service	35·2		
35.2.4 Collaboration Tools	35·3		
<b>35.3 PEER-TO-PEER NETWORKS</b>	<b>35·3</b>	<b>35.6 SECURING COLLABORATION TOOLS</b>	<b>35·16</b>
35.3.1 Dangers to the Business	35·3	35.6.1 Security versus Openness	35·16
35.3.2 Prevention and Mitigation	35·5	35.6.2 Dangers of Collaboration Tools	35·17
35.3.3 Response	35·7	35.6.3 Prevention and Mitigation	35·18
35.3.4 Case Study	35·7	35.6.4 Reaction and Response	35·19
<b>35.4 SECURING INSTANT MESSAGING</b>	<b>35·8</b>		
35.4.1 Dangers to the Business	35·8	<b>35.7 CONCLUDING REMARKS</b>	<b>35·20</b>
35.4.2 Prevention and Mitigation	35·9	<b>35.8 FURTHER READING</b>	<b>35·20</b>
35.4.3 Response	35·11	<b>35.9 NOTES</b>	<b>35·20</b>
35.4.4 Safe Messaging	35·11		

**35.1 INTRODUCTION.** Peer-to-peer (P2P) communications, instant messaging (IM), short message services (SMS), and collaboration tools must be directly addressed in any comprehensive security plan. The dangers are very real, as is the probability that at least one of these technologies is in use on almost every information system.

**35.2 GENERAL CONCEPTS AND DEFINITIONS.** This chapter is designed to present enough information and resources to aid in integrating the defense of each function into the organization's security plan. A list of resources is provided at the end of the chapter to aid in further research.

# CHAPTER 36

## SECURING STORED DATA

David J. Johnson, Nicholas Takacs, and Jennifer Hadley

<b>36.1 INTRODUCTION TO SECURING STORED DATA</b>	<b>36·1</b>	36.3.2 Trusted Hosts	36·8
36.1.1 Security Basics for Storage Administrators	36·2	36.3.3 Buffer Overflows	36·8
36.1.2 Best Practices	36·2	36.3.4 NFS Security	36·8
36.1.3 DAS, NAS, and SAN	36·3	<b>36.4 CIFS EXPLOITS</b>	<b>36·8</b>
36.1.4 Out-of-Band and In-Band Storage Management	36·4	36.4.1 Authentication	36·9
36.1.5 File System Access Controls	36·4	36.4.2 Rogue or Counterfeit Hosts	36·9
36.1.6 Backup and Restore System Controls	36·4	<b>36.5 ENCRYPTION</b>	<b>36·9</b>
36.1.7 Protecting Management Interfaces	36·5	36.5.1 Recoverability	36·9
<b>36.2 FIBER CHANNEL WEAKNESS AND EXPLOITS</b>	<b>36·6</b>	36.5.2 File Encryption	36·10
36.2.1 Man-in-the-Middle Attacks	36·6	36.5.3 Volume Encryption and Encrypted File Systems	36·10
36.2.2 Session Hijacking	36·7	36.5.4 Full Disk Encryption	36·10
36.2.3 Name Server Corruption	36·7	36.5.5 Vulnerability of Volume, File System, and Full Disk Encryption	36·11
36.2.4 Fiber Channel Security	36·7	36.5.6 Database Encryption	36·12
<b>36.3 NFS WEAKNESS AND EXPLOITS</b>	<b>36·7</b>	<b>36.6 DATA DISPOSAL</b>	<b>36·13</b>
36.3.1 User and File Permissions	36·8	<b>36.7 CONCLUDING REMARKS</b>	<b>36·14</b>
		<b>36.8 FURTHER READING</b>	<b>36·14</b>
		<b>36.9 NOTES</b>	<b>36·15</b>

**36.1 INTRODUCTION TO SECURING STORED DATA.** This chapter reviews methods of securing data stored on nonvolatile media. Nonvolatile media include magnetic disks and their (hard) drives, compact discs (CDs), and digital video disks (DVDs) with their optical drives, and flash drives (also known as USB drives, flash disks, and memory keys). Volatile storage devices, which are not covered in this

# CHAPTER 37

## PKI AND CERTIFICATE AUTHORITIES

**Santosh Chokhani, Padgett Peterson,  
and Steven Lovaas**

<b>37.1 INTRODUCTION</b>	<b>37·2</b>	37.6.7 Public Key Infrastructure Interoperability	37·14
37.1.1 Symmetric Key Cryptography	37·2	<b>37.7 FORMS OF REVOCATION</b>	<b>37·18</b>
37.1.2 Public Key Cryptosystem	37·2	37.7.1 Types of Revocation-Notification Mechanisms	37·18
37.1.3 Advantages of Public Key Cryptosystem over Secret Key Cryptosystem	37·3	37.7.2 Certificate Revocation Lists and Their Variants	37·18
37.1.4 Combination of the Two	37·3	37.7.3 Server-Based Revocation Protocols	37·20
<b>37.2 NEED FOR PUBLIC KEY INFRASTRUCTURE</b>	<b>37·4</b>	37.7.4 Summary of Recommendations for Revocation Notification	37·21
<b>37.3 PUBLIC KEY CERTIFICATE</b>	<b>37·5</b>	<b>37.8 REKEY</b>	<b>37·21</b>
<b>37.4 ENTERPRISE PUBLIC KEY INFRASTRUCTURE</b>	<b>37·7</b>	<b>37.9 KEY RECOVERY</b>	<b>37·22</b>
<b>37.5 CERTIFICATE POLICY</b>	<b>37·8</b>	<b>37.10 PRIVILEGE MANAGEMENT</b>	<b>37·24</b>
<b>37.6 GLOBAL PUBLIC KEY INFRASTRUCTURE</b>	<b>37·9</b>	<b>37.11 TRUSTED ARCHIVAL SERVICES AND TRUSTED TIME STAMPS</b>	<b>37·25</b>
37.6.1 Levels of Trust	37·9	<b>37.12 COST OF PUBLIC KEY INFRASTRUCTURE</b>	<b>37·26</b>
37.6.2 Proofing	37·10	<b>37.13 FURTHER READING</b>	<b>37·27</b>
37.6.3 Trusted Paths	37·10	<b>37.14 NOTES</b>	<b>37·27</b>
37.6.4 Trust Models	37·11		
37.6.5 Choosing a Public Key Infrastructure Architecture	37·13		
37.6.6 Cross-Certification	37·13		

## WRITING SECURE CODE

Lester E. Nichols, M. E. Kabay, and  
Timothy Braithwaite

<b>38.1 INTRODUCTION</b>	<b>38·1</b>	38.3.5 Languages	38·7
<b>38.2 POLICY AND MANAGEMENT ISSUES</b>	<b>38·1</b>	<b>38.4 TYPES OF SOFTWARE ERRORS</b>	<b>38·8</b>
38.2.1 Software Total Quality Management	38·2	38.4.1 Internal Design or Implementation Errors	38·8
38.2.2 Due Diligence	38·3	<b>38.5 ASSURANCE TOOLS AND TECHNIQUES</b>	<b>38·13</b>
38.2.3 Regulatory and Compliance Considerations	38·4	38.5.1 Education Resources	38·13
<b>38.3 TECHNICAL AND PROCEDURAL ISSUES</b>	<b>38·4</b>	38.5.2 Code Examination and Application Penetration Testing	38·13
38.3.1 Requirements Analysis	38·4	38.5.3 Standards and Best Practices	38·15
38.3.2 Design	38·5	<b>38.6 CONCLUDING REMARKS</b>	<b>38·15</b>
38.3.3 Operating System	38·5	<b>38.7 FURTHER READING</b>	<b>38·15</b>
38.3.4 Best Practices and Guidelines	38·6		

**38.1 INTRODUCTION.** The topic of secure coding cannot be adequately addressed in a single chapter. Unfortunately, programs are inherently difficult to secure because of the large number of ways that execution can traverse the code as a result of different input sequences and data values.

This chapter provides a starting point and additional resources for security professionals, system architects, and developers to build a successful and secure development methodology. Writing secure code takes coordination and cooperation of various functional areas within an organization, and may require fundamental changes in the way software development currently is designed, written, tested, and implemented.

**38.2 POLICY AND MANAGEMENT ISSUES.** There are countless security hurdles facing those writing code and developing software. Today dependence on the reliability and security of the automated system is nearly total. For an increasing number of organizations, distributed information processes, implemented via networked environments, have become the critical operating element of their business. Not only must the processing system work when needed, but the information processed must



# CHAPTER 39

## SOFTWARE DEVELOPMENT AND QUALITY ASSURANCE

**Diane E. Levine, John Mason, and Jennifer Hadley**

<b>39.1</b>	<b>INTRODUCTION</b>	<b>39·2</b>	<b>39.5</b>	<b>DESIGNING SOFTWARE TEST CASES</b>	<b>39·12</b>
<b>39.2</b>	<b>GOALS OF SOFTWARE QUALITY ASSURANCE</b>	<b>39·2</b>	39.5.1	Good Tests	39·12
39.2.1	Uncover All of a Program's Problems	39·2	39.5.2	Emphasize Boundary Conditions.	39·12
39.2.2	Reduce the Likelihood that Defective Programs Will Enter Production	39·2	39.5.3	Check All State Transitions.	39·13
39.2.3	Safeguard the Interests of Users	39·3	39.5.4	Use Test-Coverage Monitors.	39·14
39.2.4	Safeguard the Interests of Software Producers	39·3	39.5.5	Seeding.	39·15
<b>39.3</b>	<b>SOFTWARE DEVELOPMENT LIFE CYCLE</b>	<b>39·3</b>	39.5.6	Building Test Data Sets	39·15
39.3.1	Phases of the Traditional Software Development Life Cycle	39·4	<b>39.6</b>	<b>BEFORE GOING INTO PRODUCTION</b>	<b>39·15</b>
39.3.2	Classic Waterfall Model	39·5	39.6.1	Regression Testing	39·15
39.3.3	Rapid Application Development and Joint Application Design	39·7	39.6.2	Automated Testing.	39·15
39.3.4	Importance of Integrating Security at Every Phase	39·7	39.6.3	Tracking Bugs from Discovery to Removal	39·16
<b>39.4</b>	<b>TYPES OF SOFTWARE ERRORS</b>	<b>39·7</b>	<b>39.7</b>	<b>MANAGING CHANGE</b>	<b>39·16</b>
39.4.1	Internal Design or Implementation Errors	39·7	39.7.1	Change Request	39·17
39.4.2	User Interface	39·10	39.7.2	Tracking System	39·17
			39.7.3	Regression Testing	39·17
			39.7.4	Documentation	39·17
			<b>39.8</b>	<b>SOURCES OF BUGS AND PROBLEMS</b>	<b>39·18</b>
			39.8.1	Design Flaws	39·18
			39.8.2	Implementation Flaws	39·18
			39.8.3	Unauthorized Changes to Production Code	39·18

# CHAPTER 40

## MANAGING SOFTWARE PATCHES AND VULNERABILITIES

Peter Mell and Karen Kent

<b>40.1 INTRODUCTION</b>	<b>40·1</b>	Information to Administrators	40·15
<b>40.2 MOTIVATION FOR USING AUTOMATED PATCHING SOLUTIONS</b>	<b>40·2</b>	40.3.9 Verifying Remediation	40·15
		40.3.10 Vulnerability Remediation Training	40·17
<b>40.3 PATCH AND VULNERABILITY MANAGEMENT PROCESS</b>	<b>40·4</b>	<b>40.4 PATCH AND VULNERABILITY MANAGEMENT ISSUES</b>	<b>40·17</b>
40.3.1 Recommended Process	40·4	40.4.1 Enterprise Patching Solutions	40·18
40.3.2 Creating a System Inventory	40·6	40.4.2 Reducing the Need to Patch through Smart Purchasing	40·22
40.3.3 Monitoring for Vulnerabilities, Remediations, and Threats	40·9	40.4.3 Using Standardized Configurations	40·23
40.3.4 Prioritizing Vulnerability Remediation	40·10	40.4.4 Patching after a Security Compromise	40·24
40.3.5 Creating an Organization-Specific Remediation Database	40·11	<b>40.5 CONCLUSION AND SUMMARY OF MAJOR RECOMMENDATIONS</b>	<b>40·24</b>
40.3.6 Testing Remediations	40·11	<b>40.6 FURTHER READING</b>	<b>40·25</b>
40.3.7 Deploying Vulnerability Remediations	40·13	<b>40.7 NOTES</b>	<b>40·25</b>
40.3.8 Distributing Vulnerability and Remediation			

**40.1 INTRODUCTION.** *Vulnerabilities* are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer system. *Patches* are additional pieces of code developed to address problems (commonly called “bugs”) in software. Patches enable additional functionality, or they address security flaws such as vulnerabilities within a program. Not all vulnerabilities have related patches, especially when new vulnerabilities are first announced, so system administrators must be aware not only of applicable vulnerabilities and

# CHAPTER 41

## ANTIVIRUS TECHNOLOGY

They Cobb and Allysa Myers

<b>41.1 INTRODUCTION</b>	<b>41 · 1</b>	41.4.4 Intrusion Detection and Prevention	41 · 10
41.1.1 Antivirus Terminology	41 · 2	<b>41.5 CONTENT FILTERING</b>	<b>41 · 10</b>
41.1.2 Antivirus Issues	41 · 3	41.5.1 How Content Filters Work	41 · 11
<b>41.2 HISTORY OF VIRAL CHANGES</b>	<b>41 · 4</b>	41.5.2 Efficiency and Efficacy	41 · 12
<b>41.3 ANTIVIRUS BASICS</b>	<b>41 · 5</b>	<b>41.6 ANTIVIRUS DEPLOYMENT</b>	<b>41 · 12</b>
41.3.1 Early Days of AV Scanners	41 · 5	41.6.1 Desktops Alone	41 · 12
41.3.2 Validity of Scanners	41 · 6	41.6.2 Server-Based Antivirus	41 · 13
41.3.3 Scanner Internals	41 · 7	<b>41.7 POLICIES AND STRATEGIES</b>	<b>41 · 13</b>
41.3.4 Antivirus Engines and Antivirus Databases	41 · 7	<b>41.8 CONCLUDING REMARKS</b>	<b>41 · 14</b>
<b>41.4 SCANNING METHODOLOGIES</b>	<b>41 · 8</b>	<b>41.9 FURTHER READING</b>	<b>41 · 14</b>
41.4.1 Specific Detection	41 · 8	<b>41.10 NOTE</b>	<b>41 · 14</b>
41.4.2 Generic Detection	41 · 8		
41.4.3 Heuristics	41 · 9		

**41.1 INTRODUCTION.** For over two decades, computer viruses have been a persistent, annoying, and costly threat, and there is no end in sight to the problem. There are many vendors offering to provide a cure for viruses and malware, but the mere existence of these software pests is understandably vexing to those charged with system security.

Initially, most viruses were not designed to cause harm but were created more to gain notoriety for the creator or as a prank. Because these early viruses were designed to subvert legitimate program operations across multiple systems, they were more likely to cause unexpected problems. These viruses, and later some Trojans, often damaged data and caused system downtime. The cleanup required to recover from even a minor virus infection was expensive in terms of lost productivity and unbudgeted labor costs.

Viruses and Trojan behavior have merged, and now both are considered as part of the larger family referred to as malware. No longer is malware just written for a virus writer's 15 minutes of fame; today, malware is created primarily for financial gain. Malware can still cause damage, but now it is more likely to have been created to

# CHAPTER 42

## PROTECTING DIGITAL RIGHTS: TECHNICAL APPROACHES

**Robert Guess, Jennifer Hadley,  
Steven Lovaas, and Diane E. Levine**

<b>42.1</b>	<b>INTRODUCTION</b>	<b>42·1</b>	<b>42.4</b>	<b>DIGITAL RIGHTS MANAGEMENT</b>	<b>42·13</b>
	42.1.1 Digital Rights	42·2		42.4.1 Purpose	42·13
	42.1.2 Patent, Copyright, and Trademark Laws	42·2		42.4.2 Application	42·13
	42.1.3 Piracy	42·2		42.4.3 Examples	42·14
	42.1.4 Privacy	42·3	<b>42.5</b>	<b>PRIVACY-ENHANCING TECHNOLOGIES</b>	<b>42·14</b>
<b>42.2</b>	<b>SOFTWARE-BASED ANTIPIRACY TECHNIQUES</b>	<b>42·3</b>		42.5.1 Network Proxy	42·14
	42.2.1 Organizational Policy	42·4		42.5.2 Hidden Operating Systems	42·15
	42.2.2 Software Usage Counters	42·4	<b>42.6</b>	<b>FUNDAMENTAL PROBLEMS</b>	<b>42·15</b>
<b>42.3</b>	<b>HARDWARE-BASED ANTIPIRACY TECHNIQUES</b>	<b>42·5</b>	<b>42.7</b>	<b>SUMMARY</b>	<b>42·16</b>
	42.3.1 Dongles	42·5	<b>42.8</b>	<b>GLOSSARY</b>	<b>42·17</b>
	42.3.2 Specialized Readers	42·6	<b>42.9</b>	<b>FURTHER READING</b>	<b>42·20</b>
	42.3.3 Evanescent Media	42·10	<b>42.10</b>	<b>NOTES</b>	<b>42·20</b>
	42.3.4 Software Keys	42·11			

**42.1 INTRODUCTION.** Ever since publishing and commerce were introduced to the digital world, the risks to intellectual property and to personal privacy in cyberspace have steadily escalated on comparable but separate paths. These paths have now converged. Unfortunately, many times, antipiracy efforts lead to possible breaches in personal privacy.

Efforts to stem the flow of pirated software worldwide remain mediocre in efficacy; piracy is still proving to be big business in the new millennium. According to the Business Software Alliance (BSA), a 2006 study shows that “thirty-five percent of the packaged software installed on personal computers (PC) worldwide in 2005 was illegal, amounting to \$34 billion in global losses due to software piracy.”<sup>1</sup> This single-year loss equals 57 percent of the total for years 1995 to 2000 combined. Although the methods

## INTRODUCTION TO PART IV

# PREVENTION: HUMAN FACTORS

Human factors underlie all the mechanisms invented by technical experts. Without human awareness, training, education, and motivation, technical defenses inevitably fail. This part details a number of valuable areas of knowledge for security practitioners, including these chapters and topics:

- 43. Ethical Decision Making and High Technology.** A strategy for setting a high priority on ethical behavior and a framework for making ethical decisions
- 44. Security Policy Guidelines.** Guidelines for how to express security policies effectively
- 45. Employment Practices and Policies.** Policy guidelines on hiring, managing, and firing employees
- 46. Vulnerability Assessment.** Methods for smoothly integrating vulnerability assessments into the corporate culture
- 47. Operations Security and Production Controls.** Running computer operations securely, and controlling production for service levels and quality
- 48. E-Mail and Internet Use Policies.** Guidelines for setting expectations about employee use of the Web and e-mail at work
- 49. Implementing a Security Awareness Program.** Methods for ensuring that all employees are aware of security requirements and policies
- 50. Using Social Psychology to Implement Security Policies.** Drawing on the science of social psychology for effective implementation of security policies
- 51. Security Standards for Products.** Established standards for evaluating the trustworthiness and effectiveness of security products

# CHAPTER 43

## ETHICAL DECISION MAKING AND HIGH TECHNOLOGY

James Landon Linderman

<b>43.1 INTRODUCTION: THE ABCs OF COMPUTER ETHICS</b>	<b>43·1</b>		
43.1.1 Why an Ethics Chapter in a Computer Security Handbook?	43·1	43.3.4 A Guideline Approach: Ask!	43·4
43.1.2 How Much Time Do You Have for This Chapter?	43·2	43.3.5 Another Guideline Approach: An Ethics Officer	43·4
<b>43.2 AWARENESS</b>	<b>43·2</b>	<b>43.4 CONSIDERATIONS</b>	<b>43·4</b>
43.2.1 Principle 1: Ethics Counts	43·2	43.4.1 Principle 5: Ethics Need Not and Should Not Be a Hassle	43·4
43.2.2 Principle 2: Ethics Is Everybody's Business	43·2	43.4.2 Principle 6: Ethics Policies Deserve Formality	43·5
43.2.3 A Test: Put Yourself in Another's Shoes	43·2	43.4.3 Principle 7: Ethics Policies Deserve Review	43·5
43.2.4 An Approach: Disclose!	43·2	43.4.4 Principle 8: Anticipate	43·6
<b>43.3 BASICS</b>	<b>43·3</b>	43.4.5 The Smell Test	43·6
43.3.1 Principle 3: Stakeholders Dictate Ethics	43·3	43.4.6 An Approach: Stock Taking	43·6
43.3.2 Principle 4: Traditional Principles Still Apply	43·3	<b>43.5 CONCLUDING REMARKS</b>	<b>43·7</b>
43.3.3 More Tests	43·3	43.5.1 How to Keep Up	43·7
		43.5.2 Why to Keep Up	43·7
		<b>43.6 FURTHER READING</b>	<b>43·8</b>

### 43.1 INTRODUCTION: THE ABCs OF COMPUTER ETHICS

#### 43.1.1 Why an Ethics Chapter in a Computer Security Handbook?

In an information age, many potential misuses and abuses of information create privacy and security problems. In addition to possible legal issues, ethical issues affect many groups and individuals—including employees and customers, vendors, consultants, bankers, and stockholders—who have enough at stake in the matter to confront and even destroy an organization over ethical lapses. As is so often the case, consciousness raising is at the heart of maintaining control.

# CHAPTER 44

## SECURITY POLICY GUIDELINES

M. E. Kabay and Bridgitt Robertson

<b>44.1</b>	<b>INTRODUCTION</b>	<b>44·1</b>	<b>44.5</b>	<b>ORGANIZING THE POLICIES</b>	<b>44·11</b>
<b>44.2</b>	<b>TERMINOLOGY</b>	<b>44·2</b>	44.5.1	Topical Organization	44·11
	44.2.1 Policy	44·2	44.5.2	Organizational	44·12
	44.2.2 Controls	44·2			
	44.2.3 Standards	44·2	<b>44.6</b>	<b>PRESENTING THE POLICIES</b>	<b>44·12</b>
	44.2.4 Procedures	44·3	44.6.1	Printed Text	44·12
<b>44.3</b>	<b>RESOURCES FOR POLICY WRITERS</b>	<b>44·3</b>	44.6.2	Electronic One-Dimensional Text	44·13
	44.3.1 ISO/IEC 17799: 2005	44·3	44.6.3	Hypertext	44·13
	44.3.2 COBIT	44·4	<b>44.7</b>	<b>MAINTAINING POLICIES</b>	<b>44·14</b>
	44.3.3 Informal Security Standards	44·5	44.7.1	Review Process	44·15
	44.3.4 Commercially Available Policy Guides	44·9	44.7.2	Announcing Changes	44·15
<b>44.4</b>	<b>WRITING THE POLICIES</b>	<b>44·10</b>	<b>44.8</b>	<b>SUMMARY</b>	<b>44·15</b>
	44.4.1 Orientation: Prescriptive and Proscriptive	44·10	<b>44.9</b>	<b>FURTHER READING</b>	<b>44·16</b>
	44.4.2 Writing Style	44·11	<b>44.10</b>	<b>NOTES</b>	<b>44·16</b>
	44.4.3 Reasons	44·11			

**44.1 INTRODUCTION.** This chapter reviews principles, topics, and resources for creating effective security policies. It does not propose specific guidelines except as examples. Many of the chapters in this *Handbook* discuss policy; a few examples are listed next:

Chapter 23 provides an extensive overview of physical security policies.

Chapter 25 discusses local area network security issues and policies.

Chapter 38 reviews software development policies.

Chapter 39 surveys quality assurance policies.

Chapter 45 provides guidance on employment policies from a security standpoint.

# CHAPTER 45

## EMPLOYMENT PRACTICES AND POLICIES

**M. E. Kabay and Bridgitt Robertson**

<b>45.1 INTRODUCTION</b>	<b>45 · 1</b>	45.3.6 Responding to Changes in Behavior	45 · 7
<b>45.2 HIRING</b>	<b>45 · 2</b>	45.3.7 Separation of Duties	45 · 9
45.2.1 Checking Candidate's Background	45 · 2	45.3.8 No Unauthorized Security Probes	45 · 10
45.2.2 Employment Agreements	45 · 3		
<b>45.3 MANAGEMENT</b>	<b>45 · 3</b>	<b>45.4 TERMINATION OF EMPLOYMENT</b>	<b>45 · 10</b>
45.3.1 Identify Opportunities for Abuse	45 · 4	45.4.1 Resignations	45 · 11
45.3.2 Access Is Neither a Privilege Nor a Right	45 · 4	45.4.2 Firings	45 · 11
45.3.3 The Indispensable Employee	45 · 4	<b>45.5 SUMMARY</b>	<b>45 · 15</b>
45.3.4 Career Advancement	45 · 6	<b>45.6 FURTHER READING</b>	<b>45 · 15</b>
45.3.5 Vacation Time	45 · 7	<b>45.7 NOTES</b>	<b>45 · 16</b>

**45.1 INTRODUCTION.** Crime is a human issue, not merely a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world will not stop someone from getting into the computer room if the janitor believes it is “just to pick up a listing.”

People are the key to effective information security, and disaffected employees and angry ex-employees are important threats according to many current studies. For example, the 2007 CSI Computer Crime and Security Survey, published by the Computer Security Institute, reported on responses from 494 participants in a wide range of industries, nonprofits and government agencies; the authors stated:

Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.<sup>1</sup>

The same report indicated that about 64 percent of the respondents believed that insiders accounted for at least some of their cybercrime losses:



# CHAPTER 46

## VULNERABILITY ASSESSMENT

Rebecca Gurley Bace

<b>46.1 SCOREKEEPER OF SECURITY MANAGEMENT</b>	<b>46·1</b>	46.2.3 Vulnerability Scanning	46·5
46.1.1 What Is Vulnerability Management?	46·1	46.2.4 Assessment Strategies	46·5
46.1.2 What Is Vulnerability Assessment?	46·2	46.2.5 Strengths and Weaknesses of VAS	46·6
46.1.3 Where Does Vulnerability Assessment Fit in Security Management?	46·2	46.2.6 Roles for Vulnerability Assessment in System Security Management	46·7
46.1.4 Brief History of Vulnerability Assessment	46·3	<b>46.3 PENETRATION TESTING</b>	<b>46·7</b>
<b>46.2 TAXONOMY OF VULNERABILITY ASSESSMENT TECHNOLOGIES</b>	<b>46·3</b>	46.3.1 Penetration Test Goals	46·7
46.2.1 Vulnerability Assessment Strategy and Techniques	46·3	46.3.2 Attributes of Penetration Testing	46·8
46.2.2 Network Scanning	46·4	46.3.3 Social Engineering	46·8
		46.3.4 Managing Penetration Testing	46·9
		<b>46.4 FURTHER READING</b>	<b>46·10</b>
		<b>46.5 NOTES</b>	<b>46·10</b>

**46.1 SCOREKEEPER OF SECURITY MANAGEMENT.** Information security has, over time, evolved from a collection of esoteric security issues and technical remedies to its current state, in which it is more tightly integrated with the area of enterprise risk management. One effect of this move from technology to management discipline is the growth in the deployment and use of vulnerability management (and its primary technical constituent, vulnerability assessment [VA]) systems. These systems are considered fundamental to modern information security practice and have matured in architecture, features, and interfaces to accommodate the changing landscape of modern enterprises.

**46.1.1 What Is Vulnerability Management?** Vulnerability management is a process of assessing deployed IT systems in order to determine the security state of the system. It includes the determination of corrective measures to mitigate issues identified that represent exposures for the enterprise, and managing the application of those measures. Vulnerability assessment is the key technology component of vulnerability management. However, there is a synergy between VA and the other elements of

# CHAPTER 47

## OPERATIONS SECURITY AND PRODUCTION CONTROLS

M. E. Kabay, Don Holden, and Myles Walsh

<b>47.1 INTRODUCTION</b>	<b>47·1</b>	47.3.2 Installing a New Version of the Operating System	47·12
47.1.1 What Are Production Systems?	47·2	47.3.3 Patching the Operating System	47·12
47.1.2 What Are Operations?	47·2		
47.1.3 What Are Computer Programs?	47·3	<b>47.4 PROTECTION OF DATA</b>	<b>47·13</b>
47.1.4 What Are Procedures?	47·3	47.4.1 Access to Production Programs and Control Data	47·13
47.1.5 What Are Data Files?	47·3	47.4.2 Separating Production, Development, and Test Data	47·13
<b>47.2 OPERATIONS MANAGEMENT</b>	<b>47·4</b>	47.4.3 Controlling User Access to Files and Databases	47·14
47.2.1 Separation of Duties	47·4	<b>47.5 DATA VALIDATION</b>	<b>47·15</b>
47.2.2 Security Officer or Administrator	47·4	47.5.1 Edit Checks	47·15
47.2.3 Limit Access to Operations Center	47·5	47.5.2 Check Digits and Log Files	47·16
47.2.4 Change-Control Procedures from the Operations Perspective	47·6	47.5.3 Handling External Data	47·16
47.2.5 Using Externally Supplied Software	47·9	<b>47.6 CONCLUDING REMARKS</b>	<b>47·17</b>
47.2.6 Quality Control versus Quality Assurance	47·10	<b>47.7 FURTHER READING</b>	<b>47·17</b>
<b>47.3 PROVIDING A TRUSTED OPERATING SYSTEM</b>	<b>47·12</b>	<b>47.8 NOTES</b>	<b>47·18</b>
47.3.1 Creating Known-Good Boot Medium	47·12		

**47.1 INTRODUCTION.** Despite the enormous increase in individual computing on personal computers and workstations in the years since the first edition of this *Handbook* was published in 1975, many mainframe computers and their networks are

# CHAPTER 48

## E-MAIL AND INTERNET USE POLICIES

M. E. Kabay and Nicholas Takacs

<b>48.1 INTRODUCTION</b>	<b>48·2</b>	<b>48.5 LEGAL LIABILITY</b>	<b>48·30</b>
		48.5.1 Libel	48·30
		48.5.2 Stolen Software, Music, and Videos	48·30
<b>48.2 DAMAGING THE REPUTATION OF THE ENTERPRISE</b>	<b>48·2</b>	48.5.3 Plagiarism	48·30
48.2.1 Violating Laws	48·3	48.5.4 Criminal Hacking and Hactivism	48·32
48.2.2 Ill-Advised E-mail	48·3	48.5.5 Creating a Hostile Work Environment	48·32
48.2.3 Inappropriate Use of Corporate Identifiers	48·4	48.5.6 Archiving E-mail	48·35
48.2.4 Blogs, Personal Web Sites, and Social Networking Sites	48·5	<b>48.6 RECOMMENDATIONS</b>	<b>48·35</b>
48.2.5 Disseminating and Using Incorrect Information	48·5	48.6.1 Protecting Children	48·35
48.2.6 Hoaxes	48·6	48.6.2 Threats	48·36
		48.6.3 Hate Sites	48·36
<b>48.3 THREATS TO PEOPLE AND SYSTEMS</b>	<b>48·12</b>	48.6.4 Pornography	48·37
48.3.1 Threats of Physical Harm	48·12	48.6.5 Internet Addiction	48·37
48.3.2 Pedophiles Online	48·12	48.6.6 Online Dating	48·37
48.3.3 Viruses and Other Malicious Code	48·13	48.6.7 Online Games	48·39
48.3.4 Spyware and Adware	48·13	48.6.8 Online Purchases	48·39
		48.6.9 Online Auctions	48·40
<b>48.4 THREATS TO PRODUCTIVITY</b>	<b>48·14</b>	48.6.10 Online Gambling	48·40
48.4.1 Inefficient Use of Corporate E-mail	48·15	48.6.11 Preventing Malware Infections	48·41
48.4.2 Mail Storms	48·21	48.6.12 Guarding against Spyware	48·41
48.4.3 Buying on the Web	48·23	48.6.13 Junk E-mail	48·42
48.4.4 Online Gambling	48·26	48.6.14 Mail Storms	48·42
48.4.5 Internet Addiction	48·27	48.6.15 Detecting Hoaxes	48·43
48.4.6 Online Dating and Cybersex	48·28	48.6.16 Get-Rich-Quick Schemes	48·43
48.4.7 Games and Virtual Reality	48·29	48.6.17 Hacking	48·44
		<b>48.7 CONCLUDING REMARKS</b>	<b>48·44</b>
		<b>48.8 FURTHER READING</b>	<b>48·44</b>
		<b>48.9 NOTES</b>	<b>48·45</b>

# CHAPTER 49

## IMPLEMENTING A SECURITY AWARENESS PROGRAM

**K. Rudolph**

<b>49.1 INTRODUCTION</b>	<b>49·2</b>	49.4.6 Addressing the Diffusion of Responsibility	49·13
<b>49.2 AWARENESS AS A SURVIVAL TECHNIQUE</b>	<b>49·2</b>	<b>49.5 APPROACH</b>	<b>49·14</b>
49.2.1 Awareness versus Training	49·4	49.5.1 Awareness as Social Marketing	49·14
49.2.2 IT Security Is a People Problem	49·4	49.5.2 Motivation	49·14
49.2.3 Overnight Success Takes Time	49·5	<b>49.6 CONTENT</b>	<b>49·17</b>
<b>49.3 CRITICAL SUCCESS FACTORS</b>	<b>49·5</b>	49.6.1 What Do Security Incidents Look Like?	49·19
49.3.1 In-Place Information Security Policy	49·6	49.6.2 What Do I Do about Security?	49·19
49.3.2 Senior-Level Management Support	49·6	49.6.3 Basic Security Concepts	49·19
49.3.3 Example	49·7	49.6.4 Technical Issues	49·20
49.3.4 Budget	49·7	49.6.5 Reporting	49·20
49.3.5 Security Staff Backing	49·7	<b>49.7 TECHNIQUES AND PRINCIPLES</b>	<b>49·21</b>
49.3.6 Reward for Good Security Behaviors	49·7	49.7.1 Start with a Bang: Make It Attention Getting and Memorable	49·21
49.3.7 Destination and Road Maps	49·8	49.7.2 Appeal to the Target Audience	49·21
49.3.8 Visibility and Audience Appeal	49·9	49.7.3 Address Personality and Learning Styles	49·22
<b>49.4 OBSTACLES AND OPPORTUNITIES</b>	<b>49·10</b>	49.7.4 Keep It Simple: Awareness Is Not Training	49·22
49.4.1 Gaining Management Support	49·10	49.7.5 Use Logos, Themes, and Images	49·22
49.4.2 Keep Management Informed	49·11	49.7.6 Use Stories and Examples: Current and Credible	49·23
49.4.3 Speak Their Language	49·11	49.7.7 Use Failure	49·24
49.4.4 Gaining Union Support	49·12		
49.4.5 Overcoming Audience Resistance	49·13		

## 49.2 IMPLEMENTING A SECURITY AWARENESS PROGRAM

49.7.8	Involve the Audience: Buy-In Is Better than Coercion	49.24	49.8.12	Videos	49.33
49.7.9	Make It Memorable	49.25	49.8.13	Trinkets and Give-Aways	49.34
49.7.10	Use Competition	49.26	49.8.14	Screen Savers	49.34
49.7.11	Incorporate User Acknowledgment and Sign-Off	49.26	49.8.15	Sign-On Screen Messages	49.35
49.7.12	Use Analogies	49.26	49.8.16	Surveys and Suggestion Programs	49.35
49.7.13	Use Humor	49.27	49.8.17	Inspections and Audits	49.35
49.7.14	Show Consequences	49.28	49.8.18	Events, Conferences, Briefings, and Presentations	49.35
49.7.15	Use Circumstances	49.28			
<b>49.8</b>	<b>TOOLS</b>	<b>49.28</b>	<b>49.9</b>	<b>MEASUREMENT AND EVALUATION</b>	<b>49.36</b>
49.8.1	Web-Based Courses	49.28	49.9.1	Changes in Behavior	49.36
49.8.2	Compliance Agreements	49.30	49.9.2	Audience Satisfaction	49.38
49.8.3	Performance Appraisals	49.30	49.9.3	Audience Involvement	49.39
49.8.4	Checklists, Pamphlets, Tip Sheets	49.30	49.9.4	Learning or Teaching Effectiveness	49.39
49.8.5	Memos from Top Management	49.30	49.9.5	Audience Performance	49.39
49.8.6	Newsletters	49.30			
49.8.7	In-Person Briefings (and Brown-Bag Lunches)	49.30	<b>49.10</b>	<b>CONCLUSION</b>	<b>49.39</b>
49.8.8	Contests	49.31	<b>49.11</b>	<b>GLOSSARY</b>	<b>49.40</b>
49.8.9	Intranet and/or Internet	49.31	<b>49.12</b>	<b>FURTHER READING</b>	<b>49.41</b>
49.8.10	Posters	49.31	<b>49.13</b>	<b>NOTES</b>	<b>49.41</b>
49.8.11	Awareness Coupons and Memo Pads	49.31			

**49.1 INTRODUCTION.** Even the best security process will fail when implemented by the uninformed. Information technology security awareness is achieved when people know what is going on around them, can recognize potential security violations or suspicious circumstances, and know what initial actions to take. Security awareness is the result of activities, tools, and techniques intended to attract people's attention and to help them focus on security. Because people play an integral role in protecting an organization's assets, security awareness among staff, contractors, partners, and customers is a necessary and cost-effective countermeasure against security breaches. Effective awareness programs motivate people and provide measurable benefits. Prerequisites for implementing a security awareness program successfully include senior-level management support, an in-place security policy, measurable goals, and a plan for reaching those goals. Attention-getting awareness materials tailored to the audience and to the technology yield maximum program impact. This chapter contains practical information on design approaches for an awareness program, including its content, techniques, principles, tools, measurement approaches, and evaluation techniques.

**49.2 AWARENESS AS A SURVIVAL TECHNIQUE.** In recent years, awareness of security concerns worldwide has increased. Business, government organizations, and individuals are conducting a significant part of their activities electronically. Electronic information (corporate and personal data) often can be easily accessed,

# CHAPTER 50

## USING SOCIAL PSYCHOLOGY TO IMPLEMENT SECURITY POLICIES

M. E. Kabay, Bridgitt Robertson, Mani Akella, and D. T. Lang

<b>50.1 INTRODUCTION</b>	<b>50·1</b>	50.3.3 Changing Attitudes toward Security	50·14
<b>50.2 RATIONALITY IS NOT ENOUGH</b>	<b>50·2</b>	<b>50.4 ENCOURAGING INITIATIVE</b>	<b>50·16</b>
50.2.1 Schema	50·3	50.4.1 Prosocial Behavior	50·16
50.2.2 Theories of Personality	50·4	50.4.2 Conformity, Compliance, and Obedience	50·17
50.2.3 Explanations of Behavior	50·7	<b>50.5 GROUP BEHAVIOR</b>	<b>50·20</b>
50.2.4 Errors of Attribution	50·7	50.5.1 Social Arousal	50·20
50.2.5 Intercultural Differences	50·10	50.5.2 Locus of Control	50·20
50.2.6 Framing Reality	50·11	50.5.3 Group Polarization	50·20
50.2.7 Getting Your Security Policies Across	50·12	50.5.4 Groupthink	50·20
50.2.8 Reward versus Punishment	50·13	<b>50.6 TECHNOLOGICAL GENERATION GAPS</b>	<b>50·21</b>
<b>50.3 BELIEFS AND ATTITUDES</b>	<b>50·13</b>	<b>50.7 SUMMARY OF RECOMMENDATIONS</b>	<b>50·22</b>
50.3.1 Beliefs	50·14	<b>50.8 FURTHER READING</b>	<b>50·24</b>
50.3.2 Attitudes	50·14	<b>50.9 NOTES</b>	<b>50·24</b>

**50.1 INTRODUCTION<sup>1</sup>.** Most security personnel 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. They shake their heads in disbelief as they recount tales of employees who hold secured doors open for their workmates—or for total strangers, thereby rendering million-dollar card-access systems useless. In large organizations, upper managers who decline to wear their identification badges discover that soon no one else will either. In trying to implement security policies, practitioners sometimes feel that they are involved in turf wars and personal vendettas rather than rational discourse.

# CHAPTER 51

## SECURITY STANDARDS FOR PRODUCTS

Paul Brusil and Noel Zakin

<b>51.1 INTRODUCTION</b>	<b>51·2</b>	51.4.1 Capability Maturity Model	51·13
51.1.1 Value of Standards	51·2	51.4.2 Quality (ISO 9000)	51·14
51.1.2 Purpose of Product Assessment	51·3	<b>51.5 COMBINED PRODUCT AND PRODUCT BUILDER ASSESSMENT</b>	<b>51·14</b>
51.1.3 Sources of Standards	51·4	51.5.1 Competing National Criteria Standards	51·14
51.1.4 Classes of Security Standards	51·5	51.5.2 Emergence of Common Criteria Standard	51·15
51.1.5 Products for Which Standards Apply	51·5	<b>51.6 COMMON CRITERIA PARADIGM OVERVIEW</b>	<b>51·16</b>
51.1.6 Breadth of Product-Oriented Standards	51·5	51.6.1 CC Scheme	51·16
51.1.7 Focus of This Chapter	51·6	51.6.2 Common Criteria Paradigm Process	51·17
<b>51.2 NONSTANDARD PRODUCT ASSESSMENT ALTERNATIVES</b>	<b>51·7</b>	51.6.3 Standards that Shape the Common Criteria Paradigm	51·18
51.2.1 Vendor Self-Declarations	51·7	<b>51.7 DETAILS ABOUT THE COMMON CRITERIA STANDARD</b>	<b>51·18</b>
51.2.2 Proprietary In-House Assessments	51·8	51.7.1 Models for Security Profiles	51·18
51.2.3 Consortium-Based Assessment Approaches	51·8	51.7.2 Security Functional Requirements Catalog	51·19
51.2.4 Open Source Approach	51·10	51.7.3 Security Assurance Requirements Catalog	51·19
51.2.5 Hacking	51·11	51.7.4 Comprehensiveness of Requirements Catalogs	51·20
51.2.6 Trade Press	51·11		
51.2.7 Initial Third-Party Commercial Assessment Approaches	51·11		
<b>51.3 SECURITY ASSESSMENT STANDARDS FOR PRODUCTS</b>	<b>51·13</b>		
<b>51.4 STANDARDS FOR ASSESSING PRODUCT BUILDERS</b>	<b>51·13</b>		

## 51.2 SECURITY STANDARDS FOR PRODUCTS

<b>51.8 DEFINE SECURITY REQUIREMENTS AND SECURITY SOLUTIONS</b>	<b>51.21</b>	51.11.1 Maintaining the Testing Infrastructure	51.27
51.8.1 Protection Profile Construction and Contents	51.21	51.11.2 Using the Testing Infrastructure	51.27
51.8.2 Security Target Construction	51.23	51.11.3 Maintaining Certification in an Evolving Marketplace	51.28
51.8.3 Benefits of PPs and STs	51.24		
51.8.4 Extant PPs and STs	51.25	<b>51.12 VALIDATED PROFILES AND PRODUCTS</b>	<b>51.28</b>
<b>51.9 COMMON TEST METHODOLOGY FOR CC TESTS AND EVALUATIONS</b>	<b>51.26</b>	<b>51.13 BENEFITS OF CC EVALUATION</b>	<b>51.29</b>
<b>51.10 GLOBAL RECOGNITION OF CEM/CC-BASED ASSESSMENTS</b>	<b>51.26</b>	51.13.1 Helping Manufacturers	51.29
<b>51.11 EXAMPLE NATIONAL SCHEME: CCEVS</b>	<b>51.26</b>	51.13.2 Helping Consumers	51.30
		<b>51.14 CONCLUDING REMARKS</b>	<b>51.30</b>
		<b>51.15 NOTES</b>	<b>51.31</b>

**51.1 INTRODUCTION.** Standards provide for uniformity of essential characteristics of products and product-related procedures. Standards allow consumers to have a better understanding of what they purchase. This section provides a general introduction to standards: who creates standards, what types of features and capabilities are standardized, why standards are important, and what types of standards apply to products.

In later sections, attention turns to standards associated with testing and evaluation of products. The nonstandard approaches confronting and befuddling consumers, as well as the issues arising from nonstandard approaches, are contrasted with the confidence obtained by using a universal, internationally accepted standard for product testing and evaluation. The common standard allows the consumer to understand with greater certainty the security and assurance features offered by a product. Increased software quality assurance became of top concern to U.S. Government agency chief information security officers (CISOs) as attention turned to the Federal Information Security Management (FISMA) Act.<sup>1</sup>

**51.1.1 Value of Standards.** Many parties benefit from standards: customers, vendors, testing houses, and more.

Customers find standards helpful in several ways. Standards help specify their needs for various security functionalities and the degrees of assurance they require in the products they buy. Standards help customers understand what security functionality and assurances that a product builder claims to provide. Standards help consumers select commercial off-the-shelf products that they can trust will conform to their security and assurance requirements and that, as needed, interoperate with comparable products. Customers under the mandates of the security-relevant regulations imposed by the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) often look to establishing due diligence by leveraging products that have established trust in their security and assurance functionality in a standard way.

Vendors find standards helpful in several ways. Use of standards provides evidence that vendors have migrated their product development to a paradigm wherein security is built-in from the start. Use of standards provides evidence that security is not some



## INTRODUCTION TO PART V

# DETECTING SECURITY BREACHES

No matter how well we implement security mechanisms, we are facing human opponents who may counter our best efforts until we can respond appropriately. How do security and network administrators find out if there has been a breach of security? How can they evaluate their own defenses before they are penetrated? This part includes chapters on:

- 52. Application Controls.** Application-software security and logging
- 53. Monitoring and Control Systems.** System logging and data reduction methods
- 54. Security Audits, Standards, and Inspections.** Measuring compliance with explicit policies and with industry standards
- 55. Cyber Investigation.** Organizing effective digital forensic studies of observed or suspected security breaches, for internal use, and for cooperation with law enforcement

# CHAPTER 52

## APPLICATION CONTROLS

Myles Walsh

<b>52.1 PROTECTION IN APPLICATION DEVELOPMENT</b>	<b>52·1</b>	<b>52.3 PROTECTING BATCH FILES</b>	<b>52·8</b>
		52.3.1 Backup File Creation	52·8
		52.3.2 Audit Controls	52·9
<b>52.2 PROTECTING ONLINE FILES</b>	<b>52·2</b>	<b>52.4 ENSURING THAT INFORMATION IN THE SYSTEM IS VALID</b>	<b>52·9</b>
52.2.1 Types of Data Corruption	52·2	52.4.1 Validation Controls	52·9
52.2.2 Database Management Subsystems	52·3	52.4.2 Diagnostic Utilities	52·11
52.2.3 Lock on Update	52·4	<b>52.5 CONCLUDING REMARKS</b>	<b>52·11</b>
52.2.4 Two-Phase Commit	52·5	<b>52.6 FURTHER READING</b>	<b>52·11</b>
52.2.5 Backup Files and System Logs	52·6	<b>52.7 NOTE</b>	<b>52·12</b>
52.2.6 Recovery and Restart	52·6		
52.2.7 Backout	52·7		
52.2.8 Roll-Forward Recovery	52·7		
52.2.9 Distributed Databases	52·7		

**52.1 PROTECTION IN APPLICATION DEVELOPMENT.** In computer installations where systems development takes place, there are technologies that tend to enhance security. These technologies, together with mandatory organizational procedures and standards, force analysts and programmers to adhere to guidelines when they are developing in-house applications or systems to be marketed. This chapter reviews some of the methods programmers use to prevent and identify problems involving data corruption or unavailability.

One of the underpinnings of modern programming is the technology known as the database management system (DBMS). Many applications are developed using this technology. A contemporary RDBMS supports relational databases. Relational databases themselves are based on an underlying technology developed in the 1960s and implemented through the remainder of the twentieth century. It seems certain that the technology will continue to be used for the foreseeable future.

RDBMSs are sets of programs that provide users with the tools to perform these tasks:

- Create database structures (file or table layouts, and screens or forms).
- Enter information into the structures.
- Establish cross-references among the files or tables.

# CHAPTER 53

## MONITORING AND CONTROL SYSTEMS

Caleb S. Coggins and Diane E. Levine

<b>53.1</b>	<b>INTRODUCTION</b>	<b>53·2</b>	53.4.2 Process Flow and Job Scheduling	53·10
53.1.1	Prevention, Detection, and Response	53·2	53.4.3 Network Connectivity	53·10
53.1.2	Controlling versus Monitoring	53·3	53.4.4 Environmental Concerns	53·11
53.1.3	Control Loop	53·4	53.4.5 System State	53·11
53.1.4	Defining the Scope and System Requirements	53·4	53.4.6 System Components	53·11
			53.4.7 Process Activities	53·12
			53.4.8 File System	53·12
			53.4.9 Access Controls	53·13
<b>53.2</b>	<b>CHANGE AND SECURITY IMPLICATIONS</b>	<b>53·4</b>	<b>53.5 LOG MANAGEMENT</b>	<b>53·13</b>
53.2.1	Regulations, Policies, and Frameworks	53·4	53.5.1 Log Generation	53·13
53.2.2	Change Management	53·5	53.5.2 Types of Log File Records	53·14
53.2.3	Configuration Protection	53·5	53.5.3 Automation and Resource Allocation	53·18
53.2.4	Performance Considerations	53·5	53.5.4 Log Record Security	53·18
<b>53.3</b>	<b>SYSTEM MODELS</b>	<b>53·6</b>	<b>53.6 DATA AGGREGATION AND REDUCTION</b>	<b>53·19</b>
53.3.1	Internal, One to One, One to Many, and Distributed	53·6	53.6.1 Centralized Data Stores	53·19
53.3.2	Automation and the Human–Machine Interface	53·6	53.6.2 Filtered Queries	53·20
53.3.3	Snapshots versus Real Time	53·7	53.6.3 Analyzing Log Records	53·20
53.3.4	Memory Dumps	53·8	53.6.4 Dashboards	53·21
<b>53.4</b>	<b>TARGETS AND METHODS</b>	<b>53·10</b>	<b>53.7 NOTIFICATIONS AND REPORTING</b>	<b>53·22</b>
53.4.1	Overview	53·10	53.7.1 Alerts	53·22
			53.7.2 Trend Analysis and Reporting	53·23

# CHAPTER 54

## SECURITY AUDITS, STANDARDS, AND INSPECTIONS

**Donald Glass, Chris Davis, John Mason,  
David Gursky, James Thomas, Wendy Carr,  
and Diane Levine**

<b>54.1</b>	<b>INTRODUCTION</b>	<b>54·2</b>	54.5.1	Publicly Available Security Publications	54·15
<b>54.2</b>	<b>AUDITING STANDARDS</b>	<b>54·2</b>	54.5.2	Federal Information Systems Management Act (FISMA)	54·17
54.2.1	Introduction to ISO	54·3	54.5.3	Risk Framework	54·18
54.2.2	ISO/IEC 27001	54·4	54.5.4	Multiple Regulations and Information Security Audits	54·19
54.2.3	Gramm-Leach-Bliley Act	54·5		Conclusion	
54.2.4	Auditing Standards Conclusion	54·6	<b>54.6</b>	<b>TECHNICAL FRAMEWORKS FOR IT AUDITS</b>	<b>54·19</b>
<b>54.3</b>	<b>SAS 70 AUDITS</b>	<b>54·7</b>	54.6.1	Framework 1: People, Processes, Tools, and Measures	54·19
54.3.1	Introduction to SAS 70 Audits	54·7	54.6.2	Framework 2: STRIDE	54·20
54.3.2	Cost and Benefits of SAS 70 Audits	54·9	54.6.3	Framework 3: PDIO	54·20
54.3.3	SAS 70 Audits Conclusion	54·10	54.6.4	General Best Practices	54·20
<b>54.4</b>	<b>SARBANES-OXLEY</b>	<b>54·10</b>	54.6.5	Technical Frameworks Conclusion	54·21
54.4.1	Introduction	54·10	<b>54.7</b>	<b>FURTHER READING</b>	<b>54·21</b>
54.4.2	Section 404	54·11	<b>54.8</b>	<b>NOTES</b>	<b>54·22</b>
54.4.3	Achieving Compliance	54·11			
54.4.4	Audit and Certification	54·13			
54.4.5	Sarbanes-Oxley Conclusion	54·14			
<b>54.5</b>	<b>ADDRESSING MULTIPLE REGULATIONS FOR INFORMATION SECURITY</b>	<b>54·14</b>			

# CHAPTER 55

## CYBER INVESTIGATION<sup>1</sup>

Peter Stephenson

<b>55.1 INTRODUCTION</b>	<b>55 · 1</b>	55.3.1 Supporting the EEDI Process	55 · 12
55.1.1 Defining Cyber Investigation	55 · 2	55.3.2 Investigative Narrative	55 · 12
55.1.2 Distinguishing between Cyber Forensics and Cyber Investigation	55 · 2	55.3.3 Intrusion Process	55 · 13
55.1.3 DFRWS Framework Classes	55 · 2	55.3.4 Describing Attacks	55 · 14
		55.3.5 Strategic Campaigns	55 · 15
<b>55.2 END-TO-END DIGITAL INVESTIGATION</b>	<b>55 · 9</b>	<b>55.4 USING EEDI AND THE FRAMEWORK</b>	<b>55 · 16</b>
55.2.1 Collecting Evidence	55 · 10	<b>55.5 MOTIVE, MEANS, AND OPPORTUNITY: PROFILING ATTACKERS</b>	<b>55 · 17</b>
55.2.2 Analysis of Individual Events	55 · 10	55.5.1 Motive	55 · 18
55.2.3 Preliminary Correlation	55 · 11	55.5.2 Means	55 · 20
55.2.4 Event Normalizing	55 · 11	55.5.3 Opportunity	55 · 20
55.2.5 Event Deconfliction	55 · 11	<b>55.6 SOME USEFUL TOOLS</b>	<b>55 · 20</b>
55.2.6 Second-Level Correlation	55 · 11	55.6.1 Link Analysis	55 · 22
55.2.7 Timeline Analysis	55 · 11	55.6.2 Attack-Tree Analysis	55 · 23
55.2.8 Chain of Evidence Construction	55 · 12	55.6.3 Modeling	55 · 23
55.2.9 Corroboration	55 · 12	<b>55.7 CONCLUDING REMARKS</b>	<b>55 · 25</b>
<b>55.3 APPLYING THE FRAMEWORK AND EEDI</b>	<b>55 · 12</b>	<b>55.8 FURTHER READING</b>	<b>55 · 25</b>
		<b>55.9 NOTES</b>	<b>55 · 26</b>

**55.1 INTRODUCTION.** Cyber investigation (also widely known as *digital investigation*) as a discipline has changed markedly since publication of the fourth edition of this *Handbook* in 2002. In 1999, when *Investigating Computer Related Crime*<sup>2</sup> was published, practitioners in the field were just beginning to speculate as to how cyber investigations would be carried out. At that time, the idea of cyber investigation was almost completely congruent with the practice of computer forensics. Today (as this is being written in April 2008), we know that such a view is too confining for investigations in the current digital environment.

## INTRODUCTION TO PART VI

# RESPONSE AND REMEDIATION

What are the options when security breaches or accidents occur? How do we prepare for trouble so that we can minimize the consequences and respond quickly and effectively? This part includes these chapters and topics:

- 56. Computer Security Incident Response Teams.** Planning and rehearsing responses to a wide variety of security problems—in advance instead of on the fly
- 57. Data Backups and Archives.** The essential tool for all forms of recovery
- 58. Business Continuity Planning.** Systematic approach to analyzing the priorities for orderly recovery when anything interrupts the smooth operation of the organization
- 59. Disaster Recovery.** Planning for rapid, cost-effective return to normal after a crisis is over
- 60. Insurance Relief.** Using modern insurance services to reduce the consequences of disasters
- 61. Working with Law Enforcement.** Establishing relations with all levels of law enforcement before there is a crisis, and coordinating efficiently and effectively to support investigation and prosecution of criminals

# CHAPTER 56

## COMPUTER SECURITY INCIDENT RESPONSE TEAMS<sup>1</sup>

Michael Miora, M. E. Kabay,  
and Bernie Cowens

<b>56.1</b>	<b>OVERVIEW</b>	<b>56·2</b>	<b>56.5</b>	<b>RESPONDING TO COMPUTER EMERGENCIES</b>	<b>56·20</b>
56.1.1	Description	56·3	56.5.1	Observe and Evaluate	56·20
56.1.2	Purpose	56·3	56.5.2	Begin Notification	56·21
56.1.3	History and Background	56·4	56.5.3	Set Up Communications	56·21
56.1.4	Types of Teams	56·6	56.5.4	Contain	56·22
<b>56.2</b>	<b>PLANNING THE TEAM</b>	<b>56·7</b>	56.5.5	Identify	56·22
56.2.1	Mission and Charter	56·7	56.5.6	Record	56·22
56.2.2	Establishing Policies and Procedures	56·8	56.5.7	Return to Operations	56·22
56.2.3	Interaction with Outside Agencies and Other Resources	56·9	56.5.8	Document and Review	56·22
56.2.4	Establish Baselines	56·10	56.5.9	Involving Law Enforcement	56·22
<b>56.3</b>	<b>SELECTING AND BUILDING THE TEAM</b>	<b>56·10</b>	56.5.10	Need to Know	56·23
56.3.1	Staffing	56·11	<b>56.6</b>	<b>MANAGING THE CSIRT</b>	<b>56·24</b>
56.3.2	Involve Legal Staff	56·12	56.6.1	Professionalism	56·24
<b>56.4</b>	<b>PRINCIPLES UNDERLYING EFFECTIVE RESPONSE TO COMPUTER SECURITY INCIDENTS</b>	<b>56·12</b>	56.6.2	Setting the Rules for Triage	56·25
56.4.1	Baseline Assumptions	56·12	56.6.3	Triage, Process, and Social Engineering	56·27
56.4.2	Triage	56·13	56.6.4	Avoiding Burnout	56·27
56.4.3	Technical Expertise	56·14	56.6.5	Many Types of Productive Work	56·28
56.4.4	Training	56·14	56.6.6	Setting an Example	56·29
56.4.5	Tracking Incidents	56·15	56.6.7	Notes on Shiftwork	56·29
56.4.6	Telephone Hotline	56·19	56.6.8	Role of Public Affairs	56·30
			56.6.9	Importance of Forensic Awareness	56·30
			<b>56.7</b>	<b>POSTINCIDENT ACTIVITIES</b>	<b>56·30</b>
			56.7.1	Postmortem	56·31

## 56.2 COMPUTER SECURITY INCIDENT RESPONSE TEAMS

56.7.2	Continuous Process Improvement: Sharing Knowledge within the Organization	56.32	<b>56.8 CONCLUDING REMARKS</b>	<b>56.35</b>
			<b>56.9 FURTHER READING</b>	<b>56.35</b>
56.7.3	Sharing Knowledge with the Security Community	56.33	<b>56.10 NOTES</b>	<b>56.35</b>

**56.1 OVERVIEW.** No matter how good one's security, at some point a security measure will fail. Knowing that helps organizations to plan for security in depth, so that a single point of failure does not necessarily result in catastrophe. Furthermore, instead of trying to invent a response when every second counts, it makes sense to have a competent team in place, trained, and ready to act. The value of time is not constant. Spending an hour or a day planning, so that an emergency response is shortened by a few seconds, may save a life or prevent a business disaster.

An essential element of any effective information security program today is the ability to respond to computer emergencies. Although many organizations have some form of intrusion detection in place, far too few take full advantage of the capabilities those systems offer. Fewer still consistently monitor the data available to them from automated intrusion detection systems, let alone respond to what they see.

The key is to make beneficial use of the knowledge that something has happened, that something is about to happen, or that something is perhaps amiss. Intrusion detection systems can be costly to implement and maintain. It therefore makes little business sense to go to the trouble of implementing an intrusion detection capability if there is not, at the same time, a way to make use of the data produced by these systems.

Computer emergency quick-response teams are generally called *computer security incident response teams* (CSIRTs, the abbreviation used in this chapter) or *computer incident response teams* (CIRTs). Sometimes one sees the term "computer emergency response team" (CERT), but that term and acronym are increasingly reserved for the Computer Emergency Response Team Coordination Center (CERT/CC<sup>®</sup>) at the Software Engineering Institute of Carnegie Mellon University, as explained in Section 56.1.3 of this chapter.

CSIRTs can provide organizations with a measurable return on their investment in computer security mechanisms and intrusion detection systems. Intrusion detection can indicate that something occurred; CSIRTs can do something about that occurrence. Often their value to an organization can be felt in more subtle ways as well. Many times computer emergencies and incidents cast an organization in an unfavorable light, and they can erode confidence in that organization. Efficient handling of computer emergencies can lessen the erosion of confidence, can help speed the organization's recovery, and in some cases can help restore its image. In addition, CSIRT postmortems (see Section 56.7) can provide information for process improvement (as discussed in Section 56.7.2).

When an incident occurs, the intrusion detection system makes us aware of the incident in one manner or another. We make use of this knowledge by responding to the situation appropriately. "Appropriately" can mean something different in different situations. Therefore, a well-trained, confident, authoritative CSIRT is essential.

Intrusion detection systems are not the only means by which we learn about incidents. In a sense, every component of a system and every person who interacts with the system forms a part of the overall defense and detection system. End users are often the first to notice that something is different. They may not recognize a particular



# CHAPTER 57

## DATA BACKUPS AND ARCHIVES

M. E. Kabay and Don Holden

<b>57.1 INTRODUCTION</b>	<b>57·1</b>	57.4.1 Retention Policies	57·18
57.1.1 Definitions	57·1	57.4.2 Rotation	57·18
57.1.2 Need	57·3	57.4.3 Media Longevity and Technology Changes	57·18
<b>57.2 MAKING BACKUPS</b>	<b>57·3</b>	<b>57.5 SAFEGUARDING BACKUPS</b>	<b>57·20</b>
57.2.1 Parallel Processing	57·3	57.5.1 Environmental Protection	57·20
57.2.2 Hierarchical Storage Systems	57·3	57.5.2 On-Site Protection	57·20
57.2.3 Disk Mirroring	57·3	57.5.3 Off-Site Protection	57·21
57.2.4 Logging and Recovery	57·6	<b>57.6 DISPOSAL</b>	<b>57·23</b>
57.2.5 Backup Software	57·6	57.6.1 Scavenging	57·23
57.2.6 Removable Media	57·7	57.6.2 Data and Media Destruction	57·24
57.2.7 Labeling	57·10	<b>57.7 COSTS</b>	<b>57·26</b>
57.2.8 Indexing and Archives	57·11	<b>57.8 OPTIMIZING FREQUENCY OF BACKUPS</b>	<b>57·26</b>
<b>57.3 BACKUP STRATEGIES</b>	<b>57·12</b>	<b>57.9 CONCLUDING REMARKS</b>	<b>57·28</b>
57.3.1 Selecting the Backup Technology	57·12	<b>57.10 FURTHER READING</b>	<b>57·28</b>
57.3.2 Exclusive Access	57·13	<b>57.11 NOTES</b>	<b>57·28</b>
57.3.3 Types of Backups	57·13		
57.3.4 Computer Systems	57·15		
57.3.5 Testing	57·17		
<b>57.4 DATA LIFE CYCLE MANAGEMENT</b>	<b>57·17</b>		

**57.1 INTRODUCTION.** Nothing is perfect. Equipment breaks, people make mistakes, and data files become corrupted or disappear. Everyone, and every system, needs a well-thought-out backup and retrieval policy. In addition to making backups, data processing personnel also must consider requirements for archival storage and for retrieval of data copies. Backups also apply to personnel, equipment, and electrical power; for other applications of redundancy, see Chapters 23 and 45 in this *Handbook*.

**57.1.1 Definitions.** *Backups* are copies of data files or records, made at a moment in time, and primarily used in the event of failure of the active files. Normally,

# CHAPTER 58

## BUSINESS CONTINUITY PLANNING

Michael Miora

<b>58.1 INTRODUCTION</b>	<b>58·1</b>		
58.1.1 Enterprise Risks and Costs	58·3	58.3.4 Definition of Departments and Functions	58·18
58.1.2 Types of Disasters	58·4		
58.1.3 Recovery Scenarios	58·6	<b>58.4 BUSINESS IMPACT ANALYSIS MATRIX ANALYSIS</b>	<b>58·25</b>
<b>58.2 DEFINING THE GOALS</b>	<b>58·8</b>	58.4.1 Listing the Functions Organizationally	58·25
58.2.1 Scope	58·9	58.4.2 Finding Cross-Department Functions	58·25
58.2.2 Correlating Objectives to Corporate Missions and Functions	58·10	58.4.3 Using the Ranking Factor	58·27
58.2.3 Validating Goals	58·12	<b>58.5 JUSTIFYING THE COSTS</b>	<b>58·29</b>
58.2.4 Mapping Goals to Recovery Phases	58·13	58.5.1 Quantitative Risk Model	58·29
58.2.5 Emergency Issues	58·14	58.5.2 Generalized Cost Consequence Model	58·31
<b>58.3 PERFORMING A BUSINESS IMPACT ANALYSIS</b>	<b>58·14</b>	<b>58.6 PLAN PRESENTATION</b>	<b>58·34</b>
58.3.1 Establishing the Scope of the Business Impact Analysis	58·15	<b>58.7 CONCLUDING REMARKS</b>	<b>58·36</b>
58.3.2 Interview Process	58·15	<b>58.8 FURTHER READING</b>	<b>58·36</b>
58.3.3 Describing the Functions	58·18		

**58.1 INTRODUCTION.** We are in an age where businesses and governments are turning in increasing numbers to high-technology systems, and to the Internet, to gain and maintain their competitive advantage. Businesses of all types are relying on high-technology products to build, promote, sell, and deliver their wares and services—as are government, educational, and nonprofit enterprises. All of these are dependent on technology to maintain their income, image, and profitability. business continuity planning (BCP) is the process of protecting organizations from the deleterious effects on their missions that can result from outages in information systems.

The goal of BCP is to protect the operations of the enterprise, not just the computing systems. Prudent planning is not restricted to computer or telecommunications systems

# CHAPTER 59

## DISASTER RECOVERY

Michael Miora

<b>59.1 INTRODUCTION</b>	<b>59·1</b>	<b>59.4 DESIGNING RECOVERY TASKS</b>	<b>59·13</b>
<b>59.2 IDENTIFYING THREATS AND DISASTER SCENARIOS</b>	<b>59·1</b>	59.4.1 Beginning Sequence	59·14
59.2.1 Threats	59·2	59.4.2 Middle Sequence	59·16
59.2.2 Disaster Recovery Scenarios	59·3	59.4.3 End Sequence	59·18
<b>59.3 DEVELOPING RECOVERY STRATEGIES</b>	<b>59·6</b>	<b>59.5 IMPLEMENTATION AND READINESS</b>	<b>59·20</b>
59.3.1 Recovery Phases	59·7	<b>59.6 CONCLUDING REMARKS</b>	<b>59·21</b>
59.3.2 Range of Strategies	59·9	<b>59.7 FURTHER READING</b>	<b>59·21</b>
59.3.3 Data Backup Scenarios and Their Meanings	59·13		

**59.1 INTRODUCTION.** In Chapter 58 in this *Handbook*, the importance of a business impact analysis (BIA) and the method of preparing one were described. Once the preliminary groundwork is finished and the BIA analysis is complete, the next step is to design specific strategies for recovery and the tasks for applying those strategies. In this chapter, we discuss the specific strategies to recover the Category I functions, the most time-critical functions identified during the BIA, as well as the remaining lower-priority functions. We examine the traditional strategies of hot sites, warm sites, and cold sites as well as a more modern technique we call reserve systems. We describe how to make good use of Internet and client/server technologies, and of high-speed connections for data backup, for making electronic journals and for data vaulting. We develop the recovery tasks representing the specific activities that must take place to continue functioning, and to resume full operations. These tasks begin with the realization that there is, or may be, a disaster in progress, continue through to full business resumption, and end with normalization, which is the return to normal operations. We examine a set of tasks taken from a real-world disaster recovery plan to illustrate how each task fits into an overall plan, accounting for anticipated contingencies while providing flexibility to handle unforeseen circumstances.

**59.2 IDENTIFYING THREATS AND DISASTER SCENARIOS.** Threat assessment is the foundation for discovery of threats and their possible levels of impact.

# CHAPTER 60

## INSURANCE RELIEF

**Robert A. Parisi, Jr. and Nancy Callahan**

<b>60.1 INTRODUCTION</b>	<b>60·1</b>	60.2.9 Common Exclusions	60·9
60.1.1 Historical Background	60·1	60.2.10 First-Party Coverage and Other Key Provisions	60·9
60.1.2 Growing Recognition of the Need for Insurance	60·2		
60.1.3 General Liability Issues	60·3	<b>60.3 PROPERTY COVERAGE</b>	<b>60·10</b>
<b>60.2 INTELLECTUAL PROPERTY COVERAGE</b>	<b>60·3</b>	<b>60.4 CRIME/FIDELITY COVERAGE</b>	<b>60·11</b>
60.2.1 Loss/Damage to Intangible Assets	60·5	<b>60.5 E-COMMERCE POLICIES</b>	<b>60·12</b>
60.2.2 Intellectual Property Policies	60·6	<b>60.6 PRIVACY AND IDENTITY THEFT EXPOSURES</b>	<b>60·13</b>
60.2.3 Claims Made versus Occurrence Coverages	60·6	60.6.1 Issues for Businesses	60·13
60.2.4 Duty to Defend versus Indemnity	60·7	60.6.2 Issues for Consumers	60·18
60.2.5 Who Is Insured?	60·8	60.6.3 Insurance for Consumers	60·18
60.2.6 Definitions of Covered Claims	60·8	<b>60.7 CONCLUDING REMARKS</b>	<b>60·18</b>
60.2.7 Prior Acts Coverage	60·8	<b>60.8 FURTHER READING</b>	<b>60·19</b>
60.2.8 Extensions of Coverage	60·9	<b>60.9 NOTES</b>	<b>60·19</b>

**60.1 INTRODUCTION.** This chapter presents an overview of traditional insurance products and discusses how they may or may not provide coverage for the risks associated with intellectual property and with computer and network security. It also addresses the new types of coverage that have been developed expressly for those risks.

**60.1.1 Historical Background.** Historically, people have responded to the risks associated with commerce by finding ways to lessen their impact or severity.

- Around 3000 BCE, Chinese merchants cooperated by distributing cargo among several ships prior to navigating dangerous waterways, so that the loss of one ship would not cause a total loss to any individual.

# CHAPTER 61

## WORKING WITH LAW ENFORCEMENT

**David A. Land**

<b>61.1</b>	<b>INTRODUCTION</b>	<b>61·1</b>	<b>61.8</b>	<b>THE KNOCK AT THE DOOR</b>	<b>61·7</b>
<b>61.2</b>	<b>RELEVANT LAWS</b>	<b>61·2</b>			
<b>61.3</b>	<b>PLAN AHEAD</b>	<b>61·2</b>	<b>61.9</b>	<b>KEEPING YOUR OPERATION RUNNING DURING AN INVESTIGATION</b>	<b>61·8</b>
	61.3.1 Federal Bureau of Investigation	61·3			
	61.3.2 U.S. Postal Inspection Service	61·5	<b>61.10</b>	<b>NONELECTRONIC RECORDS AND THE INSIDER THREAT</b>	<b>61·9</b>
	61.3.3 U.S. Secret Service	61·5			
<b>61.4</b>	<b>MEMORANDUM OF AGREEMENT</b>	<b>61·5</b>	<b>61.11</b>	<b>INFORMATION SHARING (THE HUMAN FACTOR)</b>	<b>61·10</b>
<b>61.5</b>	<b>HANDLING EVIDENCE AND THE CHAIN OF CUSTODY</b>	<b>61·6</b>	<b>61.12</b>	<b>CONCLUSION</b>	<b>61·13</b>
<b>61.6</b>	<b>ISSUES OF LIABILITY</b>	<b>61·7</b>	<b>61.13</b>	<b>FURTHER READING</b>	<b>61·13</b>
<b>61.7</b>	<b>ASK LAW ENFORCEMENT TO GIVE BACK</b>	<b>61·7</b>	<b>61.14</b>	<b>NOTES</b>	<b>61·14</b>

**61.1 INTRODUCTION.** Today, working with law enforcement is likely one of the most important aspects of computer security, and of our collective need to protect our sites and our sites' information. The entire paradigm has shifted to one where you will need law enforcement, and they will most certainly need you. In times past, however, this was not the case. Understanding their needs before, during, and after the commission of a crime significantly enhances your organization's opportunity to come back online quickly, with, it is hoped, little or no disturbance to your users or customers. Likewise, conveying your needs to law enforcement prior to an incident will serve you well later on. Working with law enforcement is, however, not your opportunity to assume the role of law enforcement. You must know your limitations and at what point to engage your law enforcement contacts.

## INTRODUCTION TO PART VII

# MANAGEMENT'S ROLE IN SECURITY

Management responsibilities include judgements of which resources can rationally be expended in defending against which threats. Managers must understand how to cope with the lack of quantitative risk estimates while using what information is available to guide investment decisions in personnel and technology. Their decisions are affected by regulatory and legal requirements and by the practical constraints of their relationships with other leaders within their organizations. This part includes chapters and topics that bear on information assurance managers' roles:

- 62. Risk Assessment and Risk Management.** Which vulnerabilities warrant repair? Which threats must be taken seriously? How much expense is justified on specific security measures?
- 63. Management Responsibilities and Liabilities.** Roles, responsibilities, due diligence, staffing security functions, and the value of accreditation and education
- 64. U.S. Legal and Regulatory Security Issues.** For U.S. practitioners especially, this chapter reviews the Gramm-Leach-Bliley Act and the Sarbanes-Oxley legislation
- 65. The Role of the CISO.** The chief information security officer as an agent of change and as a strategist working to ensure that security fits into the strategic mission of the organization, and that it is communicated effectively to other C-level executives
- 66. Developing Security Policies.** Approaches to creating a culture of security where policies grow organically from the commitment of all sectors of the organization, instead of being imposed unilaterally by security staff
- 67. Developing Classification Policies for Data.** The essential role of data classification and how to implement systems that conform to regulatory and legal requirements
- 68. Outsourcing and Security.** Security of outsourcing and outsourcing of security

# CHAPTER 62

## RISK ASSESSMENT AND RISK MANAGEMENT

Robert V. Jacobson

<b>62.1 INTRODUCTION TO RISK MANAGEMENT</b>	<b>62·1</b>		
62.1.1 What Is Risk?	62·1		
62.1.2 What Is Risk Management?	62·2		
62.1.3 Applicable Standards	62·3		
62.1.4 Regulatory Compliance and Legal Issues	62·4		
<b>62.2 OBJECTIVE OF A RISK ASSESSMENT</b>	<b>62·5</b>		
<b>62.3 LIMITATIONS OF QUESTIONNAIRES IN ASSESSING RISKS</b>	<b>62·6</b>		
<b>62.4 MODEL OF RISK</b>	<b>62·7</b>		
62.4.1 Two Inconsequential Risk Classes	62·7		
62.4.2 Two Significant Risk Classes	62·7		
62.4.3 Spectrum of Real-World Risks	62·8		
<b>62.5 RISK MITIGATION</b>	<b>62·10</b>		
62.5.1 ALE Estimates Alone Are Insufficient	62·10		
62.5.2 What a Wise Risk Manager Tries to Do	62·11		
62.5.3 How to Mitigate Infrequent Risks	62·14		
62.5.4 ROI-Based Selection Process	62·15		
62.5.5 Risk Assessment/ Risk Management Summary	62·16		
<b>62.6 RISK ASSESSMENT TECHNIQUES</b>	<b>62·16</b>		
62.6.1 Aggregating Threats and Loss Potentials	62·17		
62.6.2 Basic Risk Assessment Algorithms	62·17		
62.6.3 Loss Potential	62·18		
62.6.4 Risk Event Parameters	62·22		
62.6.5 Threat Effect Factors, ALE, and SOL Estimates	62·22		
62.6.6 Sensitivity Testing	62·23		
62.6.7 Selecting Risk Mitigation Measures	62·24		
<b>62.7 SUMMARY</b>	<b>62·24</b>		
<b>62.8 FURTHER READING</b>	<b>62·24</b>		
<b>62.9 NOTES</b>	<b>62·25</b>		

### 62.1 INTRODUCTION TO RISK MANAGEMENT

**62.1.1 What Is Risk?** There is general agreement in the computer security community with the common dictionary definition: “the possibility of suffering harm or loss.” The definition shows that there are two parts to risk: the *possibility* that

# CHAPTER 63

## MANAGEMENT RESPONSIBILITIES AND LIABILITIES

**Carl Hallberg, M. E. Kabay,  
Bridgitt Robertson, and Arthur E. Hutt**

<b>63.1 INTRODUCTION</b>	<b>63·1</b>	63.3.3 Downstream Liability	63·21
63.1.1 Role of Management	63·2	63.3.4 Audits	63·22
63.1.2 CISO	63·2		
63.1.3 Information Security Integrating into Strategic Vision	63·4	<b>63.4 COMPUTER MANAGEMENT FUNCTIONS</b>	<b>63·23</b>
63.1.4 Net Present Value of Information Security	63·5	63.4.1 Planning for Computer Security	63·23
63.1.5 Case Study: Veterans Affairs	63·6	63.4.2 Organizing	63·24
		63.4.3 Integrating	63·24
		63.4.4 Controlling	63·25
<b>63.2 RESPONSIBILITIES</b>	<b>63·10</b>	<b>63.5 SECURITY ADMINISTRATION</b>	<b>63·26</b>
63.2.1 Policy Management	63·12	63.5.1 Staffing the Security Function	63·26
63.2.2 Motivation	63·12	63.5.2 Authority and Responsibility	63·26
63.2.3 Supervision	63·14	63.5.3 Professional Accreditation and Education	63·28
63.2.4 Judgment and Adaptation	63·15		
63.2.5 Management Failures	63·16	<b>63.6 CONCLUDING REMARKS</b>	<b>63·29</b>
63.2.6 Risk Management	63·18	<b>63.7 FURTHER READING</b>	<b>63·29</b>
<b>63.3 LIABILITIES</b>	<b>63·19</b>	<b>63.8 NOTES</b>	<b>63·29</b>
63.3.1 Stakeholders	63·20		
63.3.2 Due Diligence of Care	63·20		

**63.1 INTRODUCTION.** This chapter reviews the critical roles of management in establishing, implementing, and maintaining information security policies in the modern enterprise. It also reviews some of the risks to management personnel in failing to ensure adequate standards of information security.<sup>1</sup>



# CHAPTER 64

## U.S. LEGAL AND REGULATORY SECURITY ISSUES

Timothy Virtue

<b>64.1 INTRODUCTION</b>	<b>64·1</b>	64.3.6 GLBA Safeguards Rule	64·10
<b>64.2 SARBANES-OXLEY ACT OF 2002</b>	<b>64·2</b>	64.3.7 Flexibility	64·10
64.2.1 Section 404 of SOX	64·4	<b>64.4 EXAMINATION PROCEDURES TO EVALUATE COMPLIANCE WITH GUIDELINES FOR SAFEGUARDING CUSTOMER INFORMATION</b>	<b>64·11</b>
64.2.2 Management Perspectives on SOX	64·5	<b>64.5 CONCLUDING REMARKS</b>	<b>64·11</b>
<b>64.3 GRAMM-LEACH-BLILEY ACT</b>	<b>64·6</b>	<b>64.6 FURTHER READING</b>	<b>64·15</b>
64.3.1 Applicability	64·6	<b>64.7 NOTES</b>	<b>64·15</b>
64.3.2 Enforcement	64·7		
64.3.3 Consumers and Customers	64·8		
64.3.4 Compliance	64·9		
64.3.5 Privacy Notices	64·9		

**64.1 INTRODUCTION.** The regulatory requirements facing today's business leaders can strengthen the overall business environment while offering increased safeguards to stakeholders such as consumers, suppliers, shareholders, employees, and other interested parties transacting with today's businesses. Although regulatory requirements vary from institution to institution and across different industries, the recurring theme is that management must be proactively involved and fully accountable for the actions of its organization.

Compliance is an ongoing process that can be achieved successfully only when the organization's senior leaders support compliance from both a cultural and operational perspective. In other words, the right attitudes (integrity, honesty, transparency, etc.), also known as *tone at the top*, must be exemplified in all facets of the organization while working in tandem with operational processes to create a comprehensive compliance environment. A culture of compliance must be integrated throughout the organization and must be seamlessly built into all operational facets of the business.

Many organizations are restructuring independent and isolated operational units (sometimes described as *silos*) and focusing on coordinated strategic risk management

# CHAPTER 65

## ROLE OF THE CISO

**Karen F. Worstell**

<b>65.1 CISO AS CHANGE AGENT</b>	<b>65 · 1</b>	<b>65.5 RECOMMENDATIONS FOR SUCCESS FOR CISOs</b>	<b>65 · 14</b>
<b>65.2 CISO AS STRATEGIST</b>	<b>65 · 3</b>	65.5.1 Education and Experience	65 · 14
65.2.1 Reliance on Digital Information	65 · 4	65.5.2 “Culture” of Security in the Business	65 · 15
65.2.2 Inherent Insecurity of Systems	65 · 5	65.5.3 Alliance with Corporate and Outside Counsel	65 · 16
65.2.3 World Trends	65 · 5	65.5.4 Partnership with Internal Audit	65 · 16
<b>65.3 STRATEGY, GOVERNANCE, AND THE STANDARD OF CARE</b>	<b>65 · 6</b>	65.5.5 Tension with IT	65 · 17
65.3.1 Standard of Care	65 · 6	65.5.6 Organizational Structure	65 · 17
65.3.2 Governance and Accountability	65 · 9	65.5.7 Responsibilities and Opportunities outside of CISO Internal Responsibilities	65 · 18
65.3.3 Roles and Responsibilities	65 · 11	<b>65.6 CONCLUDING REMARKS</b>	<b>65 · 18</b>
65.3.4 Reporting	65 · 12	<b>65.7 NOTES</b>	<b>65 · 19</b>
65.3.5 Monitoring	65 · 13		
65.3.6 Metrics	65 · 13		
65.3.7 Executive Visibility	65 · 13		
<b>65.4 SUMMARY OF ACTIONS</b>	<b>65 · 13</b>		

**65.1 CISO AS CHANGE AGENT.** The title of chief information security officer (CISO) has evolved because of the realization that the function of the chief information officer (CIO) is so broad as to require another person to focus specifically on the *security* elements of information. Another motivation derives from the fact that the CISO can perform functions that are not usually associated with the CIO. Our approach to information security needs to change in response to the disruptive events affecting the network and the boardroom. CISOs should be the change agents to make this happen. This is a shift from the majority of CISOs’ emphasis today as senior managers of information technology (IT) security.

Today, CISOs are in the trust business due to the need to create and maintain a network of trust among all the people, business processes, and technology of an enterprise and its partners. The interconnected ecosystem that developed since the commercialization of the Internet has seen dramatic shifts of trust: Consumers are thinking twice

# CHAPTER 66

## DEVELOPING SECURITY POLICIES

M. E. Kabay and Sean Kelley

<b>66.1 INTRODUCTION</b>	<b>66·1</b>	66.3.14 Antimalware Measures	66·10
<b>66.2 COLLABORATING IN BUILDING SECURITY POLICIES</b>	<b>66·2</b>	66.3.15 Backups, Archives, and Data Destruction	66·10
<b>66.3 PHASE 1: PRELIMINARY EVALUATION</b>	<b>66·2</b>	66.3.16 Incident Response	66·10
66.3.1 Introduction to the Study	66·4	66.3.17 Business Resumption Planning and Disaster Recovery	66·11
66.3.2 State of Current Policy	66·4	<b>66.4 PHASE 2: MANAGEMENT SENSITIZATION</b>	<b>66·11</b>
66.3.3 Data Classification	66·5	<b>66.5 PHASE 3: NEEDS ANALYSIS</b>	<b>66·12</b>
66.3.4 Sensitive Systems	66·5	<b>66.6 PHASE 4: POLICIES AND PROCEDURES</b>	<b>66·12</b>
66.3.5 Critical Systems	66·5	<b>66.7 PHASE 5: IMPLEMENTATION</b>	<b>66·12</b>
66.3.6 Authenticity	66·5	66.7.1 Upper Management	66·13
66.3.7 Exposure	66·6	66.7.2 Technical Support	66·13
66.3.8 Human Resources, Management, and Employee Security Awareness	66·6	66.7.3 Lower-Level Staff	66·13
66.3.9 Physical Security	66·6	66.7.4 Other Technical Staff	66·14
66.3.10 Software Development Security	66·7	<b>66.8 PHASE 6: MAINTENANCE</b>	<b>66·14</b>
66.3.11 Computer Operations Security	66·8	<b>66.9 CONCLUDING REMARKS</b>	<b>66·14</b>
66.3.12 Data Access Controls	66·8	<b>66.10 NOTES</b>	<b>66·14</b>
66.3.13 Network and Communications Security	66·9		

**66.1 INTRODUCTION.** This chapter reviews methods for developing security policies in specific organizations. Some of the other chapters of this *Handbook* that bear on policy content, development, and implementation are listed next:

- Chapter 23 provides an extensive overview of physical security policies.
- Chapter 25 discusses local area network security issues and policies.
- Chapter 39 reviews software development policies and quality assurance policies.

# CHAPTER 67

## DEVELOPING CLASSIFICATION POLICIES FOR DATA

Karthik Raman and Kevin Beets

<b>67.1 INTRODUCTION</b>	<b>67·1</b>	67.4.3 Compliance Standards	67·5
<b>67.2 WHY DATA CLASSIFICATION IS PERFORMED</b>	<b>67·2</b>	67.4.4 Other Standards	67·6
<b>67.3 DATA CLASSIFICATION'S ROLE IN INFORMATION SECURITY</b>	<b>67·2</b>	<b>67.5 DESIGNING AND IMPLEMENTING DC</b>	<b>67·7</b>
<b>67.4 LEGAL REQUIREMENTS, COMPLIANCE STANDARDS, AND DATA CLASSIFICATION</b>	<b>67·3</b>	67.5.1 Data Classification Solutions	67·7
67.4.1 Legal Requirements	67·3	67.5.2 Examples of Data Classification Schemas	67·8
67.4.2 Family Educational Rights and Privacy Act	67·3	<b>67.6 CONCLUDING REMARKS</b>	<b>67·9</b>
		<b>67.7 NOTES</b>	<b>67·10</b>

**67.1 INTRODUCTION.** A figure appears from the bushes on a dark and stormy night and silently slips past two guards. Inside the building, a flashlight flickers to life and begins a slow dance around a cluttered office. The beam freezes. It illuminates an envelope that is stamped with large red letters: “TOP SECRET.”

The top secret label is likely the most popularly recognized part of an example of a data classification (DC) scheme. DC labels information so that its custodians and users can comply with established data protection policies when organizing, viewing, editing, valuing, protecting, and storing data.

Historically, DC has been used by the government and military. Today, however, it has increasingly become a necessity for businesses because of the competitive value of information, because of the legal requirements for maintenance of sound financial and operational records, and because of the demands of privacy-protection laws.

This chapter explains why DC is necessary, how it relates to information security, common laws and standards associated with DC, its design and implementation in an enterprise, hardware and software solutions that can assist in performing DC, and some practical recommendations to consider when implementing DC.

# CHAPTER 68

## OUTSOURCING AND SECURITY

**Kip Boyle, Michael Buglewicz, and  
Steven Lovaas**

<b>68.1 INTRODUCTION</b>	<b>68·1</b>		
68.1.1 Definitions	68·2	68.4.2 Controlling Outsourcing Risk	68·12
68.1.2 Distinctions	68·3	68.4.3 Availability Controls	68·12
68.1.3 Insourcing	68·3	68.4.4 Utility Controls	68·13
68.1.4 Nearshoring	68·4	68.4.5 Integrity and Authenticity Controls	68·13
68.1.5 Offshoring	68·4	68.4.6 Confidentiality and Possession Controls	68·14
<b>68.2 WHY OUTSOURCE?</b>	<b>68·4</b>	68.4.7 Making the Best of Outsourcing	68·15
68.2.1 Effectiveness versus Efficiency	68·5		
68.2.2 Being Effective	68·5	<b>68.5 OUTSOURCING SECURITY FUNCTIONS</b>	<b>68·15</b>
68.2.3 Being Efficient	68·5	68.5.1 Who Outsources Security?	68·15
<b>68.3 CAN OUTSOURCING FAIL?</b>	<b>68·6</b>	68.5.2 Why Do Organizations Outsource Security?	68·15
68.3.1 Why Does Outsourcing Fail?	68·7	68.5.3 What Are the Risks of Outsourcing Security?	68·18
68.3.2 Universal Nature of Risk	68·7	68.5.4 How to Outsource Security Functions	68·18
68.3.3 Clarity of Purpose and Intent	68·8	68.5.5 Controlling the Risk of Security Outsourcing	68·21
68.3.4 Price	68·9	<b>68.6 CONCLUDING REMARKS</b>	<b>68·21</b>
68.3.5 Social Culture	68·9	<b>68.7 FURTHER READING</b>	<b>68·22</b>
68.3.6 International Economics	68·9	<b>68.8 NOTES</b>	<b>68·22</b>
68.3.7 Political Issues	68·10		
68.3.8 Environmental Factors	68·10		
68.3.9 Travel	68·10		
68.3.10 Labor	68·11		
68.3.11 Additional Risks	68·11		
<b>68.4 CONTROLLING THE RISKS</b>	<b>68·12</b>		
68.4.1 Controls on What?	68·12		

**68.1 INTRODUCTION.** The term “outsourcing” has come to identify several distinct concepts, each requiring a different risk management strategy. In this chapter,

## INTRODUCTION TO PART VIII

# PUBLIC POLICY AND OTHER CONSIDERATIONS

This edition of the *Handbook* ends with compelling issues in information security. Part VIII provides a basis for vigorous discussion about important and controversial topics such as:

69. **Privacy in Cyberspace: U.S. and European Perspectives.** With increasingly frequent losses of control over personally identifiable information, the public is ever more concerned about privacy
70. **Anonymity and Identity in Cyberspace.** How individuals are representing themselves in Internet-mediated communications; the social and legal consequences of completely anonymous interactions, and of untraceable but stable identifiers
71. **Medical Records Protection.** How the special requirements of high availability coupled with extreme sensitivity of medical information poses complex problems for security specialists in medical environments
72. **Legal and Policy Issues of Censorship and Content Filtering.** How corporations and governments around the world regulate access to information that violates social norms, or is perceived as a potential threat to state power
73. **Expert Witnesses and the *Daubert* Challenge.** How security specialists should prepare for their day in court
74. **Professional Certification and Training in Information Assurance.** Benefits and costs of education, professional certifications, examinations, and commercial training
75. **U.S. Undergraduate and Graduate Education in Information Assurance.** Initiatives in the United States have added information assurance to the curriculum of many programs at institutions of higher learning
76. **Undergraduate and Graduate Education in Information Assurance.** Perspectives on information assurance education at the baccalaureate and advanced levels in Europe and the United States
77. **The Future of Information Assurance.** A giant in the field of information assurance reviews the foundations of IA, best practices, and risk reduction and applies his expertise to computer-aided voting as a case study in applied security

# CHAPTER 69

## PRIVACY IN CYBERSPACE: U.S. AND EUROPEAN PERSPECTIVES

Henry L. Judy, Scott L. David, Benjamin S. Hayes, Jeffrey B. Ritter, and Marc Rotenberg

<b>69.1</b>	<b>INTRODUCTION: WORLDWIDE TRENDS</b>	<b>69·2</b>	<b>69.3</b>	<b>UNITED STATES</b>	<b>69·6</b>	
	69.1.1	Laws, Regulations, and Agreements	69·2	69.3.1	History, Common Law Torts	69·6
	69.1.2	Sources of Privacy Law	69·3	69.3.2	Public Sector	69·7
				69.3.3	Private Sector	69·9
				69.3.4	State Legislation	69·17
<b>69.2</b>	<b>EUROPEAN APPROACHES TO PRIVACY</b>	<b>69·3</b>	<b>69.4</b>	<b>COMPLIANCE MODELS</b>	<b>69·17</b>	
	69.2.1	History and Organization for Economic Cooperation and Development Principles	69·3	69.4.1	U.S. Legislation	69·18
	69.2.2	European Union Data Protection Directive 95/46/EC	69·4	69.4.2	U.S. Federal Trade Commission Section 5 Authority	69·18
	69.2.3	Harmonization of Non–EU European Countries to the EU Directive	69·6	69.4.3	Self-Regulatory Regimes and Codes of Conduct	69·18
	69.2.4	European Union Telecommunica- tions Directive	69·6	69.4.4	Contract Infrastructure	69·18
	69.2.5	Establishment of the European Data Protection Supervisor	69·6	69.4.5	Synthesis of Contracts, Technology, and Law	69·19
			<b>69.5</b>	<b>FURTHER READING</b>	<b>69·20</b>	
			<b>69.6</b>	<b>NOTES</b>	<b>69·21</b>	

# CHAPTER 70

## ANONYMITY AND IDENTITY IN CYBERSPACE

**M. E. Kabay, Eric Salveggio, and  
Robert Guess**

<b>70.1</b>	<b>INTRODUCTION</b>	<b>70·1</b>	<b>70.5</b>	<b>SYSTEMS ANALYSIS OF ANONYMITY</b>	<b>70·15</b>
<b>70.2</b>	<b>DEFINITIONS</b>	<b>70·3</b>	<b>70.6</b>	<b>IMPLICATIONS AND DISCUSSION</b>	<b>70·16</b>
	70.2.1 Cyberspace	70·4		70.6.1 Individuals, Families, and Schools	70·16
	70.2.2 The Real World	70·4		70.6.2 Ethical Principles	70·16
	70.2.3 Identity in the Real World	70·4		70.6.3 Corporations and Other Organizations	70·18
	70.2.4 Anonymity and Pseudonymity in the Real World	70·4		70.6.4 Internet Service Providers	70·18
<b>70.3</b>	<b>SOCIAL PSYCHOLOGY OF ANONYMITY</b>	<b>70·5</b>		70.6.5 A Free Market Model for Identity in Cyberspace	70·19
	70.3.1 Deindividuation Theory	70·5		70.6.6 Governments	70·20
	70.3.2 Identity in Cyberspace	70·8	<b>70.7</b>	<b>CONCLUDING REMARKS</b>	<b>70·21</b>
<b>70.4</b>	<b>BALANCING RIGHTS AND DUTIES</b>	<b>70·10</b>	<b>70.8</b>	<b>SUMMARY</b>	<b>70·21</b>
	70.4.1 Benefits of Anonymity and Pseudonymity	70·10	<b>70.9</b>	<b>FURTHER READING</b>	<b>70·22</b>
	70.4.2 Privacy and Freedom in Virtual Worlds	70·12	<b>70.10</b>	<b>NOTES</b>	<b>70·22</b>
	70.4.3 Disadvantages of Anonymity and Pseudonymity	70·13			

**70.1 INTRODUCTION.** As electronic communications technology becomes widespread among increasingly international populations of computer users, one of the most hotly debated questions is how to maintain the benefits of free discourse while simultaneously restricting antisocial communications and behavior on the Net. The debate is complicated by the international and intercultural dimensions of



# CHAPTER 71

## MEDICAL RECORDS PROTECTION

**Paul J. Brusil**

<b>71.1 INTRODUCTION</b>	<b>71·1</b>	71.4.3 Patient Expectations	71·7
<b>71.2 INFORMATION AND INFORMATION TECHNOLOGY IN HEALTHCARE</b>	<b>71·2</b>	<b>71.5 UNITED STATES LAWS AND GOVERNMENT POLICIES</b>	<b>71·8</b>
71.2.1 Medical Record Information Is Key to Healthcare	71·2	71.5.1 Federal Laws	71·8
71.2.2 Role of IT in Healthcare	71·3	71.5.2 State Privacy and Security Laws	71·9
<b>71.3 INFORMATION PRIVACY AND SECURITY ARE IMPORTANT IN HEALTHCARE</b>	<b>71·3</b>	71.5.3 Government Policies	71·9
71.3.1 Increasing Healthcare Information Technology Risks and Vulnerabilities	71·4	71.5.4 Emerging Legislation	71·10
71.3.2 Healthcare Information Privacy and Security Needs and Challenges	71·5	<b>71.6 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT</b>	<b>71·11</b>
71.3.3 Core Privacy and Security Model in Healthcare	71·6	71.6.1 HIPAA Administrative Simplification Overview	71·12
<b>71.4 NONMEDICAL DRIVERS FOR HEALTHCARE INFORMATION PROTECTION</b>	<b>71·7</b>	71.6.2 Privacy and Security Strategy	71·13
71.4.1 Political Pressure	71·7	71.6.3 Privacy Regulations	71·15
71.4.2 Public Pressure and Media Pressure	71·7	71.6.4 Security Regulations	71·17
		71.6.5 Enforcement, Penalties, and Liabilities	71·19
		71.6.6 Realities in Fielding HIPAA Information Protection Regulations	71·20
		<b>71.7 SUMMARY</b>	<b>71·26</b>
		<b>71.8 FURTHER READING</b>	<b>71·27</b>
		<b>71.9 NOTES</b>	<b>71·27</b>

**71.1 INTRODUCTION.** U.S. regulatory compliance forces increased attention on information protection. Regulations such as SOX 404 (Sarbanes-Oxley), FISMA (Federal Information System Management Act), GLB (Gramm-Leach Bliley), HIPAA (Health Insurance Portability and Accountability Act), and others are establishing

# CHAPTER 72

## LEGAL AND POLICY ISSUES OF CENSORSHIP AND CONTENT FILTERING

Lee Tien, Seth Finkelstein, and  
Steven Lovaas

<b>72.1 INTRODUCTION</b>	<b>72·1</b>		
72.1.1 Scope of This Chapter: Government Intervention	72·2	72.2.4 Exceptions Where Speech Can Legally Be Limited	72·10
72.1.2 Whose Laws? Whose Standards?	72·2	72.2.5 Legislation and Legislative Initiatives in the United States	72·14
72.1.3 Defining Objectionable Material: International Differences	72·3	72.2.6 Attempts to Control Access: Case Law	72·15
<b>72.2 U.S. CONTEXT: FIRST AMENDMENT RIGHTS</b>	<b>72·7</b>	<b>72.3 PARENTAL INVOLVEMENT/RESPONSIBILITY</b>	<b>72·17</b>
72.2.1 What Does the First Amendment Protect?	72·8	<b>72.4 SUMMARY</b>	<b>72·17</b>
72.2.2 Basic First Amendment Principles	72·8	<b>72.5 FURTHER READING</b>	<b>72·18</b>
72.2.3 Limitations on Government		<b>72.6 NOTES</b>	<b>72·18</b>

### 72.1 INTRODUCTION

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.<sup>1</sup>

One might think that the Internet will make this ringing proclamation a reality. Like no other technology, the Internet transcends national borders and eliminates barriers to the free flow of information. Governments, however, are trying to control speech on the Internet.

# CHAPTER 73

## EXPERT WITNESSES AND THE DAUBERT CHALLENGE

### Chey Cobb

<b>73.1 INTRODUCTION</b>	<b>73·1</b>	73.5.1 Prepare Your Résumé	73·4
<b>73.2 DAUBERT</b>	<b>73·2</b>	73.5.2 Find Out Exactly What Testimony Is Expected	73·5
73.2.1 Expert Witnesses’ Testimony	73·2	73.5.3 Examine the Paperwork	73·5
73.2.2 <i>Daubert</i> Challenge	73·3	73.5.4 Start Reading	73·5
<b>73.3 WHETHER THE DAUBERT CHALLENGE IS APPLICABLE: REFINING DAUBERT</b>	<b>73·3</b>	73.5.5 Prepare a Written Report	73·5
73.3.1 General Electric Co. v. Joiner	73·3	73.5.6 Ask for Pretrial Meetings	73·6
73.3.2 <i>Kumho Tire Co. v. Carmichael</i>	73·3	73.5.7 Be Professional	73·6
		73.5.8 Accept the Oddities	73·6
<b>73.4 DIVIDED WE FALL?</b>	<b>73·3</b>	<b>73.6 SUMMARY</b>	<b>73·6</b>
<b>73.5 BEING THE BEST YOU CAN BE</b>	<b>73·4</b>	<b>73.7 FURTHER READING</b>	<b>73·6</b>
		<b>73.8 NOTES</b>	<b>73·7</b>

**73.1 INTRODUCTION.** Whenever science or technology enters the courtroom, there must surely be an expert who can give clear and proper explanations of the subject matter to the judge and jury. As new sciences and technologies have emerged, the courts have had to decide if a person is, indeed, an expert and whether or not the science is real and admissible.<sup>1</sup>

In 1923, the United States courts began accepting scientific evidence based on a new rule. That rule used the “general acceptance” test to determine if evidence was legitimate. This test was based on the rulings in *Frye v. United States*, which declared that if a scientific practice was generally accepted among the scientific community in which it was practiced, it could be admitted in court. This has become generally referred to as the *Frye test*.<sup>2</sup>

In 1975, the federal government made the scientific assertions a bit stronger by issuing the Federal Rules of Evidence No. 702 (FRE 702), which states in part:

# CHAPTER 74

## PROFESSIONAL CERTIFICATION AND TRAINING IN INFORMATION ASSURANCE

**Christopher Christian, M. E. Kabay,  
Kevin Henry, and Sondra Schneider**

<b>74.1 BUILDING SKILLS THROUGH PROFESSIONAL EDUCATION</b>	<b>74·1</b>		
74.1.1 Training and Education	74·2		
74.1.2 Certificates, Certification, and Accreditation	74·3		
74.1.3 ANSI/ISO/IEC 17024 Accreditation of Personnel Certification	74·3		
74.1.4 NOCA/NCCA	74·4		
74.1.5 IACE	74·4		
74.1.6 Summary of Accreditation, Certification, and Certificates	74·5		
<b>74.2 INFORMATION SECURITY CERTIFICATIONS</b>	<b>74·5</b>		
74.2.1 Certified Internal Auditor (CIA)	74·7		
74.2.2 Certified Information Systems Auditor (CISA)	74·9		
74.2.3 Certified Information Security Manager (CISM)	74·10		
74.2.4 Certified Information Systems Security Professionals (CISSP)	74·12		
74.2.5 Systems Security Certified Practitioner (SSCP)	74·14		
74.2.6 Global Information Assurance Certification	74·15		
<b>74.3 PREPARING FOR SECURITY CERTIFICATION EXAMINATIONS</b>	<b>74·16</b>		
74.3.1 Newsletters	74·16		
74.3.2 Web Sites	74·17		
74.3.3 CCCure.org	74·18		
74.3.4 Books and Free Review Materials	74·19		
<b>74.4 COMMERCIAL TRAINING IN INFORMATION ASSURANCE</b>	<b>74·20</b>		
74.4.1 Security University Classes and Certifications	74·20		
74.4.2 Getronics Security University	74·22		
74.4.3 CEH Franchise	74·23		
<b>74.5 CONCLUDING REMARKS</b>	<b>74·24</b>		
<b>74.6 NOTES</b>	<b>74·24</b>		

**74.1 BUILDING SKILLS THROUGH PROFESSIONAL EDUCATION.** Perhaps one of the most critical decisions an organization has to make today is how to invest in its staff. Technology, policies, and well-defined processes are all important

# CHAPTER 75

## UNDERGRADUATE AND GRADUATE EDUCATION IN INFORMATION ASSURANCE

Vic Maconachy and Seymour Bosworth

<b>75.1 INTRODUCTION</b>	<b>75·1</b>	<b>75.3 DISTANCE LEARNING IN HIGHER EDUCATION</b>	<b>75·9</b>
		75.3.1 Media	75·9
		75.3.2 Students	75·9
		75.3.3 Teachers	75·10
		75.3.4 Providers	75·10
		75.3.5 Courses	75·11
		75.3.6 Summary	75·11
<b>75.2 U.S. INITIATIVES IN TRAINING AND EDUCATION OF INFORMATION</b>	<b>75·1</b>	<b>75.4 BUSINESS CONTINUITY MANAGEMENT</b>	<b>75·12</b>
75.2.1 TIE System	75·1	<b>75.5 CONCLUDING REMARKS</b>	<b>75·12</b>
75.2.2 Growth of IA Education Programs in the United States	75·4	<b>75.6 NOTES</b>	<b>75·12</b>
75.2.3 Information Assurance as Part of a Learning Continuum	75·5		
75.2.4 Time to Respond	75·8		

**75.1 INTRODUCTION.** Information assurance has come to the forefront of the consciousness of the modern world. Recent events such as high-publicity breaches of security, as well as pervasive small-scale abuses of the technologies available at work and at home, have highlighted the need for trained professionals able to operate in the complex world of information assurance. Toward this end, recent initiatives in the United States and Europe have added information assurance into the undergraduate and graduate curriculum of more common degrees such as computer science, and have also identified information assurance as its own discipline worthy of its own curriculum. This chapter outlines some of the initiatives that have taken place in the United States and speculates about the future of the discipline.

### **75.2 U.S. INITIATIVES IN TRAINING AND EDUCATION OF INFORMATION ASSURANCE**

**75.2.1 TIE System.** Any approach to information assurance (IA) education must be presented in a conceptual context. The Trusted Information Environment

# CHAPTER 76

## EUROPEAN GRADUATE WORK IN INFORMATION ASSURANCE AND THE BOLOGNA DECLARATION<sup>1</sup>

**Urs E. Gattiker**

<b>76.1</b>	<b>UNDERGRADUATE AND GRADUATE EDUCATION</b>	<b>76·2</b>	<b>76.9</b>	<b>WHAT DO PROGRAMS IN INFORMATION SECURITY TEACH STUDENTS?</b>	<b>76·10</b>
<b>76.2</b>	<b>CONVERGENCE OF EDUCATIONAL PROGRAMS</b>	<b>76·2</b>	<b>76.10</b>	<b>UNDERGRADUATE EDUCATION: POLYTECHNICS AND UNIVERSITY</b>	<b>76·11</b>
<b>76.3</b>	<b>BACHELOR'S AND MASTER'S IN INFORMATION SECURITY</b>	<b>76·3</b>	<b>76.11</b>	<b>INFORMATION ASSURANCE: DEFINING THE TERRITORY</b>	<b>76·11</b>
<b>76.4</b>	<b>COMPUTER SCIENCE: DOES IT ENCOMPASS INFORMATION SECURITY, ASSURANCE, AND SECURITY ASSURANCE?</b>	<b>76·3</b>	<b>76.12</b>	<b>TEACHING INFORMATION SECURITY: THE MALWARE EXAMPLE</b>	<b>76·13</b>
<b>76.5</b>	<b>BOLOGNA BACHELOR'S DEGREE</b>	<b>76·4</b>	<b>76.13</b>	<b>CONCLUSION OF EUROPEAN INITIATIVES OVERVIEW</b>	<b>76·13</b>
<b>76.6</b>	<b>MOVING FROM UNDERGRADUATE TO GRADUATE EDUCATION: BOLOGNA</b>	<b>76·5</b>	<b>76.14</b>	<b>IMPLICATIONS FOR EDUCATION</b>	<b>76·15</b>
<b>76.7</b>	<b>EXECUTIVE AND SPECIALIZED MASTER'S DEGREES</b>	<b>76·8</b>	<b>76.15</b>	<b>IMPLICATIONS FOR MANAGERS</b>	<b>76·16</b>
<b>76.8</b>	<b>SIMILARITIES AND DIFFERENCES: ARTS AND SCIENCE</b>	<b>76·8</b>	<b>76.16</b>	<b>NOTES</b>	<b>76·17</b>

A fundamental fact in computer, information, and network security<sup>2</sup> is the impossibility of 100 percent assurance that a computer system is trusted.<sup>3</sup> How education can help in achieving the required level of trust considering various stakeholders (e.g.,

# CHAPTER 77

## THE FUTURE OF INFORMATION ASSURANCE<sup>1</sup>

Peter G. Neumann

<b>77.1 INTRODUCTION</b>	<b>77·1</b>	77.3.14 System Evaluation and Certification	77·9
<b>77.2 VIEW OF THE FUTURE</b>	<b>77·3</b>		
<b>77.3 FOUNDATIONS OF ASSURANCE</b>	<b>77·5</b>	<b>77.4 BEST PRACTICES FOR INCREASING ASSURANCE</b>	<b>77·10</b>
77.3.1 Methodology	77·5	<b>77.5 ASSURANCE-BASED RISK REDUCTION</b>	<b>77·13</b>
77.3.2 Guarantees	77·5	77.5.1 Security	77·13
77.3.3 Pervasively Integrated Assurance	77·5	77.5.2 Human Safety	77·14
77.3.4 Analysis of Requirements	77·5	77.5.3 Reliability, Availability, and Survivability	77·14
77.3.5 Analysis of Compositions	77·6	77.5.4 Operational Assurances	77·15
77.3.6 Analysis of Property Transformations	77·7	77.5.5 Sound User Interfaces	77·15
77.3.7 Analysis of Dependencies	77·7	<b>77.6 ILLUSTRATIVE APPLICATION: COMPUTER-AIDED VOTING</b>	<b>77·16</b>
77.3.8 Detecting and Eliminating Vulnerabilities	77·7	77.6.1 Election Process	77·16
77.3.9 Software and Hardware Consistency Analysis	77·8	77.6.2 Voting-Related Requirements	77·17
77.3.10 System-Oriented Analyses	77·8	<b>77.7 CONCLUSIONS</b>	<b>77·19</b>
77.3.11 Development Tools	77·9	<b>77.8 FURTHER READING</b>	<b>77·21</b>
77.3.12 Measures of Assurance	77·9	<b>77.9 NOTES</b>	<b>77·21</b>
77.3.13 Risk Analysis and Risk Abatement	77·9		

### 77.1 INTRODUCTION

*Assurance is in the eye of the beholder.*

Although this chapter is at the end of the *Handbook*, we are still only at the beginning of the quest for meaningfully trustworthy systems. We begin by asserting that there

# INDEX

## A

- A posteriori* testing, 10·8–10·9
- A priori* testing, 10·8
- Abagnale, Frank, 2·4–2·5, 19·2–19·3
- Abstract Syntax Notation 1 (ASN.1), 37·5, 37·18
- Access control:
  - access control entries (ACEs), 24·16–24·18
  - access control list (ACL), 7·33, 16·10–16·11, 24·7–24·8, 26·5–26·6, 26·17, 36·4, 53·13, 53·18–53·19
  - access matrix, 24·7–24·8
  - alarms. *See* Alarms
  - audit trails. *See* Audit trail
  - and authentication, 23·20, 23·23–23·25. *See also* Authentication
  - authorization, 1·9
  - breaching, 15·14–15·18
  - bypass keys and passwords, 23·26
  - card entry systems, 23·21–23·22, 23·25
  - and computer crime investigation, 61·11
  - data-oriented, 24·7–24·9
  - diagnostic utilities, 53·8
  - discretionary access control list (DACL), 24·16, 24·18
  - distributed access control, 6·3–6·4
  - e-commerce security services, 30·6
  - encryption-based, 7·6, 7·27
  - evaluation phase, security policy development, 66·8–66·9
  - file sharing access rights, 24·10–24·11
  - file system, 36·4
  - HIPAA requirements, 71·18
  - integrated card access systems, 23·25
  - Internet-accessible systems, 30·35–30·36
  - local area networks, 1·10–1·11
  - locks and door hardware. *See* Locks and door hardware
  - log files, 53·18, 61·11
  - logical access control, 1·9
  - and malicious code, 16·3
  - and mathematical models of computer security. *See* Models of computer security
  - matrix model, 9·3–9·5
  - methods of, 47·5
  - operating systems, 24·2
  - operations center, 47·5
  - overview, 23·19–23·20
  - and penetration techniques, 15·7, 15·14–15·18. *See also* System and network penetration
  - physical, 1·9, 1·11, 7·27, 16·3, 53·18–53·19, 71·18
  - and piracy policy, 42·4
  - portal machines, 23·25–23·26
  - privileges, 23·19–23·20
  - production programs and control data, 47·13
  - proximity and touch cards, 23·22–23·23
  - radio-frequency identification (RFID), 23·19, 23·21–23·23, 23·25, 53·25
  - read-only access, 36·8
  - surveillance systems. *See* Surveillance systems
  - System Access Control List (SACL), 24·16
  - terminated employees, 13·2, 13·8
  - user access to files and databases, 47·14–47·15
  - user-oriented, 24·6–24·8
  - virtual private networks, 32·9
  - visitor badges and log ins, 23·22–23·23, 47·5–47·6
  - Web servers, 30·29
  - Web sites, 15·26
  - Windows 2000 security example, 24·14–24·19
  - wireless LANs, 25·7–25·8
  - World Wide Web, 17·11–17·12
- Access mask, 24·17–24·18
- Access matrix, 24·7–24·8
- Access token, 24·14–24·17
- Accessibility, 4·21
- Accidents, 22·17–22·18. *See also* Physical threats
- Account permissions, 8·10–8·11
- Accountability:
  - chief information security officer (CISO), 65·9–65·13
  - healthcare information, 71·6. *See also* Health Insurance Portability and Accountability Act (HIPAA)
  - infrastructure security, 23·55
  - system accountability, 77·11
  - vendors, 68·8, 68·20–68·21
- Acknowledgment numbers, 5·20



## I • 2 INDEX

- Active code, 26•16, 48•44
- Active Directory, 34•11–34•12
- Active Server Pages (ASPs), 15•29
- Active taps, 6•4
- ActiveSync Service, 33•13
- ActiveX:
  - buffer overflows, 39•13
  - controls, 17•6–17•8, 17•10–17•12, 19•18, 25•10
  - and e-commerce security, 21•8, 21•21
  - and hacker Web sites, 48•44
  - and information warfare, 14•18
  - malicious code, 16•8
  - and mobile code, 17•2, 17•5–17•12, 21•8, 30•32
  - and network security, 26•16
- Actor-observer effect, 50•8–50•9
- Ad-Aware, 21•9, 48•42
- Addiction, 12•11–12•12, 48•14, 48•27–48•28, 48•37
- Administrators:
  - database administrator (DBA), 21•20
  - information security administrators (ISAs), 47•4–47•5, 63•26–63•29
  - local area network, 1•11
  - passwords, access to by system administrators, 28•5
  - security administrators, 47•4–47•5, 63•26–63•29
  - and software patches, 40•6, 40•15
  - system administrators, password access, 28•5
  - system administrators, responsibility for software patches, 40•6
- Adobe:
  - Acrobat, 7•26, 44•14
  - antipiracy programs, 42•5
  - and Digital Rights Management, 42•13–42•14
  - Flash, 16•8
- Advance-fee fraud, 2•20, 16•10, 19•8
- Advanced Encryption Standard (AES), 7•38, 7•42–7•43, 34•13–34•14, 37•2
- Advanced Technology Attachment (ATA), 57•24
- Adware, 48•13–48•14, 48•41–48•42
- Agents, 53•11
- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 11•35–11•39
- Aircrack, 33•20, 33•37–33•38
- Airsnarf, 33•14
- Airsnort, 33•20, 33•37–33•38
- AJAX, 26•5
- Alarms:
  - circuit breaks or failures, 22•20
  - delayed-access egress, 23•32
  - desktop systems, 22•25
  - duress, 23•27
  - environmental, 23•27
  - fire, 23•35
  - intrusion alarms, 22•19, 23•26–23•27
  - open-door alarms, 22•24, 23•18, 23•27
  - overt and covert, 23•18
  - premises-wide alerts, 23•35–23•36
  - silent, 23•35
- Alerts, 53•11, 53•22–53•23
- Algorithms:
  - best practices, 77•11
  - Blowfish, 7•22, 7•27
  - Data Encryption Algorithm (DEA), 7•20, 7•37
  - defined, 7•2
  - Diffie-Hellman algorithm, 7•20, 7•23–7•24, 7•35–7•36, 37•16
  - encryption, 7•2–7•3, 7•43, 37•15–37•16. *See also* Encryption
  - Grover's algorithm, 7•40–7•41
  - public key cryptosystems, 37•4–37•6, 37•15–37•16, 37•20, 37•22
  - risk assessment, 62•17–62•18, 62•22
  - RSA algorithm, 7•24–7•27, 7•35–7•37, 37•16, 37•22
  - Secure Hash Algorithms (SHA), 34•14
  - Shor's algorithm, 7•40–7•41
- All-Hazard Mitigation Plan, 23•6, 23•52
- Allen, Paul, 1•9
- Allowed path vulnerabilities, 21•7
- Always-on generation, 50•21–50•22
- Amazon.com, 48•24
- America Online (AOL), 70•9–70•10
- American Bar Association, *Digital Signature Guidelines*, 37•8
- American Institute of Certified Public Accountants (AICPA), SAS 70, 54•7–54•10
- American Library Association, 72•15–72•16
- American National Standards Institute (ANSI), 6•22, 23•7
- ANSI/ISO/IEC 17024, 74•3–74•4, 74•6
- ANSI X3.106-1983, 7•20
- certifications, 74•5
- American Society for Industrial Security International (ASIS) Certified Protection Professionals, 74•14
- American Standard Code for Information Interchange (ASCII), 4•3
- Americans with Disabilities Act, 29•18
- Annoy.com, 48•4
- Anonymity:
  - benefits of, 70•10–70•12
  - and content filtering, 31•11
  - cybersmearing, 69•14–69•15
  - cyberspace versus real world, 70•4–70•5
  - disadvantages of, 70•13–70•14
  - ethical principles, 70•16–70•18
  - government, role of, 70•20–70•21
  - and identity in cyberspace, 70•8–70•10
  - and Internet Service Providers, 70•18–70•20
  - overview, 70•1–70•2, 70•21–70•22
  - preserving benefits of, 70•16–70•21
  - and privacy rights, 69•14–69•15, 70•11–70•13
  - pseudonymity, 70•9–70•14, 70•16

- social psychology issues, 70·5–70·10. *See also*
  - Social psychology
  - systems analysis, 70·15–70·16
  - terminology, 70·3–70·5
  - theory of nymity, 70·8
  - types of, 70·9
  - virtual worlds, 70·12–70·13
  - and Web monitoring, 31·11
- Anonymizing remailers, 42·15, 48·4, 70·9–70·10
- ANSI. *See* American National Standards Institute (ANSI)
- Antibot software, 20·32
- Antimalware, 17·2, 26·13, 26·15–26·16, 48·14, 66·10
- Antisniffer tools, 25·4
- Antispoofing, 26·11
- Antispyware programs, 5·3, 19·17–19·18, 48·14
- Antivirus programs:
  - antivirus databases, 41·7
  - antivirus engines, 41·7
  - automatic updates, 41·3
  - content filtering, 41·10–41·12
  - deployment, 41·12–41·13
  - e-commerce security services, 30·6
  - and extent of malware, 41·1–41·2
  - generic detection, 41·7–41·9
  - heuristics, 41·7, 41·9–41·10
  - intrusion detection and prevention, 41·7, 41·10. *See also* Intrusions
  - issues, 41·3
  - for MacOS, 25·14
  - malicious code prevention, 16·9–16·10
  - overview, 41·14
  - personal computers, 5·3, 26·9
  - policy, 41·13–41·14
  - scanners, 41·3, 41·5–41·7
  - scanning methodologies, 41·8, 41·10, 48·9
  - and social engineering attacks, 19·17–19·18
  - software patches, 40·12
  - specific detection, 41·7–41·8
  - terminology, 41·2–41·3
  - updating, importance of, 41·3
  - viruses. *See* Viruses
  - and VoIP, 34·11
  - and vulnerability assessments, 46·4
  - WildList, 41·3, 41·6
- Apple Computer, 1·10, 51·29
- AppleTalk, 6·26, 25·14–25·15
- Applets, 16·8, 17·2, 17·9, 17·11, 21·8, 48·34
- Appliances, 26·9–26·10
- Application isolation, 25·11
- Application layer gateways (ALGs), 26·7, 34·11
- Application program interface (API), 19·7, 26·2
- Application servers, 21·8
- Application service providers (ASPs), 30·41–30·42
- Application tunneling, 31·10
- Applications. *See also* Software
  - application-based monitoring for intrusion detection, 27·7
  - application-layer gateways, 26·7, 34·11
  - backup and recovery procedures, 52·6–52·9, 52·11
  - batch files, protecting, 52·2, 52·8–52·9
  - core layer, 5·10
  - database management. *See* Databases
  - design, 30·26
  - development, 52·1–52·2
  - diagnostic utilities, 52·11
  - hosted, 26·2
  - joint application development (JAD), 39·7, 52·2
  - online files, protecting, 52·2–52·8
  - overview, 5·8–5·9
  - peer-to-peer (P2P), 5·25
  - rapid application development (RAD), 39·7, 52·2
  - and relational database management system (DBMS), 52·1–52·2
  - standards, 5·26–5·28
  - validation controls, 52·2, 52·9–52·11
  - Web application firewall, 26·4–26·5
  - and Web site protection, 30·26
- ARPANET (Advanced Research Projects Agency Network), 1·8–1·9, 1·12, 77·15
- Artificial intelligence (AI), 53·21
- ASCII, 4·3
- Asymmetric attacks, 21·5
- Asynchronous communications, 15·9, 26·5
- Asynchronous time, 4·11
- Attacks. *See also* Security incidents
  - asymmetric, 21·5
  - brute force attacks. *See* Brute force attacks
  - buffer overflow. *See* Buffer overflow
  - Fluhrer, Mantin, and Shamir (FMS) attacks, 33·19–33·20
  - man-in-the-middle. *See* Man-in-the-middle attacks
  - security incident taxonomy, 8·12–8·16
- Attitudes, 50·13–50·16
- Attribution errors, 50·7–50·10
- Audit trail, 23·20, 26·27–26·28, 30·6, 53·14. *See also* Audits; Logs and logging
- Auditability, 27·3–27·4
- Auditing Standard (AS) No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, 54·12
- Auditor, 33·36–33·37
- Auditors, internal and external, 54·13–54·14
- Audits:
  - audit controls, 19·16
  - audit file, 24·13
  - audit trail. *See* Audit trail
  - batch files, 52·9
  - best practices, 54·20
  - frameworks for IT audits, 54·19–54·21

## I • 4 INDEX

### Audits (*Continued*)

- purpose of, 63•22–63•23
- security auditing, WLANs, 33•36–33•39
- standards, 54•2–54•10. *See also*
  - Gramm-Leach-Bliley Act (GLBA);
  - International Organization for Standardization (ISO); Standards

### Aureate/Radiate, 48•14

### Authentication:

- access control, 23•20, 23•23–23•25. *See also*
  - Access control
- biometric. *See* Biometric authentication
- and Common Internet File System exploits, 36•9
- costs of technologies, 28•16
- cross-domain, 28•15–28•16
- defined, 28•2
- device authentication, 34•12
- e-commerce security services, 30•6
- e-mail certificates, 19•18
- and encryption, 7•4–7•5
- extranets, 32•14–32•15
- host site, 21•10–21•11
- identity. *See* Identification
- IEEE standards. *See* IEEE 802 standards
- importance of, 29•2
- and information systems security, 15•2
- issues, 28•16–28•17
- and mobile code, 17•4
- open, 33•15–33•16
- and operations security, 47•5
- overview, 28•1–28•2, 28•17
- password-based. *See* Passwords
- person-to-computer versus computer-to-person, 28•2
- personal identification number (PIN), 17•7, 23•23, 28•3, 28•8, 28•14
- preliminary evaluation phase, security policy development, 66•5
- principles of, 28•2–28•5
- and Public Key Infrastructure, 37•24–37•25. *See also* Public Key Infrastructure (PKI)
- RSA encryption, 7•25–7•26
- and security incident common language, 8•5–8•10
- shared-key, 33•16
- smart cards. *See* Smart cards
- token-based, 28•13–28•15. *See also* Tokens
- two-factor, 25•6, 28•3, 28•8, 28•13
- user authentication, VoIP, 34•12
- vendors, software patches, 40•12
- virtual private networks, 32•5
- and Wired Equivalent Privacy (WEP), 25•7–25•8

### Authenticity:

- e-commerce security services, 30•6
- and operating system security, 24•2
- and outsourcing risks, 68•13–68•15
- as source of loss, 3•2, 3•5–3•6, 3•8–3•12
- and trust, 7•25–7•26

### Authenticode, 17•5, 17•7

### Authority Revocation List (ARL), 37•19

### Authorization:

- access control, 1•9
- defined, 28•1–28•2
- e-commerce security services, 30•6
- and information systems security, 15•2
- and sandboxes, 17•4
- and security incident common language, 8•6, 8•13–8•15
- unauthorized use of computers or networks, 3•2, 3•16

### Automatic updates, 16•10, 17•11

### Automation:

- computer security incident information, 56•14
- monitoring and control systems, 53•2, 53•6–53•7, 53•18, 53•26

### AV scanners. *See* Antivirus programs

### Availability:

- controls, 68•12–68•13, 68•15
- data, 24•3
- extranet systems, 32•15
- firewalls and gateway security devices, 26•19
- hardware, 24•3
- healthcare information, 71•6
- high-availability (HA) configuration, 26•23
- and operating system security, 24•2
- software, 24•3
- as source of loss, 3•2, 3•4, 3•8–3•12
- virtual private networks, 32•10

### Avalanche photodiode (APD), 6•10

### Avatars, 48•29

### Aviation, importance of information assurance, 77•14–77•15

### Awareness programs:

- antivirus technology, 41•13
- audience involvement, 49•23–49•24
- audits and inspections, 49•35
- budget, 49•7, 49•10
- and compliance agreements, 49•29
- content of, 49•17–49•20
- contests, 49•30
- elements of, 49•5–49•10
- fear, uncertainty, and doubt (FUD factor), 49•13, 49•40
- focus groups, use of, 49•14
- give-aways, 49•31–49•34
- goals, 49•8–49•9
- humor, use of, 49•26–49•27
- and learning styles, 49•21–49•22
- as long-term activity, 49•5, 49•9
- management support, 49•7, 49•10–49•12
- metrics, 49•8, 49•35–49•39
- motivation, 49•14–49•17
- newsletters, use of, 49•9, 49•30
- overview, 49•2, 49•39
- penalties, 49•14–49•17, 49•27
- people as security problem, 49•4–49•5, 49•36
- and performance appraisals, 49•29
- posters, 49•9, 49•31

presentation of materials, 49·20–49·27  
 quizzes, 49·12, 49·23  
 resistance to, 49·13  
 responsibility issues, 49·13–49·14  
 rewards, 49·7–49·8, 49·14–49·17, 49·27  
 screen savers, 49·9, 49·34  
 security policy, 49·6, 66·14  
 social engineering attacks, 19·17  
 as social marketing, 49·5, 49·14, 49·40  
 suggestion programs, 49·34–49·35  
 as survival technique, 49·2–49·5  
 terminology, 49·40–49·41  
 tools, 49·27–49·35  
 training distinguished, 49·4  
 union support, 49·12–49·13  
 videos, 49·32  
 visibility and appeal, 49·9–49·10  
 Web-based courses, 49·25, 49·28–49·29,  
 49·37

**B**

Babel Fish, 31·1, 31·11  
 Back door utilities, 15·25  
 Back Orifice (BO) and Back Orifice 2000  
 (BO2K), 2·23, 21·4, 21·10, 25·10  
 Back pocket file, 24·13  
 Backdoor.IRC.Snyd.A, 17·3  
 Background checks, 13·2, 13·6–13·8, 16·9,  
 45·2–45·3  
 Backoff schemes, 6·13  
 Backout and recovery, 47·6, 47·8, 52·7  
 Backups:  
   application, 57·14  
   batch files, 52·8  
   data. *See* Data backups  
   and data losses, 3·15  
   data storage, 36·4–36·5  
   database management, 52·6  
   encryption, 36·5  
   hardware, 4·18–4·19  
   need for, 4·17, 52·11  
   and new versions of software, 47·6–47·7  
   personnel, 4·18  
   plans for, 4·17–4·18  
   power, 4·19–4·20  
   and restore functionality, 26·23  
   system, 57·14  
   testing, 4·20  
 Backward learning, 6·24  
 Bandwidth consumption attacks, 18·7–18·9  
 Banks. *See also* Financial industry  
   business continuity planning regulations, 58·3  
   Gramm-Leach-Bliley Act. *See*  
     Gramm-Leach-Bliley Act (GLBA)  
   media storage, 57·22  
 Banner ads, 21·8  
 Baseband bus, 6·6  
 Basel II, 65·3  
 Batch processing, 52·2, 52·8–52·9  
 BD-R disks, 4·9

BD-RE disks, 4·9  
 Behavior. *See also* Psychology; Social psychology  
   explanations of, 50·7  
   group behavior, 50·20–50·21  
   management, 56·29  
   professionalism, 56·24–56·25  
   social pressure and behavior change, 50·18  
 Beliefs and attitudes, 50·13–50·16  
 Bell-LaPadula model, 9·2, 9·9–9·12, 9·18–9·19  
 Benefit-cost analysis (BCA), 23·53  
 Berkeley Software Distribution (BSD) License,  
   11·34  
 Berne Convention, 11·35, 11·37  
 Best practices, 54·15, 54·20–54·21,  
   77·10–77·12  
 BFile sharing, 11·23–11·24  
 Bias, self-serving, 50·9  
 Biba's strict integrity policy model, 9·2, 9·9,  
   9·12–9·14, 9·18–9·19  
 Binary design, 4·2–4·4  
 Bind, 21·12  
 Biological and chemical warfare, 23·50  
 Biometric authentication:  
   and authentication principles, 28·2, 28·4  
   biometrics, 29·4–29·5  
   costs, 29·18  
   crossover error rate (equal error rate),  
     29·15–29·16  
   disadvantages and concerns, 29·16–29·21  
   and double enrollment prevention, 29·7  
   dynamic biometrics, 28·4–28·5  
   encryption, 29·20–29·21  
   enrollment, 29·7–29·8, 29·16  
   facial scans, 23·24, 29·10–29·12, 29·16,  
     29·18–29·19, 29·21–29·22  
   facilities access (physical access), 29·7  
   failure to enroll, 29·16  
   false accepts, 29·15, 29·19  
   false rejects, 29·15  
   finger scans, 23·24, 29·8–29·10,  
     29·16–29·18, 29·20, 29·24  
   fraud, 29·18, 29·29  
   government use of, 29·21  
   hand geometry scan, 29·12–29·13,  
     29·17–29·19, 29·24  
   history of, 29·2–29·3  
   iris scan, 23·25, 29·13–29·14, 29·17–29·19  
   keystroke scans, 29·15  
   overview, 23·24, 28·15, 29·2–29·4, 29·24  
   privacy issues, 29·17, 29·19–29·21  
   public identification systems, 29·7  
   retinal scanning, 23·25, 29·15  
   security (logical access), 29·6–29·7  
   signature scans, 29·15  
   static biometrics, 28·4  
   technologies, comparison chart, 29·23  
   templates for data acquisition, 29·8  
   trends, 29·21–29·22, 29·24  
   verification of identity, 29·5–29·6  
   voice recognition, 23·25, 29·14, 29·17–29·18

## I • 6 INDEX

- Bitlocker Drive Encryption, 25•11
  - Bits, 4•3
  - Black box testing, 38•14, 51•11
  - Black boxes, 69•9
  - Blades, 26•8
  - Block lists, 20•19–20•20, 31•7–31•8
  - Blogs, 48•5, 48•30
  - Blowfish, 7•22, 7•27
  - Blu-ray, 4•9, 57•8
  - BMC, 51•29
  - Bogus network addresses (BOGONs), 16•10
  - Bologna Declaration. *See* Europe, educational system
  - Boot sector viruses, 16•4. *See also* Viruses
  - Booting, 4•8
  - Border Gateway Protocol (BGP), 5•22, 5•26, 32•9
  - Bot herders, 16•8
  - Bot Roast II, 17•11
  - Botnets, 15•29–15•30, 19•8, 20•19, 20•32, 32•10, 55•13
  - Bots, 11•28, 16•6–16•8, 17•11
  - Boundary condition violations, 38•9
  - Bribery, 19•7
  - Brick walls, 17•4
  - Bridges, 6•24–6•25
  - British Standard 7799 (BS7799), 54•3–54•4, 62•3
  - Broadband access lines, 5•4
  - Broadband bus, 6•6
  - Broadband Technology Advisory Group (BBTAG), 6•17
  - Broadband Wireless Access (BBWA), 6•18
  - Brownouts. *See* Power failures and disturbances
  - Brute force attacks:
    - cryptanalysis, 7•9–7•11, 7•17, 21•12, 37•21
    - and e-commerce, 21•12
    - penetration techniques, 15•15
    - and VoIP theft of service, 34•10, 53•13
  - Buffer overflow:
    - application server program, 21•19
    - boundary violations, 38•9
    - denial-of-service attacks, 18•7
    - and distributed denial-of-service attacks, 18•20–18•21
    - and extranets, 32•14
    - and IM applications, 35•9
    - and network file system, 36•8
    - and system penetration, 15•23, 15•27–15•28
    - and testing software, 39•13
    - UNIX, 25•13
    - Web and mail servers, 21•4
  - Buffers, 53•9
  - Bugs:
    - commercial off-the-shelf software, 21•13
    - debugging, 39•5, 39•18–39•20, 77•11
    - seeding, 39•15
    - software, 5•9
    - tracking and removal, 39•16
    - and wiretapping, 23•48–23•49. *See also* Wiretapping
  - Build Security In (BSI), 38•13
  - Burma (Myanmar), Internet content regulation, 72•7
  - Bus topology, 6•5–6•6
  - Bus-wired ring, 6•6, 6•8
  - Business continuity planning (BCP):
    - business impact analysis, 58•14–58•29
    - and computer security incident response team, 56•7–56•8
    - and corporate mission, 58•10–58•12
    - cost justification, 58•29–58•34
    - disaster recovery. *See* Disaster recovery
    - disasters, types of, 58•4–58•6
    - educational programs, 75•12–75•13
    - evaluation phase, security policy development, 66•11
    - Generalized Cost Consequence (GCC) model, 58•6, 58•31–58•34
    - goals, 58•8–58•14
    - overview, 58•1–58•2
    - postincident analysis, 56•31
    - presentation of plan, 58•34–58•36
    - public relations, 58•14
    - purpose of, 58•2
    - quantitative risk model, 58•29–58•31
    - recovery process, phases of, 58•13–58•14
    - recovery scenarios, 58•6–58•8
    - and risk, 58•3–58•4
    - safety issues, 58•14
    - scope of plan, 58•9–58•10
  - Business impact analysis (BIA):
    - criticality of functions, 58•21–58•22
    - departments and functions, 58•18, 59•19–59•20
    - function category, 58•23–58•24
    - and goals of business continuity planning, 58•9–58•13
    - interview process, 58•15–58•18
    - key persons and key alternate, 58•20
    - matrix analysis, 58•25–58•29
    - operational impact, 58•22–58•23
    - overview, 58•14
    - scope of, 58•15
    - survival time, 58•20–58•21
    - system elements, 58•24–58•25
  - Business-to-business (B2B) transactions, 21•6–21•8, 30•13–30•17
  - Business-to-customer (B2C) transactions, 30•3–30•4, 30•9–30•13, 30•17
  - BUTTsniiffer, 25•4
  - Bytes, 4•3, 5•2
- ## C
- C, 21•14, 21•19, 38•8
  - C++, 21•14, 38•8, 47•3
  - Cable Communications Policy Act, 69•12

- Cable-TV Based Broadband Communication Networks, 6·17
- Cables:
  - coaxial cable (coax), 6·2, 6·8–6·9, 6·12, 6·18
  - fiber optic. *See* Fiber optic cable
  - and threats to information infrastructure, 22·18–22·20
  - unshielded twisted pair. *See* Unshielded twisted pair (UTP) wire
- Cache files, 15·17, 26·16
- Cache services, 31·12
- Calculation errors, 38·9, 39·8
- Cameras. *See* Surveillance systems
- CAN-SPAM Act, 16·8, 20·15, 20·25–20·26
- Canada, 72·2, 72·4
- Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC), 51·15
- Capability Assessment for Readiness (CAR) Report, 23·7
- Capability Maturity Model (CMM), 51·13–51·14
- Capability tickets, 24·8
- Card entry systems, 23·21–23·22
- Carding, 2·26
- Carrier sense multiple access with collision avoidance (CSMA/CA), 6·13
- Carrier sense multiple access with collision detection (CSMA/CD), 6·13–6·14, 6·16
- Catastrophic events. *See* Physical threats
- Cathode-ray terminals (CRTs), 5·12
- Causality versus association, 10·7–10·8
- CC Testing Labs (CTLs), 51·27
- CCCure.org, 63·28, 74·18
- CD-R, 4·9
- CD-ROM, 57·19
- CD-RW, 4·9, 57·19
- CDC*, 15·33
- Cellular phones and modems, 15·11–15·12, 21·8, 35·14–35·15. *See also* Short message service (SMS)
- Censorship, 72·1–72·18
- Centers for Medicare and Medicaid Services (CMS), 54·16, 71·8, 71·12, 71·14
- Centers of Academic Excellence in Information Assurance Education (CAE), 74·4–74·5, 75·4–75·5, 76·13
- Central processing unit (CPU) log file, 53·17
- CERT/CC. *See* Computer Emergency Response Team Coordination Center (CERT/CC)
- Certificate Policy (CP), 37·8–37·9, 37·17
- Certificate Revocation List (CRL), 37·6, 37·13, 37·16–37·22, 37·25
- Certification:
  - ANSI/ISO/IEC 17024 standard, 74·3–74·4
  - Center of Academic Excellence in Information Assurance Education (CAEIAE), 74·4–74·5, 75·4–75·5, 76·13
  - certificate courses and degree programs, 63·29
  - Certification Commission for Health IT (CCHIT), 71·15
  - Certification in Control Self-Assessment (CCSA), 74·7, 74·9
  - Certified Financial Services Auditor (CFSA), 74·7, 74·9
  - Certified Government Auditing Professional (CGAP), 74·7, 74·9
  - Certified Information Security Manager (CISM), 74·10–74·12
  - Certified Information Systems Auditor (CISA), 74·9–74·10, 76·11
  - Certified Information Systems Security Professional (CISSP), 74·6–74·7, 74·12–74·14, 74·20, 74·22, 75·3, 76·13, 76·16
  - Certified Internal Auditor (CIA), 74·7–74·9
  - versus conferred professionalization, 75·4
  - distance learning programs, 75·9–75·12
  - examinations, preparing for, 74·16–74·20
  - Global Information Assurance Certification (GIAC), 74·15–74·16, 75·3
  - as global trend, 76·17
  - IACE, 74·4–74·5
  - information security management system (ISMS), 54·5
  - information systems security, 74·5–74·16
  - International Council of Electronic Commerce Consultants (EC-Council), 74·23–74·24
  - management, 63·28–63·29
  - NOCA/NCCA, 74·4–74·5
  - overview, 74·5, 74·24
  - Security Plus, 75·3
  - Security University, 74·5, 74·20–74·22
  - Systems Security Certified Practitioner (SSCP), 74·14, 74·22
  - terminology, 74·3
  - and Trusted Information Environment model, 75·3–75·4
- Certification Authority (CA), 17·5, 21·10–21·11, 37·5–37·22, 51·29. *See also* Digital certificates
- Certification practice statement (CPS), 37·8–37·9
- CGI. *See* Common Gateway Interface (CGI)
- CGI/PHP (Hypertext Processing), 21·13
- Chain letters, 48·9–48·11, 48·14
- Chain of custody, log records, 53·19
- Challenge-handshake authentication protocol (CHAP), 25·9–25·10
- Change:
  - CISO as change agent, 65·1–65·3, 65·11, 65·18
  - incremental change, 50·19
  - management, 39·16–39·18
  - and monitoring and control systems, 53·5
  - operations staff responsibilities, 47·6
  - social psychology. *See* Social psychology
- Chaos Computer Club, 2·22, 17·7–17·8
- Chargeback systems, 53·21, 53·23
- Check digits, 47·16, 52·9
- Check Mark program, 51·12

## I • 8 INDEX

- Checklist for hardware security, 4•25–4•27
- Checksums, 7•4, 39•20, 46•4, 47•8, 52•9, 53•13, 53•18–53•19
- Chief information officer (CIO), 22•7, 63•2
- Chief information security officer (CISO):
  - accountability, 65•9–65•13
  - as change agent, 65•1–65•3, 65•11, 65•18
  - executive visibility, 65•13
  - governance, 65•9–65•11
  - information technology, relationship with, 65•17
  - internal audit, relationship with, 65•16–65•17
  - legal counsel, role of, 65•16
  - metrics, 65•13
  - and organizational culture, 65•15–65•16
  - and organizational structure, 65•17–65•18
  - overview, 65•18
  - professional and trade organizations, involvement with, 65•18
  - qualifications, 65•14–65•15
  - reporting, 65•12–65•13, 65•17
  - responsibilities, 63•2–63•4, 65•11–65•14, 65•18
  - standard of care, 65•6–65•8, 65•13–65•14, 65•18
  - as strategist, 65•3, 65•5–65•6
- Chief technology officer (CTO), 63•2
- Child Internet Protection Act (CIPA), 31•3, 72•14–72•15, 72•17
- Child Online Privacy Protection Act, 48•14
- Child Online Protection Act (COPA), 72•14
- Child pornography, 61•3, 72•12–72•13
- Children:
  - and cybersex sites, 48•28–48•29
  - and Internet pornography, 48•35
  - and plagiarism, 48•30–48•31
  - protecting, recommendations for, 48•35–48•39
  - and video games, 48•29
- Children's Online Privacy Protection Act of 1998 (COPPA), 11•29, 30•19, 69•11
- China:
  - Internet content regulation, 72•4–72•6
  - and piracy, 11•20
  - reliability of Chinese-manufactured computer components, 2•14
  - technological attacks on defense and R&D facilities, 16•3
- Chinese Wall model (Brewer-Nash model), 9•2, 9•16–9•19
- Chipping code, 25•7
- ChoicePoint Inc., 49•6–49•7
- Christmas Tree worm, 2•15, 18•2, 18•4
- Cipher block chaining (CBC), 53•19
- Ciphers, 4•17, 7•2, 7•6–7•16, 7•18–7•19. *See also* Encryption
- Ciphertext, 7•2–7•3, 37•2–37•3, 53•19. *See also* Encryption
- Cisco, 51•29
- Civil disruptions, 22•26
- Clark-Wilson model, 9•2, 9•9, 9•14–9•16, 9•18–9•19
- Cleaning and maintenance, 22•24
- Clearinghouses and HIPAA compliance, 71•22
- Client/server systems, 26•4–26•5
- Clinger-Cohen Act (Information Technology Management Reform Act of 1996), 54•17
- Clinical Information Systems Security model, 9•18
- Coalition Against Unsolicited Commercial E-mail (CAUCE), 20•13, 20•17
- Coaxial cable (coax), 6•2, 6•8–6•9, 6•12, 6•18
- COBIT. *See* Control Objectives for Information and Related Technology (COBIT)
- COBOL, 47•3
- Code Red Worm, 18•21, 18•25–18•26
- Codes and coding. *See also* Encryption
  - assurance tools, 38•13–38•15
  - best practices and guidelines, 38•6–38•7, 38•15
  - and binary design, 4•3–4•4
  - buffer overflow vulnerabilities, 38•13. *See also* Buffer overflow
  - debugging, 77•11
  - decoding and debugging phase of software development, 39•5
  - design phase, 38•5
  - digital signatures, 38•7, 47•8
  - due diligence, 38•3–38•4
  - dynamic code analysis, 77•11
  - errors, 16•10, 21•7, 38•7–39•12, 38•8–38•13
  - languages, 38•7–38•8
  - malicious code. *See* Malware
  - mobile code. *See* Mobile code
  - open source. *See* Open source code
  - operating system considerations, 38•5
  - policy and management issues, 38•1–38•4
  - regulatory compliance issues, 38•4
  - requirements analysis, 38•4–38•5
  - secure code, overview, 38•1, 38•15
  - security integration, 38•4, 38•15
  - self-checking codes, 4•6
  - self-replicating code, 16•2
  - signed code, 17•4–17•8, 17•10–17•12
  - software errors, 38•8–38•13, 39•7–39•12
  - software total quality management, 38•2–38•3
  - source code, 47•3, 47•8–47•9
  - standards, 38•15
  - static code analysis, 77•11
  - testing, 38•15, 77•11
- Codes of conduct, 69•18
- Coexistence Technical Advisory Group, 6•18
- Collaboration tools, 35•3, 35•16–35•20
- Colleges and universities:
  - business continuity management degree, 75•13
  - Center of Academic Excellence in Information Assurance Education (CAE) certification, 74•4–74•5, 75•4–75•5, 76•13
  - certificate courses and degree programs, 63•29

- data classification schemas, examples of, 67·8–67·9
- distance learning programs, 75·9–75·12
- in Europe. *See* Europe, educational system
- malware, courses on, 76·13–76·14
- Coloured Petri Nets (CPNets), 55·25
- Commercial off-the-shelf (COTS) software, 14·3, 17·3, 21·13, 21·21, 47·9
- Commercial Product Evaluation Program, 24·13
- Committee for National Security Systems (CNSS), 75·5, 75·7
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission, 54·10–54·12, 54·19
- Common Body of Knowledge (CBK), 74·12, 74·18
- Common Criteria (CC), 51·10, 51·12, 51·15–51·31
- Common Criteria Evaluation and Validation Scheme (CCEVS), 1·13, 51·15, 51·17–51·18, 51·25–51·30
- Common Criteria Portal, 51·29
- Common Evaluation Methodology (CEM), 51·26
- Common Evaluation Methodology/Common Criteria (CEM/CC), 51·26
- Common Gateway Interface (CGI), 15·26, 21·2–21·3, 21·13–21·15, 21·17
- Common Internet File System (CIFS), 36·3, 36·8–36·9, 57·4
- Common language for security incidents, 8·1–8·20, 55·14
- Common Object Model (COM), 21·13
- Common Object Request Broker Architecture (CORBA), 21·13
- Communications:
  - data, 4·13–4·16, 4·24
  - encryption, 7·27–7·35
  - intercepting, 15·8–15·14
  - and outsourcing, 68·13
  - software, 6·26
- Communications Assistance for Law Enforcement Act (CALEA), 34·4–34·5, 69·9
- Communications Decency Act (CDA), 72·14
- Compact discs (CDs), 36·1
- Compact-disk read-only memory (CD-ROM), 4·9
- Compartmentalization, 30·34–30·35
- Compatible Time Sharing System (CTSS), 1·7
- Component-based software (CBS), 21·13–21·14
- Computer Abuse Amendments Act of 1994, 61·6
- Computer crime:
  - credit card fraud, 2·6
  - criminals. *See* Computer criminals
  - data diddling, 2·9–2·10
  - data theft, 4·21
  - denial-of-service attacks, 2·20–2·21
  - detection, 10·2
  - and discarded media, 57·23
  - embezzlement, 45·6
  - and employees, 45·1–45·2. *See also* Employees
  - extortion, 2·11
  - financial rewards of, 20·33
  - fraud. *See* Fraud
  - hackers, 2·21–2·26
  - history of, reasons for studying, 2·2
  - identity theft, 2·7
  - impersonation, 2·4–2·7
  - information technology insiders. *See* Insiders, information technology
  - insurance coverage, 60·11
  - investigation. *See* Cyber investigation
  - law enforcement involvement, security incidents, 56·10, 56·22–56·23, 56·30. *See also* Law enforcement, cooperation with
  - legislation, 61·6–61·7, 73·2
  - logic bombs, 2·10–2·11, 13·6–13·7, 16·4, 45·9
  - and malicious code, 16·3, 16·11. *See also* Malware
  - online gambling, 48·27
  - pedophiles, 48·12–48·13
  - phone phreaking, 2·7–2·8
  - and physical threats to infrastructure, 22·2
  - Ponzi schemes, 48·9–48·10
  - reporting, 10·2
  - research methodology, 10·3–10·11
  - sabotage, 2·2–2·4, 4·21
  - salami fraud, 2·10
  - social engineering. *See* Social engineering
  - spam. *See* Spam
  - statistics on, limitations, 10·3–10·4
  - and system penetration techniques. *See* System and network penetration
  - time bombs, 2·10–2·11
  - trends, 2·2, 2·26–2·27, 19·15
  - Trojan horses. *See* Trojan horses
  - unauthorized security probes, 45·10
  - viruses. *See* Viruses
  - workplace issues, 48·32
  - worms. *See* Worms
- Computer criminals. *See also* Computer crime; Cyber investigation
  - aggressive behaviors, 12·4–12·8
  - anonymity, 12·4, 12·7, 12·15
  - antisocial personality disorder, 12·8–12·9, 12·21
  - and Asperger syndrome, 12·10–12·11
  - categories of, 8·16
  - classifications of, 12·15–12·22
  - computer addiction, 12·11–12·12, 12·21
  - cyberterrorism, 12·3, 12·19
  - cyberterrorists, 12·19
  - deindividuation, 12·6
  - ethical immaturity, 12·12–12·15, 12·21
  - five-factor model of personality, 12·9–12·10
  - hackers, 12·2, 12·16



## I • 10 INDEX

- Computer criminals (*Continued*)
  - motivation, 12•2–12•4, 12•20–12•21, 55•17–55•20
  - narcissistic personality disorder, 12•9, 12•21
  - overview, 12•1–12•2, 12•21–12•22
  - personality disorders, 12•8–12•12
  - profiling, 55•17–55•20
  - and social context, lack of, 12•5–12•6
  - social identity model of deindividuation effects, 12•6–12•7
  - social learning theory, 12•7–12•8
  - social presence, 12•5–12•6
  - social psychology. *See* Social psychology
  - victim-blaming, 12•4–12•5, 12•20
  - virus creators, 12•19–12•21
- Computer Emergency Response Team
  - Coordination Center (CERT/CC), 8•2–8•3, 15•13, 15•28, 38•8, 56•2, 56•4–56•5
  - assistance during security incident, 56•9
  - and denial-of-service attacks, 18•12
  - reporting incidents to, 56•33–56•34
  - security improvement modules, 44•5–44•6
- Computer Fraud and Abuse Act (CFAA), 11•26–11•30, 16•5–16•6, 16•8, 61•6
- Computer languages, 38•7–38•8, 41•4, 47•3
- Computer Matching and Privacy Protection Act of 1988, 67•3
- Computer Output to Microfilm (COM), 57•20
- Computer program, defined, 47•3
- Computer Science and Technology Board, 1•13
- Computer Security Act of 1987, 61•7, 75•5
- Computer Security Incident Handling Guide*, 56•32
- Computer security incident response team (CSIRT):
  - baselines, 56•10, 56•12–56•13
  - burnout, 56•27–56•28
  - common services, 56•5–56•6
  - conferences, attending and speaking at, 56•34–56•35
  - contacts, establishing list of, 56•9–56•10
  - continuous process improvement, 56•7, 56•32–56•33
  - described, 56•3
  - documentation, 56•15–56•19, 56•22
  - emergency response, 56•20–56•24
  - establishing, 56•7–56•10
  - functions of, 56•5
  - help desk, role of, 56•19, 56•25
  - history and background, 56•4–56•6
  - in-house versus outsourcing, 56•6–56•7
  - law enforcement involvement, 56•10, 56•22–56•23, 56•30
  - legal staff involvement, 56•12
  - managing, 56•24–56•30
  - mission and charter, 56•7–56•8
  - outside agencies, interaction with, 56•9–56•10
  - overview, 56•2–56•3, 56•35
  - policies and procedures, 56•8–56•9, 56•27
  - postincident activities, 56•30–56•33
  - public affairs, role of, 56•30
  - purpose of, 56•3–56•4
  - reporting security incidents, 56•33–56•35
  - role of, 56•3–56•4
  - selection of team, 56•10–56•12, 56•19–56•20
  - shiftwork, 56•29–56•30
  - and social engineering, 56•27
  - technical expertise, 56•11, 56•14
  - telephone hotline, 56•19–56•20
  - tracking incidents, 56•15–56•19
  - training, 56•14–56•15
  - triage, 56•11, 56•13–56•14, 56•25–56•27
  - types of teams, 56•6–56•7
- Computer Security Institute (CSI), 13•8, 25•10, 56•34
- Computer Security Resource Center (CSRC), 23•31
- Computers:
  - client/server systems, 26•4–26•5
  - internal clocks and time issues, 4•10–4•11
  - LAN components, 6•2
  - laptops, 1•18, 33•12–33•13, 36•10–36•11, 57•16–57•17
  - large-scale, 1•4–1•5
  - mainframe systems, 26•4
  - medium-size, 1•5–1•6
  - personal computers (PCs), 1•8–1•10, 4•20–4•25, 5•3, 26•5
  - small-scale, 1•6–1•7
  - system assets, 24•3
- Computers and Risk*, 1•13–1•15
- Conferences, 63•13
- Confidence limits, 10•6–10•7
- Confidentiality. *See also* Privacy
  - breaches of, insurance coverage for, 60•13–60•18
  - and disclosure of information, 3•16
  - employee nondisclosure agreements, 45•14
  - and encryption, 7•3–7•4. *See also* Encryption
  - healthcare information, 71•6. *See also* Health Insurance Portability and Accountability Act (HIPAA)
  - and operating system security, 24•2
  - and outsourcing risks, 68•14
  - regulatory compliance, 26•2
  - as source of loss, 3•2, 3•6–3•14
  - threat information, 22•26–22•27
- Configuration:
  - adjustment, 40•13
  - firewalls and gateway security devices, 26•22–26•23
  - monitoring and control systems, 53•5, 53•13
  - standardized, 40•23–40•24
  - Web servers, 21•16–21•17, 21•21
- Consortium-based product assessments, 51•7–51•10

- Construction concerns:
  - and clean electrical power, 23·36–23·38
  - confidential design details, 23·12–23·13
  - electrical power, 23·36–23·44
  - electrical standards, 23·14
  - emergency power, 23·38–23·44
  - equipment cabinets, 23·17–23·18
  - equipment rooms, 23·33–23·35
  - facility design, 23·31
  - firestops, 23·17
    - and occupied spaces, 23·16–23·17
    - physical site security, 23·33–23·35
    - site selection, 23·31–23·32
    - telecommunications standards, 23·14
    - violence prevention and mitigation, 23·13–23·14
- Consumer Privacy Legislative Forum, 71·10
- Consumers:
  - and benefits of CC-based testing, 51·30
  - in-house assessments of products, 51·7–51·8
  - insurance policies, 60·18
- Content filtering. *See also* Web monitoring and antivirus technology, 41·10–41·12
- censorship. *See* Censorship legislation, 72·14
- network security, 26·15
- pornography, 48·34–48·35
- Contention network, 6·12–6·13
- Contingency planning, HIPAA requirements, 71·19
- Contingency tables, 10·7
- Continuous process improvement, 56·7, 56·32–56·33
- Control (command) structure errors, 38·11–38·12, 39·11
- Control groups, 10·8
- Control loop, 53·4
- Control mode, 24·9
- Control Objectives for Information and Related Technology (COBIT), 44·4–44·5, 49·35, 53·3, 53·5, 53·8, 53·26, 54·12–54·13, 54·15, 65·8, 67·6
- Control systems. *See* Monitoring and control (M&C) systems
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 11·29
- Controls:
  - ActiveX, 17·6–17·8, 17·10–17·12, 19·18, 25·10. *See also* ActiveX information security, 3·14–3·17. *See also* Information security (IS), new framework proposal
- Convergence, 1·19
- Cookie poisoning, 21·18
- Cookies, 19·18, 21·8–21·9, 21·18–21·19, 48·24–48·25, 69·15
- COPS vulnerability assessment system, 46·3
- Copying, as means of information loss, 3·2, 3·16
- Copyright law:
  - copyright ownership, 11·8–11·9
  - database protection, 11·21
  - derivative works, 11·12
  - Digital Millennium Copyright Act, 11·13–11·18, 11·22–11·23
  - fair use exception, 11·9–11·12, 11·16–11·17, 11·21–11·23
  - first sale doctrine, 11·9
  - formulas, 11·10
  - hyperlinks, 11·23
  - infringement, 1·19, 11·12–11·14
  - interfaces, 11·11
  - international law, 11·34–11·39
    - and licensing, 11·9. *See also* Licenses and licensing
  - “look and feel” of software, 11·10–11·11
  - overview, 11·8, 42·2
  - registration of copyright, 11·9
  - remedies for infringement, 11·13–11·14
  - remedies for violation of DMCA, 11·18
  - and reverse engineering, 11·11, 11·16–11·17
  - Semiconductor Chip Protection Act, 11·12
  - transformative use, 11·11–11·12, 11·21–11·24
    - and TRIPS, 11·37
  - watermarks, use of, 42·11–42·12
  - works for hire, 11·8–11·9
- Core layers, 5·9–5·10
- Corporate culture. *See* Organizational culture
- Cost-benefit analysis, information infrastructure protection, 23·53
- Costs:
  - authentication technologies, 28·16
  - biometric authentication, 29·18
  - business continuity planning, cost justification, 58·29–58·34
  - Cost Effectiveness Tools*, 23·53
  - data backup systems, 57·26–57·28
  - denial-of-service attacks (DoS), 18·4–18·5
  - gateway security devices, 26·29–26·30
  - Generalized Cost Consequence (GCC) model, 58·6, 58·31–58·34
  - HIPAA compliance, 71·3, 71·20, 71·24–71·25
  - physical threats, 22·6, 22·13–22·14
  - Public Key Infrastructure (PKI), 37·26
  - spam, 20·6–20·7, 20·10–20·13
  - virtual private networks, 32·10
- Council for Responsible E-mail (CRE), 20·15
- Counter mode/CBC-MAC protocol (CCMP), 33·33–33·34, 33·39–33·40
- Counterfeit Access Device and Computer Fraud and Abuse Law, 73·2
- CoWPAtty, 33·37–33·38
- Crack, 15·24, 25·8
- Crackers, and information warfare, 14·17
- Crashes, 4·10
- Credit card fraud, 2·6, 2·26

## I • 12 INDEX

- Credit card transactions, 21•8
- Crime and criminals. *See also* Computer crime;  
Computer criminals; Cyber investigation  
investigations and privacy law, 69•8–69•9  
reporting, 22•3–22•4
- Criminal liability:  
and cooperation with law enforcement. *See*  
Law enforcement, cooperation with  
exposure of consumers' PII, 39•13  
and First Amendment rights, 72•12  
HIPAA violations, 71•19–71•20  
and litigation issues, 30•40
- Cross-certification, 37•13–37•14
- Cross-domain authentication, 28•15–28•16
- Cross-domain solutions (CDS), 75•2
- Cross-site request forgeries (CSRF), 21•19
- Cross-site scripting (XSS), 16•4–16•5, 21•19,  
26•13, 32•14
- CryptoCard, 28•13
- Cryptographic viruses, 16•5
- Cryptography, 7•3–7•16, 37•2. *See also*  
Encryption
- CTSS (Compatible Time Sharing System), 1•7
- Cult of the Dead Cow (cDc), 2•22–2•23
- Culture:  
corporate culture. *See* Organizational culture  
cultural differences, 50•10–50•11
- Customer relationship management (CRM)  
applications, 26•2
- Customers:  
business-to-customer security services,  
30•3–30•4, 30•9–30•13, 30•17  
defined under Gramm-Leach-Bliley Act  
(GLBA), 64•8  
and information security breaches, 63•4  
loss of, 30•23  
monitoring, 30•39
- Cyber investigation:  
analysis of individual events, 55•10, 55•16  
attack-tree analysis, 55•21, 55•24  
correlation, 55•11, 55•16–55•17  
cyber forensics compared, 55•2  
deconfliction of events, 55•11, 55•16  
describing attacks, 55•14–55•15  
end-to-end digital investigation (EEDI), 55•2,  
55•9–55•17  
end-to-end process, 55•9–55•12  
evidence, 55•10, 55•12, 55•16–55•17  
framework for, 55•2–55•9, 55•12–55•17  
intrusion process, 55•13–55•14  
investigative narrative, 55•12–55•13  
law enforcement agencies, 61•6–61•7. *See also*  
Law enforcement, cooperation with  
link analysis, 55•21–55•24  
means, 55•17–55•18, 55•20  
modeling, 55•21, 55•25  
motive, 55•17–55•20  
normalizing events, 55•11, 55•16  
opportunity, 55•17–55•18, 55•20  
overview, 55•1–55•9, 55•25  
Rogers taxonomy, 55•2–55•3  
strategic campaigns and tactical attacks,  
55•15–55•16  
threat agents, 55•17–55•20  
timeline analysis, 55•11–55•12, 55•17  
tools for, 55•20–55•25
- CyberCash, 21•10
- Cyberharassment, 70•2–70•3
- Cybersecurity Research and Education Act, 75•8
- Cybersex, 48•28–48•29
- Cyberspace, defined, 70•4
- Cyberterrorism, 12•3, 12•19, 12•22,  
14•15–14•16. *See also* Information warfare  
(IW)
- Cyberwar. *See* Information warfare (IW)
- Cylink, 7•27
- D**
- Daemons, 15•22, 15•25, 15•27, 18•5,  
18•15–18•18, 25•13
- DARPA. *See* Defense Advanced Research  
Projects Agency (DARPA)
- Dashboards, 53•2–53•3, 53•21–53•22
- Data:  
access to, 47•13. *See also* Access control  
aggregation, 53•19–53•21  
backups. *See* Data backups  
classification, 30•7, 66•5, 67•1–67•9  
collection, 53•2, 66•3–66•4  
communications, 4•13–4•16, 4•24  
corruption, 39•19, 52•2–52•3  
data life cycle management (DLM),  
57•17–57•20  
destruction, 30•7, 66•10  
dictionaries, 52•2  
diddling, 2•9–2•10, 3•15  
files, defined, 47•3–47•4  
grinding, 19•7  
integrity, 24•3, 47•16  
leakage, 15•7–15•8, 26•3  
mining, 19•7  
protection, 47•13–47•15  
reduction, 53•2  
repositories, 52•2  
retention, 30•7, 53•14  
scavenging, 15•17–15•18, 57•23  
security, 24•3  
sets, 52•4  
stacks, 53•9  
storage. *See* Data storage  
test data, 47•13–47•14  
theft, 4•21  
validation, 47•15–47•17  
vaults, 57•22
- Data backups:  
application backups, 57•14  
archives, 57•2, 57•11–57•12  
Blu-ray discs, 57•8

- buffer for processing during backup, 57•13
- CD-RW, 57•8
- Computer Output to Microfilm (COM), 57•20
- and computer systems, 57•15–57•17
- content-addressed storage (CAS), 57•12
- continuous data protection (CDP), 57•2–57•3
- costs of, 57•26–57•28
- daily, 57•15
- data life cycle management, 57•17–57•20
- data storage capacities, 57•2
- delta, 57•14
- differential, 57•2, 57•13–57•14
- and disaster recovery, 59•13
- disk mirroring, 57•3
- disposal of backup media, 57•23–57•25
- double, 57•2, 57•17
- DVD, 57•8
- evaluation phase, security policy development, 66•10
- external hard disk drives, 57•7–57•8
- files in inconsistent state, 57•13
- flash drives, 57•10
- frequency of, 57•26–57•28
- full, 57•13
- hierarchical storage systems, 57•3
- HIPAA requirements, 71•19
- holographic disks, 57•8
- incremental, 57•2, 57•14
- indexing, 57•11–57•12
- labeling, 57•10–57•11
- laptops, 57•16–57•17
- logging, 57•6
- mainframes, 57•15
- Millipede, 57•10
- mobile devices, 57•17
- need for, 57•1, 57•3
- network-attached storage (NAS), 57•4
- online, 57•22–57•23
- optical storage, 57•8–57•9
- parallel processing, 57•3
- partial, 57•15
- policies, 57•28
- recovery, 57•6
- recovery point objectives (RPO), 57•3
- redundant array of independent disks (RAID), 57•4–57•5, 57•22
- removable hard disk drives, 57•8
- removable media, 57•7
- servers, 57•15
- software for, 57•6–57•7
- storage area network (SAN), 57•4
- storage of, 57•20–57•23
- strategies, 57•12–57•17
- system backups, 57•14
- tape cartridge systems, 57•9
- technology selection, 57•12–57•13
- terminology, 57•2
- testing, 57•17
- Virtual Tape Library (VTL), 57•2, 57•9–57•10
- workstations, 57•4, 57•6, 57•15–57•16
- Data centers, 1•9
- Data dictionaries, 52•2
- Data diddling, 2•9–2•10, 3•15
- Data Encryption Algorithm (DEA), 7•20, 7•37
- Data Encryption Standard (DES), 7•2, 7•16, 7•19–7•22, 7•26, 7•37–7•38, 25•11, 37•2
- Data Execution Prevention, 25•11
- Data leakage prevention (DLP), 26•3
- Data life cycle management (DLM), 57•17–57•20
- Data mining, 19•7
- Data Protection Directive (EU), 11•29, 11•37, 49•4
- Data storage. *See also* Storage media
  - backup security, 36•4–36•5
  - best practices, 36•2–36•3
  - Common Internet File System (CIFS) exploits, 36•8–36•9
  - database encryption, 36•12–36•13
  - direct attached storage (DAS), 36•3
  - disposal of data, 36•13, 57•23–57•25
  - encryption, 36•9–36•13
  - fiber channel threats, 36•6, 37•7
  - file system access controls, 36•4
  - in-band management, 36•4
  - and management interfaces, 36•5–36•6
  - memory, 4•8–4•9
  - network attached storage (NAS), 36•3
  - network file system threats, 36•7–36•8
  - nonvolatile media, 36•1
  - out-of-band management, 36•4
  - overview, 36•1–36•2, 36•14
  - restore system controls, 36•4–36•5
  - secondary storage, 4•9–4•10
  - security basics, 36•2
  - storage area network (SAN), 36•3–36•4
- Database administrator (DBA), 21•20
- Databases:
  - attacks, 21•7–21•8
  - backout, 52•7
  - backup files, 52•6
  - copyright protection, 11•21
  - database management system (DBMS), 52•1–52•8
  - distributed, 52•7–52•8
  - encryption, 36•12–36•13
  - locking, 52•4–52•5
  - management subsystems, 53•3–53•4
  - privacy issues, 21•11
  - relational database management system (RDBMS), 52•1–52•2
  - roll-forward recovery, 52•7
  - security, 21•19–21•20
  - system logs, 52•6
- Dataveillance, 70•12–70•13
- Daubert v. Merrell Dow Pharmaceuticals*, 73•2–73•4. *See also* Expert witnesses

## I • 14 INDEX

- DDR-3 (Double Data Rate 3 SDRAM), 4•8
- Deadlocks, 52•5
- Debug utilities, 53•8
- Decryption, 7•2–7•3, 7•6, 7•8–7•10, 7•12–7•14, 7•22–7•24, 7•26, 7•31–7•32, 7•36, 7•43.  
*See also* Encryption
- Deducibility security, 9•18–9•19
- Defacement of Web pages, 15•26–15•27
- DefCon, 15•33
- Defense Advanced Research Projects Agency (DARPA), 1•13, 5•6, 7•41, 38•8, 56•4
- Defense in depth, 16•9, 16•11, 19•16, 21•5, 36•5–36•6, 53•3, 75•2–75•3
- Defense Information Systems Agency (DISA):
  - computer security incident training, 56•8–56•9, 56•11, 56•13, 56•24, 56•26–56•28
  - Security Technical Implementation Guides (DISA-STIG), 54•15
- Degaussing, 57•24–57•25
- Delta CRL, 37•20–37•21
- Demand priority, 6•17
- Demilitarized zone (DMZ), 26•18, 30•27, 30•32–30•34, 32•12
- Demon (war) dialing, 4•14–4•15, 15•15, 21•12
- Denial-of-service attacks (DoS). *See also*
  - Distributed denial-of-service (DDoS) attacks
    - accidental, 30•36
    - arnudp, 18•12
    - and autoforwarding e-mail, 48•22
    - bandwidth consumption, 18•7–18•9
    - boink, 18•12
    - bonk, 18•12
    - buffer overflow attacks, 18•7. *See also* Buffer overflow
    - costs of, 18•4–18•5
    - decline of, 55•14
    - defined, 8•15
    - against Department of Defense, 18•3, 18•5
    - destructive devices, 18•6
  - Domain Name System attacks, 5•24, 18•9–18•10
  - e-mail and e-mail subscription bombings, 18•6–18•7
  - history of, 2•20–2•21, 18•2–18•4
  - and information warfare, 14•18
  - and instant messaging, 35•9
  - and Java, 18•11
  - and LANs, 25•5
  - and loss of information, 3•15
  - mail bombing, 48•3
  - management issues, 18•27–18•28
  - overview, 18•1–18•2
  - Ping, 18•12
  - Ping of Death, 18•7, 25•14
  - prevention, 18•12–18•13
  - reactive detection, 53•2
  - resource starvation, 18•11
  - responding to, 18•12–18•13
  - router attacks, 18•12
  - routing and Domain Name System attacks, 18•9–18•10
  - SMURF, 18•8, 18•13
  - SYN flooding, 18•4, 18•10–18•11
  - types of, 18•5
  - Web site attacks, 15•26
  - and Windows XP, 25•11
  - and wireless local area networks (WLANs), 33•9
- Dense wave division multiplexing (DWDM), 6•10
- Department of Commerce, National Voluntary Laboratory Accreditation Program (NVLAP), 51•27
- Department of Defense (DoD):
  - CCEVS certified products, 51•29
  - and Common Language Project, 8•3
  - Computer Security Center, 24•13, 54•14–54•15
  - Computer Security Initiative, 1•13
  - Defense Advanced Research Projects Agency (DARPA). *See* Defense Advanced Research Projects Agency (DARPA)
  - denial-of-service attacks against, 18•3, 18•5
  - Directive 8570.1 and CISSP certification, 74•6–74•7
  - encryption algorithms, 7•2
  - and IPv6, 32•11
  - Policy 8500, 54•16
  - sanitizing electronic media, guidelines for, 36•13
  - Trusted Computer System Evaluation Criteria (TCSEC) (Orange Book)*. *See* *Trusted Computer Systems Evaluation Criteria (TCSEC) (Orange Book)*
- Department of Homeland Security (DHS), 1•16
  - Centers of Academic Excellence in Information Assurance Education (CAE), 74•4–74•5, 75•4–75•5, 76•13
  - guidelines for security management, 23•10–23•11
  - National Cyber Security Division, 38•13
  - National Incident Management System (NIMS), 23•3–23•4, 23•7
  - National Infrastructure Protection Plan (NIPP), 23•5
  - National Response Plan, 23•3–23•5, 23•7
  - and risk management, 23•55
  - and security auditing standards, 23•7
  - security planning and management procedures, 22•8, 22•10, 22•27
  - Vulnerability Discovery and Remediation Open Source Hardening Project, 51•10
- Department of Veterans Affairs, 63•6–63•10
- Destruction, disclosure, use, and modification (DDUM), 3•18
- Destruction of information, 3•2, 3•10–3•11, 3•14–3•15
- Dial-up phone lines, 15•9–15•10

- Dial-up server, 25·5
- Dialers, 16·6
- Diffie-Hellman algorithm, 7·20, 7·23–7·24, 7·35–7·36, 37·16
- Digital cash, 70·13
- Digital certificates, 7·31–7·35, 17·5, 17·8, 21·8, 32·15
- Digital coin payments, 21·11–21·12
- Digital Equipment Corp. (DEC), 1·7–1·8, 6·19
- Digital Forensics Research Workshop (DFRWS), framework for digital investigation, 55·2–55·9
- Digital information, reliance on, 65·4–65·5
- Digital investigation. *See* Cyber investigation
- Digital Millennium Copyright Act (DMCA), 11·13–11·18, 11·22–11·23, 31·8, 42·9–42·10, 42·12, 42·17
- Digital rights. *See also* Intellectual property
  - Digital Rights Management (DRM), 42·3, 42·13–42·14, 42·16–42·17
  - overview, 42·1–42·2
  - piracy. *See* Piracy
  - and privacy, 42·2
  - privacy-enhancing technologies, 42·14–42·15
  - problems with protecting, 42·15–42·16
  - terminology, 42·17–42·20
- Digital Rights Management (DRM), 42·3, 42·13–42·14, 42·14·16, 42·17
- Digital Signature Guidelines*, 37·8
- Digital Signature Standard (DSS), 37·22
- Digital signatures:
  - and Digital Rights Management, 42·14
  - Digital Signature Guidelines*, 37·8
  - Digital Signature Standard (DSS), 37·22
  - and e-mail, 21·7
  - and file system security, 53·13
  - and integrity checking, 46·4
  - and log record security, 53·18–53·19
  - production programs, validating, 47·8
  - and protecting Web applications, 21·8
  - and public key cryptosystems, 37·3–37·5, 37·11, 37·13, 37·15, 37·18, 37·20, 37·25–37·26
  - source code, 38·7, 47·9
  - validation controls, 52·10
- Digital Subscriber Line (DSL), 4·15–4·16, 5·3–5·4
- Digital Versatile Disk, 4·9
- Digital Video Disks (DVDs), 4·9, 36·1, 42·11, 57·19
- Direct Access File System (DAFS), 57·4
- Direct access storage devices (DASDs), 4·10
- Direct attached storage (DAS), 36·3, 36·5
- Direct memory access (DMA), 24·5–24·6
- Direct Sequence Spread Spectrum (DSSS), 6·12, 25·7–25·8
- Directory browsing, 21·18
- Dirt and dust, 4·12
- Disaster Mitigation Act of 2000, 23·6
- Disaster recovery. *See also* Business continuity planning (BCP)
  - business impact analysis. *See* Business impact analysis (BIA)
  - cold sites, 59·10
  - commercial recovery services, 59·12–59·13
  - and computer security incident response team, 56·7–56·8
  - data backup scenarios, 59·13
  - evaluation phase, security policy development, 66·11
  - and gateway security devices, 26·28
  - HIPAA requirements, 71·19
  - hot sites, 59·10, 59·16–59·18
  - implementation of plan, 59·20–59·21
  - internal redundancy, 59·11
  - mobile data centers, 59·11–59·12
  - and network access, 26·23
  - overview, 59·1, 59·21
  - phases, 59·7–59·9
  - postincident analysis, 56·31
  - priority replacement agreements, 59·12
  - reciprocal agreements, 59·10–59·11
  - recovery scenarios, 58·6–58·8
  - recovery strategies, 59·6–59·13
  - recovery tasks, 59·13–59·20
  - reserve systems, 59·13
  - scenarios, 59·3–59·6
  - testing of plan, 59·20–59·21
  - threats and threat assessment, 59·1–59·2. *See also* Threats
- Disclosure of information, 3·2, 3·16
- Discretionary access control list (DACL), 24·16, 24·18
- Discretionary access controls, 9·2, 9·6, 9·9
- Discussion groups, 48·9
- Disintermediation, 48·5
- Disk-based operating system (DOS), 1·9
- Disk space, log records for, 53·17
- Disks:
  - BD-R, 4·9
  - BD-RE, 4·9
  - compact-disk read-only memory (CD-ROM), 4·9
  - formatting, 57·24
  - holographic, 57·8
  - magnetic, 36·1
- Distributed access control, 6·3–6·4
- Distributed COM (DCOM), 21·13
- Distributed denial-of-service (DDoS) attacks:
  - Code Red Worm, 18·21, 18·25–18·26
  - defenses, 18·22–18·27
  - history of, 2·21, 18·13–18·14
  - and information warfare, 14·18
  - and intrusion detection response, 27·11
  - management issues, 18·27–18·28
  - and mobile code, 17·11
  - NIMDA, 18·21–18·22, 18·25–18·26
  - overview, 1·19, 16·7, 18·13–18·16

## I • 16 INDEX

### Distributed denial-of-service (DDoS) attacks

(Continued)

- real-time monitoring, 53•8
  - Shaft, 18•19–18•20
  - Stacheldraht, 18•13, 18•19
  - terminology, 18•14–18•15
  - tools, 18•16–18•20
  - Tribe Flood Network 2K (TFN2K), 18•19
  - Tribe Flood Network (TFN), 18•13, 18•18
  - Trinity, 18•13, 18•20
  - Trinoo (Trin00), 18•13, 18•17–18•19
- Distributed polling, 6•13–6•14
- DNSSEC, 5•25
- Do not call list, 11•29
- Document root, 21•17–21•18
- Documentation:
- changes, 39•17–39•18
  - computer security incidents, 56•15–56•19, 56•22
  - HIPAA, 39•15, 39•18, 71•18
  - preservation of records, 48•35
  - and regulatory compliance, 39•18
  - software development, 38•11, 39•10, 39•17–39•18
- Domain Name System (DNS):
- attacks, 21•12
  - and block lists, 31•5–31•6
  - cache poisoning, 5•24
  - denial-of-service attacks (DoS), 5•24, 18•9–18•10
  - DNS poisoning, 19•9
  - and host info (HINFO) resource record, 25•9
  - and network file system, 36•8
  - security, 5•24–5•25
  - server hierarchy, 5•25
  - and site names, 8•17
  - spoofing, 8•8, 17•9
  - updating DNS zones, 30•24
- Domain names, and certification authority, 37•17
- Dongles, 28•4, 28•13–28•14, 42•5–42•6. *See also* Locks and door hardware; Smart cards
- Dot dot attacks, 15•28–15•29
- Downloading software, 48•13
- Downtime, 4•13
- Driver's Privacy Protection Act, 69•8
- Due diligence:
- and business continuity planning, 58•3
  - and code security, 38•3–38•4
  - and information security framework, 3•14, 3•20
  - and record keeping, 56•12
  - and regulatory compliance, 71•1
  - and risk assessment, 63•20–63•21
- Dumpster diving, 15•18, 19•4, 19•6, 57•23
- Duties, separation of, 45•9–45•10, 47•4
- Dynamic Host Configuration Protocol (DHCP), 5•3, 34•11–34•12
- Dynamic link libraries (DLLs), 47•9
- Dynamic random access memory (DRAM), 4•8

### Dynamic routing protocols, 5•26

Dynamic rule modification, 26•12–26•13

Dynamic WEP, 33•20, 33•23

## E

E-business. *See* E-commerce

E-cash, 21•11–21•12

E-commerce:

- applications design, 30•26–30•27
  - business losses, 30•22–30•23
  - business-to-business security services, 30•13–30•17
  - business-to-customer security services, 30•3–30•4, 30•9–30•13, 30•17
  - ethical issues, 30•38
  - and extranets, 32•13
  - and hackers, 21•1, 22•2
  - insurance policies, 60•12–60•13
  - interruptions, 30•23
  - and just-in-time production, 30•23
  - and law enforcement cooperation, 30•19–30•20
  - legal issues, 30•38–30•42
  - loss of customers, 30•23
  - operational requirements, 30•24–30•30
  - overview, 1•12, 21•21, 30•2–30•3, 30•42
  - PR image, 30•22–30•23
  - risk analysis, 30•22–30•24
  - rules of engagement, 30•20–30•21
  - security framework, use of, 30•9–38•17
  - technical issues, 30•30–30•38
  - threat and hazard assessment, 30•24
  - threats, responding to, 30•24
  - vulnerabilities, 21•1–21•5, 21•8–21•21
  - Web application system security, 21•5–21•8
  - Web site protection, 30•17–30•21
- E-mail:
- addressing options, 20•14
  - anonymizing remailers, 42•15, 48•4, 70•9–70•10
  - antivirus systems, 16•10
  - appending services, 20•16
  - archiving, 48•35
  - attachments, malicious software. *See* Malware
  - authentication, 20•24–20•25
  - autoforwarding, 48•22
  - black holes, 20•19–20•20
  - blacklists, 20•4
  - block lists, 20•19–20•20
  - CC and BCC functions, 48•20–48•21
  - centralized distribution lists, 48•18
  - chain letters, 48•9–48•11, 48•14
  - content filtering, 19•16–19•17
  - corporate identifiers, 48•4–48•5
  - digital signatures, 21•7
  - disclaimers, 48•17–48•18
  - distribution lists, 48•20
  - employee misuse of, 48•3–48•4
  - encryption, 20•18–20•19

- flaming, 48·3–48·4
- forwarding, 48·15
- Group Mail, 20·14
- harvesting of addresses, 20·8
- headers, 20·5, 48·2, 48·8, 70·10
- hostile working environment, 48·3
- HTML, 28·2, 48·19–48·20
- impact of spam, 20·7–20·8
- inefficient use of, 48·15–48·21
- information about, obtaining, 20·5–20·6
- and Internet hoaxes, 48·6–48·11, 48·43
- junk e-mail. *See* Spam
- list servers, 48·22
- mail-bombing, 18·6–18·7, 48·3, 48·42
- mail storms, 18·7, 48·21–48·23, 48·42–48·43
- mass mailing, 20·13–20·16
- monitoring, 69·13
- multi-level marketing schemes, 48·10–48·11
- opt-out choice, 20·17
- overview, 48·2
- and pedophiles, 48·12–48·13
- permission issues, 20·16–20·17
- Ponzi schemes, 48·9–48·10
- private e-mail in the workplace, 48·21
- reply all, 48·20
- responsible practices, 20·15–20·16
- Simple Mail Transfer Protocol (SMTP), 5·27, 17·12–17·13
- Simple Mail Transport Protocol (SMTP), 20·3–20·5, 20·24
- as source of phishing attacks, 19·8. *See also* Phishing
- spam. *See* Spam
- subject line, 48·15–48·16
- and threats of physical harm, 48·12
- transfer standards, 5·27
- Unified Threat Management (UTM), 31·9
- unsolicited commercial e-mail (UCE). *See* Spam
- and viruses, 41·11
- whitelists, 20·4, 20·18, 20·21–20·22
- worms, 16·6
- E-Sign Bill. *See* Electronic Signatures in Global and National Commerce Act (E-Sign Bill)
- E-warfare. *See* Information warfare (IW)
- Earthquakes and tsunamis, 22·17. *See also* Physical threats
- Eavesdropping, 33·9, 33·17, 34·10–34·11
- EBay, 48·25
- Echo, 4·6, 5·23
- Echo reply, 5·23
- Edit checks, 47·15–47·16
- EFF DES Cracker, 7·20, 7·37
- Egress filtering, 18·12, 18·23, 18·25
- Election process and computer-aided voting, 77·16–77·19
- Electrical EPROMs (EEPROMs), 4·9
- Electrical power. *See* Power failures and disturbances
- Electromagnetic pulse attack (EMP), 22·21
- Electromagnetic pulses and magnetic fields and media storage, 57·20
- Electromagnetic radiation (EMR), 25·5. *See also* TEMPEST (Transient ElectroMagnetic Pulse Emission Standard)
- Electronic Communications Privacy Act (ECPA), 11·30, 30·40, 34·4, 69·8, 69·14
- Electronic Data Interchange (EDI), 32·13, 71·12
- Electronic Health Records, 71·11, 71·15
- Electronic Healthcare Network Accreditation Commission (EHNAC), 71·26
- Electronic Signature Act of 2000 (E-Sign Act), 71·8
- Electronic Signatures in Global and National Commerce Act (E-Sign Bill), 42·14
- Elliptic curve cryptography, 7·35–7·36
- Embedded systems, 1·14
- Emergency Management Assessment Program (EMAP), 22·10, 23·7
- Emergency Operations Plan, 23·6
- Emergency power, 23·38–23·44
- Emergency response plans, 22·9–22·10. *See also* Business continuity planning (BCP); Disaster recovery; Physical site security
- Emergency Support Functions (ESF), 23·54
- Emerging technologies, 30·38
- Employees:
  - abuse, opportunities for, 45·4
  - access issues, 13·2, 13·8, 45·4
  - background checks, 13·2, 13·6–13·8, 16·9, 45·2–45·3
  - backup plans, 4·18
  - behavioral changes, 45·7–45·9
  - blogs, 48·5
  - career advancement, 45·6–45·7
  - and computer crime, 45·1–45·2
  - confidentiality agreements, 45·14
  - cross-training, 45·4–45·6
  - dangerous insiders. *See* Insiders, information technology
  - downloads, 19·18
  - duty of loyalty, 11·3
  - e-mail monitoring, 69·13
  - employment agreements, 11·4, 45·3
  - extranet services for, 32·13
  - fiduciary duties, 11·3, 11·29
  - health and safety issues, 22·3, 22·17, 23·50–23·51, 58·14
  - identification and authentication issues, 28·16
  - indispensable, 45·4–45·6
  - Internet use, policies on, 48·44. *See also* Internet
  - key person and alternate, business impact analysis, 58·20
  - and management practices, 45·3–45·10, 45·15
  - mobility of, 26·2
  - motivation, 63·12–63·14
  - noncompetition agreements, 45·14–45·15



## I • 18 INDEX

- Employees (*Continued*)  
online games and virtual reality, 49•29  
overview, 45•15  
personal Web sites, 48•5  
productivity, threats to, 48•14–48•29  
reward and punishment, 50•13, 50•15, 63•13  
security awareness programs. *See* Awareness programs  
security policy implementation, 66•13–66•14  
separation of duties, 45•9–45•10  
shiftwork, 56•29–56•30  
and social engineering. *See* Social engineering and social networking, 48•5  
social psychology, use of in implementing security policies. *See* Social psychology  
stress, 13•4–13•6  
supervision, 63•14–63•15  
termination, 13•2, 13•8, 45•10–45•15  
training. *See* Training  
and unauthorized security probes, 45•10  
vacation time, 45•7  
Web monitoring, 31•3–31•4, 69•13–69•14.  
*See also* Web monitoring
- Employment agreements, 11•4, 45•3
- Enclaves, 17•1–17•3, 17•12. *See also* Mobile code
- Encrypting File System (EFS), 25•11
- Encryption:  
additional decryption keys (ADKs), 36•10  
Advanced Encryption Standard (AES), 7•38, 7•42–7•43  
algorithms, 7•2–7•3, 37•15–37•16, 37•22  
and applications design, 30•26–30•27  
authenticity and trust, 7•25–7•26  
biometric encryption, 29•20–29•21  
brute force cryptanalysis, 7•9–7•11, 7•17, 21•12, 37•21  
Caesar cipher, 7•4, 7•7–7•11  
cell phones, 15•12  
ciphers, 4•17, 7•2, 7•6–7•16, 7•18–7•19  
ciphertext, 7•2–7•3, 37•2–37•3, 53•19  
codes, 7•2  
communications, 7•27–7•35  
cryptography, 7•3–7•16, 37•2  
cryptology, 7•2  
cryptoviruses, 16•5  
data backups, 36•5  
data encryption, 37•22–37•24  
Data Encryption Algorithm (DEA), 7•20, 7•37  
Data Encryption Standard (DES), 7•2, 7•16, 7•19–7•22, 7•26, 7•37–7•38, 25•11  
data storage, 36•9–36•13  
databases, 36•12–36•13  
decryption, 7•2–7•3, 7•6, 7•8–7•10, 7•12–7•14, 7•22–7•24, 7•26, 7•31–7•32, 7•36, 7•43  
defined, 31•2  
digital certificates, 7•31–7•35  
Digital Rights Management. *See* Digital Rights Management (DRM)  
double encryption, 7•20  
e-commerce security services, 30•6  
EFF DES Cracker, 7•20  
elliptic curve cryptography, 7•35–7•36  
Encrypting File System (EFS), 25•11  
file system security, 53•13  
frequency analysis, 7•12–7•13, 7•15–7•17  
and information warfare, 14•19  
ISO/IEC/ITU 9594-8 (X.509). *See* X.509 certificate format  
key escrow, 36•10  
key-exchange problem, 7•8, 7•22–7•23  
keys, 4•17, 7•2  
keyspace, 7•3, 7•10, 7•20, 7•22, 15•15–15•16  
limitations of, 7•6  
and log record security, 53•18–53•19  
Message Authentication Code (MAC), 7•4–7•5, 7•29, 38•7  
mobile data systems, 1•18  
modern techniques, development of, 7•15–7•19  
need for, 4•16–4•17  
one-time pad, 7•17–7•18  
overview, 7•1–7•2  
and password cracking, 15•24  
passwords, 28•9–28•11  
plaintext, 7•2–7•3, 7•6  
Point-to-Point Encryption, 25•7  
private keys, 7•5, 7•8, 7•26–7•27, 7•31–7•32, 7•43  
public key, 5•27, 7•5, 7•22–7•27, 7•36–7•37, 7•43, 28•10–28•11, 31•2  
Public Key Infrastructure (PKI). *See* Public Key Infrastructure (PKI)  
quantum cryptography, 7•38–7•42  
RC4, 7•29–7•30  
RSA algorithm, 7•24–7•27, 7•35–7•37  
Secure Sockets Layer (SSL), 7•28–7•30  
and security controls, generally, 3•14  
SEEK, 7•27  
steganography, 31•11  
terminology, 7•2–7•3  
Transport Layer Security (TLS), 7•28–7•30  
transposition, 7•18–7•20  
trust, 37•2  
and VoIP, 34•13–34•14  
Web applications, protecting, 21•7  
and Web monitoring, 31•11  
wireless networks, 15•12, 25•7–25•8  
X.509 certificate format. *See* X.509 certificate format  
XOR (Exclusive-Or), 7•15–7•16
- End point protection, 26•13–26•14
- End-to-end digital investigation (EEDI). *See* Cyber investigation
- End user license agreement (EULA), 16•6–16•7

- Endangerment, 3•2, 3•17–3•18
- Enhanced Interior Gateway Routing Protocol (EIGRP), 5•26
- Ensconce Data Technology, 57•25
- Enterprise applications, 26•2
- Enterprise JavaBeans (EJB), 21•13
- Enterprise resource planning (ERP) systems, 32•12
- Enumerating, 55•13–55•14
- Environment. *See* Physical threats
- Equipment cabinets, 23•17–23•18, 23•31–23•35
- Erasable, programmable read-only memory (EPROM), 4•9
- Errors:
  - attribution errors, 50•7–50•10
  - biometric authentication crossover error rate (equal error rate), 29•15–29•16
  - calculation errors, 38•9, 39•8
  - codes and coding, 16•10, 21•7, 38•7–39•12, 38•8–38•13, 39•7–39•12
  - control (command) structure errors, 38•11–38•12, 39•11
  - functionality errors, 38•11, 39•10
  - initialization errors, 38•8–38•9, 39•7–39•8
  - input, 52•9
  - load condition errors, 38•10, 39•8–39•9
  - logic flow errors, 38•9, 39•8, 52•3
  - output format errors, 38•12–38•13, 39•11–39•12
  - parameter-passing errors, 38•9, 39•8
  - performance errors, 38•12, 39•11
  - performance (speed) errors, 38•12
  - program conflict errors, 38•10, 39•9
  - programming, 52•3
  - race conditions, 38•9–38•10, 39•9, 39•14, 52•4
  - resource exhaustion errors, 38•10, 39•9
  - software errors, types of, 38•8–38•13, 39•7–39•12
- E.T. applications, 48•13
- Ethereal, 25•4, 33•37–33•38
- Ethernet, 1•10, 5•12, 6•3, 6•23
- Ethernet II, 6•19–6•20
- Ethics:
  - and computer crime, 12•12–12•15
  - consequentialism (teleology), 70•17
  - customer monitoring, 30•39
  - defined, 43•1–43•2
  - and dummy security devices, 23•19
  - importance of, 43•1–43•2, 43•7–43•8
- Information Systems Audit and Control Association (ISACA), 74•9–74•12
- Institute of Internal Auditors (IIA) code of ethics, 74•8
- International Information Systems Security Certification Consortium (ISC), 74•12, 74•14
- and penetration testing, 46•9–46•10
- principles, 43•2–43•7, 70•17–70•18
- resources, 43•7
- responsibility for, 43•7
- rights and duties (deontology), 70•17
- and surveillance systems, 23•29
- and Web site management, 30•38–30•40
- EU Data Protection Act, 65•13
- EU Data Protection Directive 95/46/EC, 69•4–69•6
- and codes of conduct, 69•18
- implementation of, 69•4, 69•6
- U.S./EU safe harbor, 69•5, 69•12–69•13, 69•18
- EU Telecommunications Directive, 69•6
- Europe, educational system:
  - applied universities (technical schools), 76•10–76•12
  - art and science, 76•8–76•11
  - bachelor's degree requirements, 76•4–76•5, 76•14
  - Bologna Declaration, 76•2–76•17
  - computer science terminology, 76•4
  - Continuous Masters program, 76•9, 76•11–76•12, 76•14–76•15
  - course credits, 76•3–76•8
  - declarative knowledge, 76•9
  - graduate programs, 76•5–76•8
  - implications of standardization, 76•15–76•17
  - information assurance, courses on, 76•13
  - information assurance, use of term, 76•4, 76•12
  - information security curriculum, 76•10–76•11, 76•13–76•14
  - information security degrees, 76•3
  - malware, courses on, 76•13–76•14
  - and mathematics, importance of, 76•8, 76•15–76•17
  - Specialized Master's degrees, 76•8–76•9, 76•11–76•15
- European Credit Transfer and Accumulation System (ECTS), 76•3–76•8
- European Data Protection Supervisor, 69•6
- European Union Data Protection Directive 95/46/EC. *See* EU Data Protection Directive 95/46/EC
- Evaluation Assurance Levels (EALs), 51•20
- Evanescent media, 42•10
- Events, 8•4–8•11. *See also* Security incidents
- Evidence. *See also* Cyber investigation
  - chain of custody, 55•12, 55•17, 61•7–61•8
  - collecting, 55•10, 55•16
  - corroboration of, 55•12, 55•17
  - and cyber investigation. *See* Cyber investigation
  - law enforcement agencies, cooperation with, 61•7–61•8
- Exam preparation, 74•19–74•20
- Exception reports, 53•23
- Executive Order 12958, 67•5–67•6

## I • 20 INDEX

- Executives. *See also* Management  
chief information officer (CIO), 22•7, 63•2  
chief information security officer (CISO). *See*  
Chief information security officer (CISO)  
chief technology officer (CTO), 63•2  
physical security, responsibility for, 22•6–22•7
- Expert witnesses:  
admissibility of scientific evidence, 73•1–73•4  
appearance, 73•6  
background, 73•1–73•2  
*Daubert v. Merrell Dow Pharmaceuticals*,  
73•2–73•4  
Federal Rules of Evidence, 73•1–73•2  
fees, 73•5  
*Frye v. United States*, 73•1  
*General Electric Co. v. Joiner*, 73•3  
*Kumho Tire Co. v. Carmichael*, 73•3  
overview, 73•6  
preparation for testimony, 73•4–73•6  
pretrial meetings, 73•6  
qualifying as, 73•4–73•5  
state law, 73•4  
written report, 73•5–73•6
- Extended Key Usage, 37•6
- Extensible Markup Language (XML), 17•2,  
21•13
- Extortion, 2•11
- Extranets, 32•11–32•15
- F**  
414s, 2•22  
Fabric Login (FLOGI), 36•7  
Facebook, 48•5  
Facilities security. *See* Physical site security  
Fair and Accurate Credit Transaction Act of 2003,  
11•29  
Fair use. *See* Copyright law  
False Claims Act, 71•8  
False data, 3•2, 3•15  
Family Educational Rights and Privacy Act,  
67•3  
Faraday cages, 22•21, 25•5  
Federal Acquisitions Regulation Council, 71•10  
Federal Bureau of Investigation (FBI):  
adversarial matrix of behavioral characteristics,  
55•18–55•20  
adversarial matrix of operational  
characteristics, 55•20–55•21  
adversarial matrix of resource characteristics,  
55•20, 55•22  
Bot Roast II, 17•11  
Carnivore program, 69•9  
DCS1000, 69•9  
InfraGard, 1•13, 1•18, 22•27, 61•12, 70•13  
Project Megidido report, 22•6  
reporting threats and incidents to,  
23•49–23•50, 61•6–61•7  
as source of threat information, 22•27  
and use of spyware, 17•3  
Federal Communications Commission (FCC),  
34•3–34•5  
Federal Emergency Management Agency  
(FEMA):  
*Cost Effectiveness Tools*, 23•53  
guidelines for security management,  
23•10–23•11  
Independent Study Program (ISP), 75•9  
Publication 386-2, *Understanding Your Risks*,  
23•52  
Publication 386-4, *Bringing the Plan to Life*,  
23•54  
and regulatory compliance, 23•4  
and risk management, 23•55–23•56  
and security auditing standards, 23•7  
security planning and management procedures,  
22•8, 22•10  
*State and Local Mitigation Planning* guides,  
23•42  
Federal Information Processing Standard (FIPS)  
Publications:  
FIPS 46, 7•20  
FIPS 197, Advanced Encryption Standard, 7•38  
FIPS 200, 54•16  
Federal Information Security Management Act  
(FISMA), 49•4, 49•35, 50•4, 54•5, 54•15,  
65•13, 71•8–71•9, 75•7  
Federal Information System Controls Audit  
Manual (FISCAM), 54•16  
Federal Information System Management Act  
(FISMA), 54•17–54•18, 71•f1  
Federal Rules of Civil Procedure (FRCP), 26•3,  
57•12, 57•18, 67•5  
Federal Rules of Evidence (FRE), 73•1–73•2  
Federal Trade Commission (FTC):  
and Gramm-Leach-Bliley Act enforcement,  
64•7, 69•10  
and privacy breaches, 60•13–60•14  
privacy law enforcement, 69•18  
reporting identity theft to, 61•6  
unfair and deceptive trade practices,  
investigation of, 69•18  
Fiber channels, 36•3, 36•6–36•7  
Fiber Distributed Data Interface (FDDI), 6•14  
Fiber optic cable, 15•10, 22•19–22•20  
Fiber Optics Technology Advisory Group  
(FOTAG), 6•17  
File close log record, 53•16  
File I/O (input/output) log, 53•16  
File infector viruses, 16•4  
File open log record, 53•16  
File sharing, 11•23–11•24, 24•10–24•11  
File system activities, 53•12–53•13  
File Transfer Protocol (FTP), 5•27, 21•12,  
30•36  
Financial industry:  
Basel Committee on Banking Supervision,  
65•3  
biometric authentication, use of, 29•22

- privacy laws, 69·10–69·11. *See also* Gramm-Leach-Bliley Act (GLBA); Privacy
  - Financial Institution Reform Recovery and Enforcement Act (FIRREA), 64·8
  - Financial Services Modernization Act of 1999. *See* Gramm-Leach-Bliley Act (GLBA)
  - Finland, 7·37
  - Fire and smoke, 22·22, 23·16–23·17, 23·46–23·48, 53·11, 59·18–59·19. *See also* Disaster recovery
  - Firewalls. *See also* Gateways
    - access control lists, 26·5–26·6
    - appliance, 26·9
    - application-layer gateway, 26·7
    - architectures, 26·5–26·8
    - background, 26·1–26·2, 26·4–26·10
    - and cable, 4·16
    - and changing security landscape, 26·2–26·3
    - deployment, 26·17–26·23
    - embedded, 26·10
    - encryption, 26·14–26·15, 26·18–26·19. *See also* Encryption
    - evaluation of network security devices, 26·23–26·33
    - gateway security device as replacement for, 26·24
    - as gateway security devices (GSDs), 26·3
    - host-based, 26·8–26·9
    - and host environment, 26·7–26·8
    - and internal partitions, 30·25–30·26
    - intrusion detection. *See* Intrusions
    - and IP addresses, 5·15
    - and Linux, 63·28
    - and malicious code, 16·10
    - managed security service provider (MSSP), 26·32
    - management, 26·19–26·23
    - and mobile code, 17·3
    - monitoring, 26·19
    - monolithic, 30·32
    - multifunction hybrids, 26·7
    - and network operating systems, 25·16
    - network security mechanisms, 26·10–26·17
    - operating system security, 21·20–21·21
    - overview, 26·32–26·33
    - packet filtering, 26·6
    - penetration testing, 26·20–26·21
    - platforms, 26·8–26·10
    - policy, 26·19–26·20
    - routers, 5·3, 26·8
    - stateful inspection, 26·5–26·7, 26·10
    - and use of RFC 1918 addresses, 30·31
    - virtual, 26·9–26·10
    - and virtual private networks, 32·5
    - and VoIP, 34·11
    - Web application, 26·4
    - and Web application protection, 21·7–21·8
    - and Web monitoring, 26·15, 31·8–31·9
    - Windows XP, 25·11
  - First Amendment, U.S. Constitution, 48·4, 72·2, 72·7–72·17
  - Flag fields, 5·19
  - Flash, 26·16
  - Flash drives, 1·18, 21·9, 36·1, 41·12, 57·19, 57·24
  - Flash memory, 4·9–4·10
  - Flashing, 4·9
  - Flooding, 22·16, 22·23. *See also* Physical threats
  - Fuhrer, Mantin, and Shamir (FMS) attacks, 33·19–33·20
  - Flux bot, 15·30
  - Focus groups and computer crime research methods, 10·9–10·10
  - Footprinting, 55·13
  - Foreign Intelligence Surveillance Act (FISA), 34·4
  - Forum of Incident Response and Security Teams (FIRST), 56·34
  - Fraggle attacks, 18·8
  - Frame Relay networks, 5·5
  - Frames, 5·3, 5·7–5·8, 5·11–5·12
  - Framework for information security. *See* Information security (IS), new framework proposal
  - France, 72·2, 72·4
  - Fraud:
    - advance fee fraud, 2·20, 16·10, 19·8
    - and biometric authentication, 29·18, 29·29
    - credit card fraud, 2·6, 2·26
    - digital certificates, 17·8
    - and get-rich-quick schemes, 48·11, 48·43–48·44
    - healthcare IT risks and vulnerabilities, 71·4
    - insurance coverage, 60·11
    - loss of possession of information, 3·14
    - Nigerian 411/419 fraud (advance-fee fraud), 2·20, 16·10, 19·8
    - and online auctions, 48·25
    - as security threat, 1·19
    - as source of loss, 3·10–3·11
  - Free speech. *See* First Amendment, U.S. Constitution
  - Freedom of Information Act (FOIA), 69·7–69·8
  - Freeware, 48·41
  - Frequency Hopping Spread Spectrum (FHSS), 6·11–6·12, 15·11, 25·7–25·8
  - Friendster, 48·5
  - Frye v. United States*, 73·1
  - FTP. *See* File Transfer Protocol (FTP)
  - Functional requirements, security, 51·19–51·21
  - Functionality errors, 38·11, 39·10
- G**
- Garbage in, garbage out (GIGO), 52·2, 52·9
  - Gases as security hazard, 3·17
  - Gates, Bill, 1·9

## I • 22 INDEX

- Gateways. *See also* Routers  
application layer gateways (ALGs), 26•7, 34•11  
Border Gateway Protocol (BGP), 5•22, 5•26  
Common Gateway Interface (CGI), 15•26, 21•2–21•3, 21•13–21•15, 21•17  
Enhanced Interior Gateway Routing Protocol (EIGRP), 5•26  
gateway security devices (GSDs), 26•3, 26•19–26•21, 26•23–26•33, 32•10. *See also* Firewalls  
terminology, 5•7  
and VoIP, 34•11
- General Accounting Office (GAO), 54•16
- General Agreement on Tariffs and Trade (GATT), 11•35
- General Electric Co. v. Joiner*, 73•3
- General Public License (GPL), 11•33–11•34
- Generalized Cost Consequence (GCC) model, 58•6, 58•31–58•34
- Generation gap, technological, 50•21–50•22
- Genetic Information Nondiscrimination Act, 69•16
- Germany, 44•9, 72•3–72•4, 76•10
- Getronics Security University, 74•22–74•23
- Gibibytes, 4•4
- Glass box testing approach, 39•14
- Global Information Assurance Certification (GIAC), 74•15–74•16, 75•3
- Global Information Grid (GIG), 53•7
- Global Technology Audit Guide—Information Technology Controls (GTAG-ITC), 62•3–62•5
- Globalization, 65•5–65•6, 68•4, 69•1–69•2, 76•15. *See also* Outsourcing
- Google:  
background checks, 45•3  
and collaboration tools, 35•3, 35•16. *See also* Collaboration tools  
and Internet censorship, 72•6–72•7  
*Perfect 10* litigation, 11•23  
report on malware, 15•30  
Safe Search, 31•12
- GotoMyPC, 32•10
- Government:  
and anonymity in cyberspace, 70•20–70•21  
biometric authentication, 29•21  
censorship, 72•2–72•15  
and healthcare services, 71•7  
and privacy law, 69•7  
role of in cyberspace, 70•20–70•21  
role of in information assurance, 1•13
- Government Accountability Office (GAO), 63•8
- Gramm-Leach-Bliley Act (GLBA):  
applicability, 64•6–64•7  
compliance evaluation procedures, 64•11–64•14  
consumer defined, 64•8  
customer defined, 64•8  
and data classification, 67•4  
and data management, 57•17  
and documentation of changes, 39•18  
due diligence, 71•1  
electronic communications and privacy, 11•29  
enforcement, 64•7–64•8  
flexibility, 64•10–64•11  
metrics, 49•35  
nonpublic personal information, 60•16  
overview, 64•6, 64•11, 64•14  
penalties, 34•6  
personally identifiable information, 26•2, 57•17  
privacy notices, 64•9–64•10  
provisions of, 54•5–54•6, 64•9, 69•10–69•11  
Safeguards Rule, 64•10–64•11  
security awareness training, 49•4  
security levels, 64•10–64•11  
and security planning, 23•6  
standard of care, 65•13  
and VoIP compliance, 34•2–34•3, 34•8
- Gray box testing, 38•14
- Groupthink, 50•20–50•21
- GTAG Information Technology Controls (GTAG-ITC), 62•3–62•5
- ## H
- Hackers:  
attackers, categories of, 8•16  
and computer criminals, 12•2, 12•16  
and e-commerce systems, 21•1–21•5. *See also* E-commerce  
ethics, 12•12–12•15  
hacking approach to product security  
assessment, 51•11  
history, 2•21–2•26  
and information warfare, 14•17  
insiders, 13•6–13•7  
and link analysis, 55•22–55•23. *See also* Cyber investigation  
motivation, 4•21  
penetration techniques, 15•3–15•4, 15•6. *See also* System and network penetration  
proprietors, 13•7–13•8  
protecting against, 48•44  
and social engineering, 19•3. *See also* Social engineering  
and software development, 39•19–39•20  
support groups, 15•33–15•34  
workplace issues, 48•32
- Haephrati, Michael, 2•13–2•14
- Handbook for Computer Security Incident Response Teams (CSIRTs)*, 56•5
- Handshake protocols, 7•28–7•29, 25•9–25•10, 34•13
- Harassment and anonymity in cyberspace, 70•2–70•3
- Hard drives, 4•10, 57•23–57•25

- Hardware. *See also* Computers
- antipiracy techniques, 42•5–42•12
  - backup plans, 4•18–4•19. *See also* Backups
  - binary design, 4•2–4•4
  - cryptography. *See* Encryption
  - data communications, 4•13–4•16
  - and data corruption, 52•2–52•3
  - drivers, 6•26
  - interrupts, 4•7–4•8
  - memory, 4•8–4•9
  - obsolete, 57•20
  - operations, 4•6–4•7
  - parity, 4•4–4•6
  - personal computers, 4•20–4•25
  - physical and environmental threats, 4•11–4•13
  - recovery procedures, 4•20
  - role of in computer security, 4•2
  - secondary data storage, 4•8–4•10
  - security checklist, 4•25–4•27
  - security program, need for, 4•25
  - threats, 24•3
  - time functions, 4•10–4•11
  - tokens, 7•30, 28•14
- Harvard University Extension School, 75•10
- Hash totals, 46•4, 52•9
- Hashed Message Authentication Code (HMAC-SHA1), 34•14
- Hate speech, 48•32–48•33, 48•36–48•37, 72•3–72•4
- Hazardous materials, 22•21
- Health and Human Services (HHS), Centers for Medicare and Medicaid Services (CMS), 54•16, 71•8, 71•12, 71•14
- Health and safety issues:
  - and business continuity planning, 58•14
  - pandemics, 22•3, 22•17, 23•50–23•51. *See also* Physical threats
- Health Care Finance Agency (HCFA), 71•9
- Health Information Trust Alliance (HITRUST), 71•26
- Health Insurance Portability and Accountability Act (HIPAA). *See also* Medical records
- Administrative Simplification regulations, 71•8, 71•12–71•13
  - benefits of, 71•20–71•21
  - and business continuity planning, 58•3
  - compliance issues, 54•5, 54•15, 71•20–71•26
  - costs of compliance, 71•3, 71•20, 71•24–71•25
  - covered entities, 71•13
  - and data classification, 67•2–67•4
  - and data management, 57•17
  - documentation, 39•15, 39•18, 71•18
  - electronic communications and privacy, 11•29
  - Electronic Data Interchange (EDI) transactions, 71•12
  - enforcement, 71•13, 71•19–71•20
  - government-provided healthcare, 71•7
  - liability, 71•19–71•20
  - metrics, 49•35
  - and monitoring and control systems, 53•4–53•5
  - overview, 71•1–71•2, 71•11–71•12
  - penalties, 34•6, 71•13, 71•19–71•20, 71•24
  - privacy regulations, 71•13–71•16
  - protected health information, 26•2, 60•16–60•17, 71•12–71•26
  - provisions of, 69•11–69•12
  - and RFID badges containing personally identifiable information, 53•25
  - security awareness and training, 49•4
  - and security planning, 23•6
  - security regulations, 17•19, 71•13–71•15, 71•17–71•18
  - standard of care, 65•13
  - and VoIP compliance, 34•2–34•3, 34•7–34•8
- Health threats, 22•3, 22•17, 23•50–23•51. *See also* Physical threats
- Healthcare industry:
  - biometric authentication, use of, 29•22
  - costs and role of IT, 71•3
  - HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)
  - information assurance, importance of, 77•14, 77•16
  - medical records. *See* Health Insurance Portability and Accountability Act (HIPAA); Medical records
- Heating, ventilation, and air conditioning (HVAC), 23•16–23•17, 23•44–23•46
- Help desk, 19•4–19•5, 56•19, 56•25, 56•27–56•28
- Help files, 44•14
- Heuristic malicious code detection, 16•8–16•9
- Heuristics, 53•11
- Hidden fields, 21•16–21•17
- High-energy radio-frequency (HERF) weapons, 22•21
- High Level Interface (HLI), 6•16
- Homeland Security Presidential Directives, 23•3–23•6, 71•10, 75•f12
- Honey pots, 63•22
- Honeynet Project, 63•13
- Host:
  - defined, 5•2
  - rogue or counterfeit, 36•9
  - scanners, 40•16
  - trusted, 36•8–36•9
- Host Intrusion Prevention System (HIPS), 2•14, 26•9, 53•11
- Hostile work environment, 48•32–48•35, 72•16
- Hot spots, 33•24–33•25
- Hotfix. *See* Software patches
- HP, 51•29
- HTML. *See* Hypertext Markup Language (HTML)
- HTTP. *See* Hypertext Transfer Protocol (HTTP)
- HTTPS, 30•27–30•28, 30•32, 30•38

## I • 24 INDEX

- Hubs, 6•23–6•25
- Human-machine interface (HMI), 53•2,  
53•6–53•7, 53•22–53•23, 77•15–77•16
- Humidity, 4•12, 22•23, 23•45–23•46, 53•11
- Hurricane Katrina, 22•2, 22•10, 22•17
- Hyperlinks, 11•23, 44•13–44•14
- Hypertext Markup Language (HTML), 5•27,  
15•27, 17•2, 17•13, 21•16–21•18, 28•2,  
44•13–44•14, 48•19–48•20
- Hypertext Processing (CGI/PHP), 21•13
- Hypertext Processor (PHP), 15•29
- Hypertext Transfer Protocol Daemon (HTTDP),  
15•27
- Hypertext Transfer Protocol (HTTP), 5•10, 5•27,  
21•7, 21•10, 21•12, 30•11–30•12, 30•15,  
30•27–30•28, 30•32
- Hypothesis testing, 10•4–10•5
- I**
- IBM:
  - and Christmas Tree worm, 18•2, 18•4
  - computers, 1•5, 1•6•1•7, 1•7–1•10, 26•4
  - crypto-coprocessor cards, 7•30
  - Data Encryption Standard, 7•19–7•20
  - and Digital Rights Management, 42•13–42•14
  - Electronic Media Management System, 42•14
  - Lucifer product cipher, 7•19–7•20
  - memory protection, IBM System/370, 24•5
  - Millipede, 57•10
  - Predictive Failure Analysis (PFA), 4•10
  - product ciphers, 7•19
  - product validation, 51•29
  - quantum computing, 7•41–7•42
  - System/370, 24•5
  - Token Ring, 6•9, 6•14, 6•20–6•22
  - Virtual Machine technology, 17•12
  - Virtual Tape Server, 57•9
- IBv4, 21•7
- ICSA Labs, 41•6, 51•12
- Idaho State University, 75•8–75•9
- Identification:
  - defined, 28•2
  - digital certificates, 32•15
  - e-commerce security services, 30•6
  - federal employees and contractors, 28•15
  - importance of, 29•2
  - and information systems security, 15•2
  - issues, 28•16–28•17
  - and operations security, 47•5
  - software versions, tracking, 47•6–47•7
  - verification, 29•5–29•6
- Identity, 70•4, 70•8. *See also* Anonymity
- Identity theft, 1•18–1•19, 60•13–60•18, 70•2,  
71•4
- IEEE 488 standard, 44•3
- IEEE 802 standards, 4•16, 5•3, 5•5, 5•12,  
6•13–6•14, 6•16–6•23, 25•7,  
33•14–33•36, 33•39–33•44, 53•10
- Impersonation, 19•4
- Implementing Recommendations of the 9/11  
Commission Act, 75•12
- Incidents, security. *See* Security incidents
- Incremental information leveraging, 15•6–15•7
- Industrial control systems (ICSs), 53•5, 53•11,  
53•24
- Inference, in statistics, 10•4, 10•8
- Information Assurance Courseware Evaluation  
(IACE) Program, 74•4–74•5
- Information assurance (IA):
  - awareness, literacy, training, and education  
continuum, 75•5–75•8
  - certifications. *See* Certification
  - distance learning, 75•9–75•12
  - education and training initiatives, 75•1
  - education programs in Europe. *See* Europe,  
educational system
  - education programs in the U.S., growth of,  
75•4–75•5
  - future of. *See* Information assurance (IA),  
future of
  - government's role, 1•13
  - importance of, 75•8–75•9
  - and learning continuum, 75•5–75•8
  - model, 75•8
  - NRC System Security Study Committee results  
and recommendations, 1•13–1•16
  - and recoverability of data, 36•9–36•10
  - standards, 1•13. *See also* Standards
  - studies and recommendations, 1•13–1•15,  
1•16•1•17
  - Trusted Information Environment (TIE) model,  
75•1–75•4
- Information assurance (IA), future of:
  - best practices, 77•10–77•12
  - composition analysis, 77•6–77•7
  - computer-aided voting example, 77•16–77•19
  - dependencies analysis, 77•7
  - development tools, 77•9
  - and education and training initiatives, 75•1,  
75•13
  - guarantees, 77•5
  - integrated, 77•5
  - measures of assurance, 77•9
  - methodologies, impact of, 77•5
  - overview, 77•3–77•5, 77•19–77•21
  - property transformation analysis, 77•7
  - requirements analysis, 77•5–77•6
  - risk abatement, 77•9
  - risk analysis, 77•9
  - software and hardware consistency analysis,  
77•8
  - system evaluation and certification,  
77•9–77•10
  - system-oriented analyses, 77•8–77•9
  - and trustworthiness, 77•2–77•5
  - vulnerabilities, detection and elimination of,  
77•7–77•8
- Information flow control, 24•2

- Information infrastructure:
  - access control. *See* Access control
  - overview, 23·2–23·3
  - physical site security. *See* Physical site security
  - protection, elements of, 23·11–23·16
  - responsibility for, 23·9
  - security planning, 22·6–22·9, 23·3–23·7
  - strategic planning, 23·7–23·11
  - threats to, 22·2, 22·18–22·20, 23·8, 23·16–23·19, 23·48–23·52. *See also* Physical threats
- Information life cycle management (ILM), 67·2
- Information security administrators (ISAs), 47·4–47·5, 63·26–63·29
- Information Security and Control Association (ISACA), 54·12, 65·11. *See also* Control Objectives for Information and Related Technology (COBIT)
- Information security (IS):
  - certifications, 74·5–74·16. *See also* Certification
  - cost-benefit analysis, 23·53
  - and federal guidelines, 23·55–23·56
  - framework. *See* Information security (IS), new framework proposal
  - implementation, accountability, and follow-up, 23·54–23·55
  - mitigation plan, 23·52
  - net present value of, 63·5
  - planning process, 23·52–23·55
  - responsibilities of management, 63·10–63·19
  - and risk management, 23·56
  - security incidents. *See* Security incidents
  - security response plan, 23·54
  - and strategic goals, 63·4–63·5
  - trends, 65·5–65·6
- Information security (IS), new framework proposal:
  - acts that cause loss, 3·2
  - components of, 3·2–3·3
  - need for, 3·1–3·2
  - objectives of information security, 3·3
  - purpose of, 3·20, 3·23
  - safeguard functions, 3·3, 3·19–3·20
  - safeguard selection methods, 3·3, 3·20
  - security elements, 3·2, 3·4–3·9
  - sources of loss, 3·2, 3·10–3·19
  - terminology, 3·9–3·10
  - threats, assets, vulnerabilities model, 3·2, 3·20–3·22
- Information security management system (ISMS), 54·3–54·5
- Information Security Policies and Procedures*, 44·10
- Information Security Policies Made Easy (ISPME)*, 44·9
- Information Systems Audit and Control Association (ISACA), 54·15, 74·9–74·12
- Information systems (IS):
  - audits, 35·6, 35·19
  - history of, 1·3–1·12
  - infrastructure. *See* Information infrastructure
  - rapid technology changes and security threats and vulnerabilities, 1·18–1·19
  - recent developments, 1·18
  - security, overview, 1·1, 15·1–15·2
- Information Technology Infrastructure Library (ITIL), 54·15, 65·8
- Information technology (IT):
  - insiders, dangerous. *See* Insiders, information technology
  - managers, 63·2
  - and role of CISO, 65·11–65·12, 65·17. *See also* Chief information security officer (CISO)
  - specialists, psychological characteristics of, 13·2
- Information Technology Management Reform Act (Clinger-Cohen Act), 54·17
- Information Technology Security Evaluation Criteria (ITSEC)*, 51·15
- Information warfare (IW):
  - and activists, 14·17
  - biological and chemical weapons, 14·21
  - and China, 14·13–14·15, 16·3
  - and computer crime, 14·17. *See also* Computer crime; Computer criminals
  - and computer security vulnerabilities, 14·21
  - corporations as victim of, 14·16
  - and critical infrastructure, 14·2–14·3
  - and cryptography, 14·19. *See also* Encryption
  - cyberterrorists, 14·15–14·16
  - defenses, 14·21–14·23
  - defined, 14·1
  - denial of service attacks, 14·18
  - distributed denial-of-service (DDos) attacks, 14·18
  - goals and objectives, 14·4–14·13
  - hackers and crackers, 14·17
  - malicious code, use of, 14·18
  - and off-the-shelf software, 14·3
  - overview, 14·2, 14·23–14·24
  - physical attacks, 14·20–14·21
  - and psychological operations (PSYOP), 14·19–14·20
  - views on, 14·3–14·4
  - weapons of, 14·17–14·21
  - weapons of mass destruction, 14·21
- InfraGard, 1·13, 1·18, 22·27, 61·12, 70·13
- Infrared (IR), 6·11
- Infrastructure:
  - information infrastructure. *See* Information infrastructure
  - and information warfare (IW), 14·2–14·3
  - local area network (LAN) security, 25·3–25·8
  - maintenance and repair, 23·15–23·16
  - National Infrastructure Protection Plan (NIPP), 23·5



## I • 26 INDEX

- Public Key. *See* Public Key Infrastructure (PKI) security. *See* Physical security (infrastructure security)
- Ingress filtering, 18•12, 18•25
- Initialization errors, 38•8–38•9, 39•7–39•8
- Initiative, encouraging, 50•16–50•19
- Injection layer diode (ILD), 6•10
- Input/output (I/O), 4•7, 24•2, 24•4–24•6, 53•16
- Insiders, information technology:
  - and classification of computer criminals, 12•18–12•19
  - extent of incidents, 13•8
  - motivation for computer crime, 13•6–13•8
  - pathway to computer crime, 13•4–13•5
  - prevention of incidents, 13•8–13•9
  - psychological characteristics of, 13•2–13•4
  - stress, impact of, 13•4–13•6
  - as threat to security, 13•1–13•2
  - types of, 13•2, 13•6–13•8
- Insourcing, 68•3–68•4, 68•15
- Installation, 23•15–23•16
- Instant messaging (IM):
  - and always-on generation, 50•21
  - business threats, 35•8–35•9
  - and denial-of-service attacks, 35•9
  - and need for security, 35•1
  - overview, 35•2, 35•8, 35•20
  - security breach prevention and mitigation, 35•9–35•11
  - security incident response, 35•11
  - and social engineering, 19•9
  - and viruses, 41•5
- Institute for Electronics and Electrical Engineers (IEEE), 6•16
  - IEEE 488 standard, 44•3
  - IEEE 802 standards. *See* IEEE 802 standards
- Institute of Internal Auditors (IIA), 65•11, 74•7
- Insurance:
  - business interruption, 60•10
  - claims made coverage, 60•6–60•8
  - commercial general liability (CGL) policies, 60•3, 60•12, 60•17
  - and compliance with standards, 22•10
  - consumers, 60•18
  - crime and fraud policies, 60•11
  - directors and officers (D&O), 60•17
  - and disaster recovery, 59•16
  - duty to defend, 60•7–60•8
  - e-commerce policies, 60•12–60•13
  - errors and omissions (E&O), 60•17
  - exclusions, 60•9
  - first-party coverage, 60•9–60•10
  - gross negligence, 22•8
  - and HIPAA compliance, 71•22–71•23
  - history, 60•1
  - identity theft, 60•13–60•18
  - indemnity, 60•7–60•8
  - intellectual property coverage, 60•3–60•10
  - need for, 60•2–60•3, 60•18–60•19
  - occurrence coverage, 60•6–60•7
  - prior acts coverage, 60•8–60•9
  - privacy breaches, 60•13–60•18
  - property coverage, 60•10–60•11
  - and SOX compliance, 34•2
- Intangible assets:
  - insurance coverage for loss or damage, 60•5–60•6, 60•10–60•11
  - intellectual property. *See* Intellectual property
- Integrated Services LAN (ISLAN), 6•17
- Integrity:
  - checking, 46•4
  - data, 24•3
  - e-commerce security services, 30•7
  - and encryption, 7•4. *See also* Encryption
  - firewalls and gateway security devices, 26•19
  - healthcare information, 71•6
  - and operating system security, 24•2
  - and outsourcing risks, 68•13–68•15
  - referential integrity, 52•4
  - as source of loss, 3•2, 3•5, 3•8–3•12
- Integrity Check Value (ICV), 33•14, 33•16–33•17, 33•45
- Intellectual property:
  - Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 11•35–11•39
  - circumvention of technical measures to secure copyrights, 11•14–11•18
  - Computer Fraud and Abuse Act, 11•26–11•30
  - and contracts for protecting technology, 11•3–11•5, 11•25–11•26
  - copyright law. *See* Copyright law
  - Digital Millennium Copyright Act, 11•13–11•18, 11•22–11•23, 31•8
  - Electronic Communications Privacy Act, 11•30
  - insurance coverage, 60•3–60•10
  - international law, 11•34–11•39
  - and open source, 11•33–11•34
  - overview, 11•2–11•3, 11•39
  - patents. *See* Patent law
  - piracy, 11•20–11•24
  - privacy issues. *See* Privacy
  - Stored Communications Act, 11•32–11•33
  - terms of use, 11•25–11•26
  - trade secrets. *See* Trade secrets
  - trademarks, 42•2
  - trespass, 11•24–11•25
  - unauthorized intrusions, legal remedies, 11•24–11•33
  - Wiretap Act, 11•30–11•32
  - World Intellectual Property Organization Copyright Treaty, 11•14–11•15
- Interconnection devices, 6•23–6•25
- Interference with use of information, 3•2, 3•15
- Internal audits, 65•16–65•17, 74•7–74•9
- International Council of Electronic Commerce Consultants (EC-Council), 74•23–74•24

- International Electrotechnical Commission (IEC):
  - ANSI/ISO/IEC 17024, 74·3–74·4, 74·6–74·7
  - ISO/IEC standards. *See* International Organization for Standardization (ISO)
- International Information Systems Security Certification Consortium (ISC), 74·12–74·14, 74·22
- International law:
  - intellectual property, 11·34–11·39
  - Internet objectionable content, 72·3–72·7 and VoIP, 34·5
- International Organization for Standardization (ISO):
  - 9000 standards, 38·2
  - ANSI/ISO/IEC 17024, 74·3–74·4, 74·6–74·7
  - commercial general liability insurance, 60·3–60·4
  - Common Criteria, 51·18. *See also* Common Criteria (CC)
  - ISO 9000 standard, 51·14, 54·3
  - ISO 14000, 54·3
  - ISO 17799, 23·7, 38·15, 44·4, 49·35, 53·3, 54·2, 54·4, 62·3–62·4, 67·6, 71·9
  - ISO 27000, 54·3–54·4, 54·15
  - ISO 27000 series, 62·4
  - ISO 27001, 54·2, 54·5, 62·4
  - ISO/IEC 1702, 74·6
  - ISO/IEC 13335-1:2004, 65·8
  - ISO/IEC 13335 MICTS Part 2, 54·5
  - ISO/IEC 15408, Evaluation Criteria for IT Security, 38·15
  - ISO/IEC 17799, 54·16, 62·3–62·4, 67·6
  - ISO/IEC 17799:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management*, 44·3, 54·4, 65·4, 65·7–65·8
  - ISO/IEC 27000, 54·3, 54·5
  - ISO/IEC 27001, 54·4–54·5
  - ISO/IEC 27001:2005, 65·8
  - ISO/IEC 27002, 54·5
  - ISO/IEC 27003, 54·5
  - ISO/IEC 27004, 54·5
  - ISO/IEC 27005, 54·5
  - ISO/IEC 27006, 54·5
  - ISO/IEC/ITU 9594-8 (X.509). *See* X.509 certificate format
  - ISO/IEC WD 15443, *Information Technology: Security Techniques*, 38·15
  - and OSI, 5·10
- International Telecommunications Union – Telecommunications Standards Sector (ITU-T), 5·10
- Internet:
  - addiction, 48·14, 48·27–48·28, 48·37
  - adware. *See* Adware
  - disconnection, 30·37
  - and dissemination of incorrect information, 48·5–48·6
  - Domain Name Service. *See* Domain Name System (DNS)
  - games, 48·29
  - get-rich-quick schemes, 48·11, 48·14, 48·43–48·44
  - history, 1·8–1·9, 1·12
  - hoaxes, 48·6–48·11, 48·43
  - international law and censorship, 72·2, 73·3
  - objectionable content, international differences, 72·3–72·7
  - online auctions, 48·14, 48·25–48·26, 48·40
  - online dating, 48·28, 48·37–48·39
  - online gambling, 48·14, 48·26, 48·40–48·41
  - online shopping, 48·14, 48·23–48·26, 48·39–48·40
  - overview, 5·6–5·8, 48·2, 48·44
  - and pedophiles, 48·12–48·13
  - pornography. *See* Pornography and reputation damage, 48·2–48·11
  - site-to-site VPNs, 32·6–32·7, 32·9–32·10
  - and spyware. *See* Spyware
  - system and network penetration through Web sites, 15·25–15·29
  - and viruses. *See* Viruses
  - Web monitoring. *See* Web monitoring
  - Web page defacement, 15·26–15·27
- Internet Assigned Numbers Authority (IANA), 30·31
- Internet Control Message Protocol (ICMP), 5·23–5·24, 30·27–30·28
- Internet Corporation for Assigned Names and Numbers (ICANN), 31·6
- Internet Engineering Task Force (IETF), 7·28
  - and consortium-based product assessment, 51·8
- IPsec. *See* IPsec
- PKI for X.509 Certificate (PKIX) working group, 37·8. *See also* X.509 certificate format
- RFC 822, 37·17
- RFC 1918, 16·10, 30·31
- RFC 2196, 25·1–25·3
- RFC 2196, *Site Security Handbook*, 44·8–44·9
- RFC 2246, 7·28
- RFC 2267, 16·10
- RFC 2385, 5·22
- RFC 2527, 37·17
- RFC 2535, 5·25
- RFC 2560, 37·21
- RFC 2634, 5·27
- RFC 2822, 5·27
- RFC 3280, 37·5–37·6
- RFC 3704, 16·10
- RFC 3833, 5·24
- RFC 3850, 5·27
- RFC 3851, 5·27
- RFC 4033–4035, 5·25

## I • 28 INDEX

- Internet Engineering Task Force (IETF)
    - (*Continued*)
    - Simple Network Management Protocol. *See* Simple Network Management Protocol (SNMP)
    - and TCP security, 5•22
    - Transport Layer Security. *See* Transport Layer Security (TLS)
  - Internet Explorer, 17•6–17•7
  - Internet Explorer (IE), 1•10, 7•26, 25•10
  - Internet Key Exchange (IKE), 32•4, 51•8
  - Internet Message Access Protocol (IMAP), 5•27, 57•23
  - Internet Protocol (IP). *See also* TCP/IP (Transmission Control Protocol/Internet Protocol)
    - address, 5•3, 5•15, 30•31
    - and denial-of-service attacks, 18•1–18•2. *See also* Denial-of-service attacks (DoS)
    - function of, 5•13
    - IP Version 4 (IPv4). *See* IPv4
    - IP Version 6, 5•15–5•16
    - IPsec. *See* IPsec
    - and layered standards architectures, 5•10
    - and network operating systems, 6•27
    - and protecting Web applications, 21•6
    - and security, 5•9
    - spoofing, 31•9–31•10
  - Internet Protocol Security (IPsec). *See* IPsec
  - Internet Protocol Telephony (IPT). *See* Voice over Internet Protocol (VoIP)
  - Internet Protocol Version 6. *See* IPv6
  - Internet Relay Chat (IRC) bots, 16•6–16•8
  - Internet Security Scanner (ISS), 46•3
  - Internet Service Providers (ISPs):
    - and anonymity in cyberspace, 70•9, 70•15, 70•18–70•20
    - and censorship, 72•2–72•3, 72•5–72•7
    - copyright issues, 11•22. *See also* Copyright law and distributed denial-of-service attacks, 18•25
    - e-mail privacy issues, 11•32
    - history, 1•12
    - and network access points, 5•8
    - parental tools for blocking Web content, 31•9
    - and security incidents, 56•10
    - and spam, 20•19–20•20, 20•25
    - spam filtering, 20•21–20•22
    - Web hosting, 48•5
  - Internetwork Packet Exchange (IPX), 6•27
  - Interprocess communications tables, 53•9
  - Interrupts, 4•7–4•8
  - Interviews:
    - and business impact analysis, 58•15–58•18
    - computer crime research methods, 10•9–10•10
  - Intranets, 5•8
  - Intrusions:
    - alarms, 22•19, 23•26–23•27. *See also* Alarms analysis schemes, 27•5–27•6, 27•8–27•10
    - blended attacks, 55•13
    - defined, 27•2
    - detection, 26•11–26•12, 26•14, 26•18, 27•2–27•5, 41•10, 53•2
    - e-commerce security services, 30•6
    - host intrusion prevention systems (HIPS), 53•11, 53•13
    - intrusion detection systems (IDSs), 27•2, 39•20
    - intrusion prevention systems (IPSs), 39•20
    - malware. *See* Malware
    - monitoring, 27•5–27•8
    - overview, 27•4–27•6, 27•16
    - prevention, 26•12–26•13, 27•2–27•3, 27•6, 41•10, 53•2, 53•10
    - process of and cyber investigation, 55•13–55•14
    - product selection and needs assessment, 27•13–27•16
    - response, 26•12–26•13, 27•5, 27•10–27•13
    - threats to information infrastructure, 22•18
    - wireless intrusion detection and prevention systems (WIDPS), 27•14
  - Invalid file access attempts, log record, 53•16
  - Inventory:
    - and business impact analysis, 58•15
    - integrated software inventory, 40•21
    - management systems, 53•12
    - system inventory, creating, 40•6–40•9
    - and vulnerability management, 46•2
  - IP spoofing. *See* Spoofing
  - IP Version 4 (IPv4). *See* IPv4
  - IP Version 6 (IPv6). *See* IPv6
  - iPhone, 17•1
  - IPsec, 5•9, 5•16, 5•22–5•23, 25•4, 32•3–32•5, 51•8–51•9
  - IPSec Developers Forum, 25•4
  - IPv4, 5•13–5•15, 26•16, 30•29, 30•31, 32•11
  - IPv6, 21•7, 26•16–26•17, 30•29, 32•11, 32•15
  - IRC bots. *See* Internet relay chat (IRC) bots
  - Ireland, 7•37
  - ISO standards. *See* International Organization for Standardization (ISO)
  - Israel, 7•37
  - IT Baseline Protection Manual*, 44•9
  - IT Governance Institute (ITGI), 65•11
  - IT-Grundschutz Catalogues*, 44•9
  - IT-Grundschutzhandbuch*, 44•9
  - iTunes Music Store, 42•8, 42•10, 42•16
- ## J
- Java:
    - applets, 16•8, 17•2, 17•9, 17•11, 21•8, 48•34
    - buffer overflows, 39•13
    - and component-based software, 21•14
    - and denial-of-service attacks (DoS), 18•11
    - and e-commerce vulnerabilities, 21•4, 21•21
    - and firewalls, 30•32
    - and hacker Web sites, 48•44
    - and information warfare, 14•18
    - Java 2 Enterprise Edition (J2EE), 21•13

security features, 38•7–38•8  
 source language programs, 47•3  
 Virtual Machine, 42•15  
 Java Run Time Environment, 17•9  
 Java Virtual Machine (JVM), 17•9  
 JavaScript, 16•8, 17•2, 21•15, 26•5, 26•16  
 JavaScript/ECMA Script, 17•12–17•13  
 JavaServer Pages, 15•29  
 Job Control Language (JCL), 47•3  
 Job scheduling, 53•10  
 Joint application development (JAD), 39•7, 52•2  
 Jones University, 75•11  
 Jukeboxes, 57•8–57•9  
 Juniper, 51•29  
 Junk e-mail. *See* Spam  
 Just-in-time (JIT) production, 30•23

**K**

Kerberos, 25•11, 28•10, 32•5, 36•8–36•9, 37•25  
 KERMITS, 30•32  
 Kernel mode, 24•9–24•10, 38•5, 41•2  
 Kernel panic attacks, 18•8–18•9  
 Key Usage extension, 37•6  
 Keys, 4•17, 7•2. *See also* Encryption  
 Keyspace, 7•3, 7•10, 7•20, 7•22, 15•15–15•16  
 Keystroke loggers, 15•14, 16•6–16•7  
 Kibibytes, 4•4  
 Kilobytes (KB), 4•4  
 Kismet, 33•36–33•37, 33•39  
 Knight-in-shining-armor attacks, 19•10  
 Knowledge, skills, and abilities (KSAs), 75•5  
*Kumho Tire Co. v. Carmichael*, 73•3

**L**

L0pht Heavy Industries, 2•26  
 L0phtCrack, 15•24, 25•8  
 LAN. *See* Local area networks (LANs)  
 LANalyzer, 25•4  
 Land attack, 18•9  
 Language translation sites, 31•11–31•12  
 Laptops, 1•18, 33•12–33•13, 36•10–36•11,  
 57•16–57•17  
 Lavasoft, 21•9, 48•14, 48•42  
 Law enforcement, cooperation with:  
   crimes, reporting, 61•2–61•6  
   and e-commerce, 30•19–30•20  
   evidence handling, 61•7–61•8  
   FBI. *See* Federal Bureau of Investigation (FBI)  
   investigations, maintaining operations during,  
   61•10  
   liability issues, 61•8–61•9  
   memorandum of agreement, 61•2, 61•7  
   nonelectronic records, 61•11–61•12  
   overview, 61•1–61•2, 61•15  
   and privacy law, 69•8–69•9  
   search warrants, 61•9  
   security incidents, 56•10, 56•22–56•23, 56•30  
   sharing information with, 61•12–61•15  
   training provided by, 61•9

U.S. Postal Inspection Service, 61•7  
 U.S. Secret Service, 61•6–61•7  
 Layered standards architectures, 5•10–5•11  
 LDAP, 32•5  
 Leaks, liquid, 22•23, 53•11  
 Leased lines, 5•5, 15•9–15•10  
 Least privilege, 24•4  
 Legacy systems, 53•10, 53•23–53•24, 53•26  
 Legal and regulatory compliance. *See also*  
   Standards  
   All-Hazard Mitigation Plan, 23•6  
   business continuity planning, 58•3  
   code security, 38•4, 39•9–39•10  
   data classification policies, 67•3–67•5  
   database encryption, 36•13  
   Department of Homeland Security. *See*  
   Department of Homeland Security (DHS)  
   Disaster Mitigation Act of 2000, 23•6  
   disaster recovery, 59•16  
   e-commerce, 30•40–30•41  
   Emergency Operations Plan, 23•6  
   evaluation procedures, 64•11–64•14  
   Federal Emergency Management Agency. *See*  
   Federal Emergency Management Agency  
   (FEMA)  
   Gramm-Leach-Bliley Act of 1999. *See*  
   Gramm-Leach-Bliley Act (GLBA)  
   Health Insurance Portability and Accountability  
   Act of 2002 (HIPAA). *See* Health Insurance  
   Portability and Accountability Act (HIPAA)  
   illegal activities and employee Internet use,  
   48•3  
   medical records. *See* Health Insurance  
   Portability and Accountability Act (HIPAA);  
   Medical records  
   and monitoring and control systems,  
   53•4–53•5  
   National Incident Management System  
   (NIMS), 23•3–23•5  
   National Infrastructure Protection Plan (NIPP),  
   23•5  
   National Response Plan (NRP), 23•3–23•5,  
   23•54  
   and need for centralized network control,  
   26•2–26•3  
   overview, 54•2, 64•1–64•2  
   privacy, 60•14–60•16. *See also* Privacy law  
   risk management, 62•4  
   Robert T. Stafford Disaster Relief and  
   Emergency Assistance Act of 1988, 23•6  
   and role of CISO, 65•2–65•3, 65•13–65•14  
   Sarbanes-Oxley Act of 2002 (SOX). *See*  
   Sarbanes-Oxley Act (SOX)  
   Voice over Internet Protocol (VoIP), 34•2–34•6  
 Legion of Doom (LOD), 2•23–2•24  
 Levin, Vladimir, 2•10  
 Liability:  
   criminal. *See* Criminal liability  
   and cyber investigations, 61•8–61•9

## I • 30 INDEX

### Liability (*Continued*)

- defamation and libel, 72•12
- destruction of e-mail records, 48•35
- downstream liability doctrine, 63•21
- employment termination, 45•14–45•15
- and federal guidelines, 23•10–23•11
- HIPAA violations, 71•19–71•20
- hostile work environment, 48•32–48•33
- identity theft, 60•13–60•14
- illegal copies of software, music, and videos, 48•30
- insurance. *See* Insurance
- libel, 48•30
- management concerns, 63•19–63•23
- negligent hiring and retention of employees, 45•2
- and physical security, 22•7–22•8, 22•10
- plagiarism, 48•30–48•31
- and VoIP, 34•5–34•6
- Web site management, 30•38–30•39

Libel, 48•30

Libraries and Internet censorship issues, 72•14–72•16

Licenses and licensing:

- Berkeley Software Distribution (BSD) License, 11•34
- and first sale doctrine, 11•9
- General Public License (GPL), 11•33–11•34
- Massachusetts Institute of Technology (MIT) License, 11•34
- open source code, 11•33–11•34
- shrink-wrap and click-wrap licenses, 11•4, 11•17
- and TRIPS anticompetitive restrictions, 11•38

Light-emitting diode (LED), 6•10

Lightweight Directory Access Protocol (LDAP), 34•12, 37•16

*Limewire*, 16•6

LinkedIn, 48•5

Linus, 63•28

Linux, 25•8, 25•11, 25•13, 26•9, 33•12, 33•36–33•37, 51•10–51•11

Liquids as security hazard, 3•17

List servers, 48•22

Litigation:

- commercial and consumer Web transactions, 30•40–30•41
- expert witnesses. *See* Expert witnesses
- Federal Rules of Civil Procedure. *See* Federal Rules of Civil Procedure (FRCP)
- Federal Rules of Evidence, 73•1–73•2

Living organisms as security hazard, 3•18

Load balancing, 26•23

Load condition errors, 38•10, 39•8–39•9

Local area networks (LANs):

- access ports, disabling, 16•10
- background, 1•10–1•12
- characteristics, 6•2
- components of, 6•2–6•3

- infrastructure security, 25•3–25•8
- interconnection devices, 6•23–6•25
- media, 6•2, 6•8–6•12
- media access control (MAC) standard, 6•3–6•5, 6•12–6•25
- and network-attached storage (NAS), 57•4
- network control, 6•3–6•4
- network design example, 6•27–6•28
- network interface card (NIC), 6•2–6•3
- network operating systems, 6•3, 6•26–6•27, 25•8–25•15
- overview, 5•4–5•5
- packet sniffing, 15•10–15•11
- physical site security, 25•3
- policy and procedure issues, 25•1–25•3
- promiscuous mode, 25•3
- protocols, 6•3, 6•14–6•23
- sample network design, 6•27–6•28
- security, generally, 25•1, 25•15–25•16
- sniffers, 25•4. *See also* Packet sniffers
- technology parameters, overview, 6•3
- topology, 6•3–6•8
- web sites, 6•28
- wireless (WLAN), 6•11, 15•12, 25•6–25•7

Local emergency operations plan, 23•54

Locks and door hardware, 22•19, 22•24, 23•20–23•21, 23•26, 36•3. *See also* Dongles

Log files. *See* Logs and logging

Logic bombs, 2•10–2•11, 13•6–13•7, 16•4, 45•9

Logic flow errors, 38•9, 39•8, 52•3

Logical domain addresses, 21•7

Logical Link Control (LLC), 6•16

Logical security (information systems security), 22•9. *See also* Information security (IS)

- authentication. *See* Authentication
- biometric authentication. *See* Biometric authentication
- passwords. *See* Passwords

Login:

- information, trapping, 15•13
- speed, 15•16
- visitors, 23•23, 47•5–47•6

Logon attempts, 53•16

Logs and logging:

- alerts, 53•22–53•23
- archiving log files, 53•20–53•21
- chargeback systems, 53•21
- data aggregation, 53•19–53•20
- file system activities, 53•12–53•13
- filtered queries, 53•20
- and gateway security devices, 26•21–26•22, 26•26–26•27
- log files, 30•40–30•41, 47•16, 53•2, 53•13–53•18
- log management, 53•13–53•19, 53•22
- log review, 46•4
- log server, 39•19–39•20
- and new versions of software, 47•6–47•8

patch logs, 40·16–40·17  
 records, analyzing, 53·20–53·21  
 security, 53·18–53·19  
 system logs, 52·6  
 transaction logs, 53·14  
 Lotus Notes, 6·26  
 Love Bug virus, 41·11  
 Low-tech social engineering attacks, 19·4,  
 19·6–19·8

**M**

MacOS, 25·8, 25·14–25·15, 26·9  
 Macro facilities, 14·14  
 Macro viruses, 16·4  
 Magnetic disks, 36·1  
 Magnetic fields, 4·12  
 Maintenance and repair:  
   cleaning, 22·24  
   personal computers, 4·24–4·25  
   and protection of infrastructure, 23·15–23·16  
   Web site maintenance and updating, 30·29  
 Malicious code. *See* Malware; Mobile code  
 Malware. *See also* Mobile code  
   antimalware, 26·13, 26·15–26·16, 66·10  
   and antivirus technology. *See* Antivirus  
   programs  
   automated malware attacks, 55·13  
   detecting, 16·8–16·9  
   and e-commerce, 21·9–21·10  
   financial gain, 41·1–41·2  
   history, 2·14–2·19  
   and information warfare, 14·18  
   IRC bots, 16·6–16·8  
   overview, 16·1–16·2, 16·11  
   as part of computer science curriculum,  
     76·13–76·14  
   prevention, 16·9–16·11  
   rootkits, 16·7. *See also* Rootkits  
   and social engineering attacks, 19·8  
   spyware, 16·6–16·7. *See also* Spyware  
   and system penetration, 15·29–15·30  
   threat model, 16·2–16·3  
   Trojans, 16·6, 16·8. *See also* Trojan horses  
   viruses, 16·3–16·5. *See also* Viruses  
   worms, 16·5–16·7. *See also* Worms  
 Man-in-the-middle attacks, 21·12, 33·46,  
 34·10–34·11, 36·6–36·7, 36·9, 37·4,  
 47·15  
 Managed security service provider (MSSP),  
 26·32  
 Management:  
   awareness program support, 49·6–49·7,  
     49·10–49·12  
   communicating with, 49·11–49·12  
   computer management, 63·23–63·25  
   employee management, 45·3–45·10,  
     63·12–63·15  
   failures, 63·16–63·18  
   judgment and adaptation, 63·15–63·16

liability issues, 63·19–63·23  
 policy, 63·12  
 responsibilities of, 63·10–63·18  
 risk management. *See* Risk management  
 role of, 63·1–63·2  
 security administration, 63·26–63·29  
 security policy implementation, 66·13  
 SOX compliance, perspective on, 64·5–64·6  
 strategic goals and information security,  
   63·4–63·5, 63·29  
 support for security policy development,  
   66·11–66·12  
 and value of information security, 63·5  
   Veterans Affairs case study, 63·6–63·10  
 Management by walking around, 50·17  
 Management Information Bases (MIBs), 25·9  
 Management interfaces, 36·5–36·6  
 Mandatory access controls, 9·2, 9·6, 9·9  
 Mantraps, 23·33  
 Manual override, 53·11  
 Masquerading, 33·9  
 Massachusetts Institute of Technology (MIT)  
   License, 11·34  
 Masters of Deception (MOD), 2·23–2·24  
 Mathematical models. *See* Models of computer  
   security  
 Maximum segment size (MSS), 5·20  
 Mebibytes, 4·4  
 Media access control (MAC) standard, 6·3–6·5,  
   6·12–6·25, 25·3, 33·15–33·16, 33·46,  
   34·12  
 Media Independent Handover, 6·18  
 Medicaid, 71·8, 71·14  
 Medical emergencies, 22·5, 22·25, 23·50–23·51  
 Medical records:  
   defined, 71·2  
   federal laws, 71·8–71·9  
   government healthcare services, 71·7  
   government policies, 71·9–71·10  
   Health Insurance Portability and Accountability  
     Act. *See* Health Insurance Portability and  
     Accountability Act (HIPAA)  
   importance of in healthcare, 71·2–71·3  
   information technology role in healthcare, 71·3  
   media interests, 71·7  
   overview, 71·1–71·2  
   patient expectations, 71·7–71·8  
   patients as owners of healthcare information,  
     71·6  
   privacy and security issues, 71·5–71·6  
   privacy and security model, 71·6  
   proposed legislation, 71·10–71·11  
   public sensitivity, 71·7  
   regulatory compliance, generally, 71·1–71·2  
   risks and vulnerabilities, 71·4–71·5  
   state laws, 71·9  
 Medicare, 54·16, 71·8, 71·12, 71·14  
 Melissa virus, 1·3, 2·17–2·18, 18·4, 25·10  
 Memorandum of agreement (MOA), 61·7

## I • 32 INDEX

- Memory:
  - consumption, log records, 53•17
  - core memory, 1•7
  - main memory, 4•8
  - protection of, 24•5–24•6
  - read-only, 4•8–4•9
- Memory dumps, 53•8–53•9
- Memory keys. *See* Flash drives
- Memory management tables, 53•9
- Message Authentication Code (MAC), 7•4–7•5, 7•29, 38•7
- Metacharacters, 15•29
- Metadata, 4•4
- Metrics. *See also* Standards
  - awareness programs, 49•8
  - chief information security officers, 65•13
  - security awareness programs, 49•35–49•39
  - and service-level agreements, 68•20
- Metropolitan Area Network (MAN), 6•17
- METT-TC analysis, 47•2
- Microfilm, 57•20
- Microprogramming, 4•9
- Microsoft Corporation:
  - ActiveSync Service, 33•13
  - Assistance Markup Language, 21•18
  - Authenticode, 17•5, 17•7
  - Common Object Model (COM), 21•13
  - and Digital Rights Management, 42•13–42•14
  - Distributed COM (DCOM), 21•13
  - history, 1•9–1•10
  - Internet Explorer, 1•10, 16•4–16•5
  - Microsoft SQL Server 2005, 36•12–36•13
  - Point-to-Point Encryption, 25•7
  - product validation, 51•29
  - software registration and antipiracy programs, 42•4–42•5
  - Trustworthy Computing initiative, 25•11
  - Windows. *See* Microsoft Windows
- Microsoft Networking, 6•26
- Microsoft Office:
  - and data grinding, 19•7
  - Office 2000, 25•10
  - products, 41•4
- Microsoft Outlook, 25•10
- Microsoft Windows:
  - and ActiveX controls, 17•11–17•12. *See also* ActiveX
  - firewalls, 26•9
  - and Help documents, 21•18
  - and network operating systems, 25•8
  - RSA encryption, 7•26
  - Windows 3.0, 1•10
  - Windows 3.1, 41•4
  - Windows 3.11, 57•20
  - Windows 9x, 25•9–25•10
  - Windows 95, 25•9, 41•4
  - Windows 98, 25•9
  - Windows 2000, 24•14–24•19
  - Windows 2000/2003 Server, 6•26
  - Windows Defender, 25•11
  - Windows ME, 25•9
  - Windows NT/2000, 25•10–25•13
  - Windows NT Resource Kit, 25•12–25•14
  - Windows NT Server, 6•26
  - Windows Service Hardening, 25•11
  - Windows Update, 40•18
  - Windows Update ActiveX control, 17•11–17•12
  - Windows Vista, 16•10, 21•7, 21•18, 25•11–25•12, 42•5, 57•20
  - Windows XP, 25•11
- Microsoft Word, 48•19
- Microwave LANs, 6•12
- Middle East, Internet content regulation, 72•6–72•7
- Miliefsky, Gary S., 1•16
- Military:
  - information categories, 24•2, 24•11
  - and intrusion detection systems, history of, 27•4
  - operations security and acronyms, 47•2
  - spread spectrum radio transmission, 5•12
- MIME. *See* Multipurpose Internet Mail Extensions (MIME)
- MIS Training Institute (MISTI), 56•34
- Misrepresentation, 3•2, 3•15, 15•3–15•6
- Mission, equipment, time, troops, terrain and culture (METT-TC) analysis, 47•2
- Misuse of or failure to use information, 3•2, 3•16
- Mitigation:
  - All-Hazard Mitigation Plan, 23•6, 23•52
  - collaboration tools, security breach prevention and mitigation, 35•18–35•19
  - Disaster Mitigation Act of 2000, 23•6
  - FEMA *State and Local Mitigation Planning* guides, 23•42
  - information security mitigation plan, 23•52
  - instant messaging security breach prevention and mitigation, 35•9–35•11
  - Mitigation BCA Toolkit*, 23•53
  - peer-to-peer (P2P) networking, security breach prevention and mitigation, 35•5–35•7
  - physical threats, 23•48–23•52
  - risk, 62•10–62•16, 62•24. *See also* Risk management
  - short message service (SMS), security breach prevention and mitigation, 35•13–35•15
  - violence, prevention and mitigation, 23•13–23•14
  - Mitigation BCA Toolkit*, 23•53
- Mitnick, Kevin, 2•5–2•6, 15•6–15•7, 19•3
- Mobile Broadband Wireless Access (MBWA), 6•18
- Mobile code:
  - ActiveX, 17•2, 17•5–17•12, 21•8, 30•32. *See also* ActiveX
  - client responsibilities, 17•11–17•12
  - defined, 17•2

- and firewalls, 30-32
- and information warfare, 14-18
- Java, 17-2, 17-9, 17-11-17-13. *See also* Java malicious, 16-8, 17-2
- misappropriation and subversion, 17-11
- motivation and goals of malware, 17-3-17-4
- as multidimensional threat, 17-11
- overview, 17-1-17-2, 17-13
- restricted operating environments, 17-8-17-9
- server responsibilities, 17-12-17-13
- signed code, 17-4-17-8, 17-10-17-12
- trust issues, 17-10
- and Web servers, 17-2-17-3, 17-12-17-13
- from World Wide Web, 17-2-17-3
- Mobile data systems, 1-18
- Mobile devices. *See also* Cellular phones and modems; Wireless networks
  - and data backups, 57-17
  - and virtual private networks, 32-7
- Mobile phones. *See* Cellular phones and modems
- Models of computer security:
  - access-control matrix model, 9-3-9-5
  - Bell-LaPadula model, 9-2, 9-9-9-12, 9-18-9-19
  - Biba's strict integrity policy model, 9-2, 9-9, 9-12-9-14, 9-18-9-19
  - Chinese Wall model (Brewer-Nash model), 9-2, 9-16-9-19
  - Clark-Wilson model, 9-2, 9-9, 9-14-9-16, 9-18-9-19
  - Clinical Information Systems Security model, 9-18
  - and controls, 9-6-9-9
  - deducibility security, 9-18-9-19
  - discretionary access controls, 9-2, 9-6, 9-9
  - importance of models, 9-1-9-3
  - mandatory access controls, 9-2, 9-6, 9-9
  - noninterference security, 9-18-9-19
  - originator-controlled access control, 9-2, 9-6-9-7, 9-9
  - overview, 9-2, 9-19
  - role-based access controls, 9-2, 9-7-9-9
  - terminology, 9-3
  - traducement, 9-18
  - typed access control model, 9-6
- Modems, 1-10, 4-14-4-15, 5-4, 15-11-15-12, 25-5-25-6
- Modification of data, 3-2, 3-15
- Monitoring. *See also* Monitoring and control (M&C) systems
  - chief information security officer, role of, 65-13
  - customers, 30-39
  - e-commerce security services, 30-6
  - employee Web activities and e-mail, 69-13-69-14
  - intrusion detection, 27-5-27-8
  - output quality, 47-12
  - performance, 47-10-47-11, 53-5-53-6
  - and privacy, 69-9
  - resources, 47-11-47-12
  - vulnerabilities, remediations, and threats, 40-9-40-10
  - Web. *See* Web monitoring
  - wireless networks, 53-10-53-11, 53-24-53-25
- Monitoring and control (M&C) systems:
  - access controls. *See* Access control
  - alerts, 53-22-53-23
  - artificial intelligence programs, 53-21
  - automated, 53-2, 53-6-53-7, 53-18, 53-26
  - batch mode, 53-3-53-4
  - challenges, 53-23-53-26
  - change management. *See* Change
  - chargeback systems, 53-21
  - components of, 53-2
  - continuous mode, 53-3-53-4
  - control loop, 53-4
  - controlling versus monitoring, 53-3-53-4
  - dashboards, use of, 53-21-53-22
  - data aggregation and reduction, 53-19-53-22
  - environmental measurement, 53-11
  - exception reports, 53-23
  - file systems, 53-12-53-13
  - industrial control systems (ICSs), 53-5, 53-11, 53-24
  - job level, 53-17-53-18
  - job scheduling, 53-10
  - and legacy systems, 53-10, 53-23-53-24, 53-26
  - log management, 53-13-53-19. *See also* Logs and logging
  - mobile computing, 53-24-53-25
  - network connectivity, 53-10-53-11
  - notifications, 53-22-53-23
  - overview, 53-2-53-4, 53-26
  - prevention, detection, and response as purpose of, 53-2-53-3
  - process activities, 53-12
  - process flow, 53-10
  - real-time control, 53-7-53-8
  - real-time monitoring, 53-7-53-8
  - reporting, 53-23
  - resource allocation, 53-18
  - scope and system requirements, defining, 53-4, 53-18
  - system component status, 53-11-53-12
  - system level, 53-17-53-18
  - system management consoles, 53-22
  - system models, 53-6-53-9
  - targets of, 53-10-53-13
  - trend analysis, 53-23
  - virtualization, 53-25-53-26
  - Web monitoring. *See* Web monitoring
- Monte Carlo simulation, 62-23
- Morris, Robert T., Jr., 16-5. *See also* Morris Worm
- Morris Worm, 2-15-2-16, 16-5, 18-2-18-4, 30-36, 56-4, 65-2
- Motivation, 4-21, 22-3-22-4
- Movement as security hazard, 3-18



## I • 34 INDEX

- MP3 music files, 42•7–42•8
- MPEG compression, 42•9, 42•11
- MS-DOS, 1•10
- Multicast listener discovery (MLD), 26•16
- Multilevel security, 24•12
- Multiprotocol layer switching (MPLS), 32•6, 32•9–32•10
- Multipurpose Internet Mail Extensions (MIME), 5•27, 37•5
- Multistation access units (MAUs), 6•24
- Multiuser dungeons (MUD), 20•7
- Music downloads, 42•6–42•8, 42•10, 48•30. *See also* Piracy
- Mutual Recognition Arrangement (MRA), 51•17–51•18, 51•26, 51•29
- Myanmar (Burma), Internet content regulation, 72•7
- MySpace, 15•30, 16•4, 48•5
  
- N**
- Napster, 42•7–42•8
- NAT-Traversal (NAT-T), 34•13–34•14
- National access points (NAPs), 1•12
- National Commission for Certifying Agencies (NCCA), 74•4
- National Computer Security Association (NCSA), 41•6–41•7
- National Computer Security Center (NCSC):
  - Orange Book*, 1•13–1•14, 17•9, 17•13, 25•11, 51•11, 51•14–51•15
  - system ratings, 25•11
- National Electric Code (NEC), 23•14
- National Health Information Infrastructure, 71•11
- National Health Information Privacy and Security Collaboration, 71•11
- National Incident Management System (NIMS), 23•3–23•5, 23•7
- National Information Assurance Training and Education Center, 75•8
- National Infrastructure Protection Plan (NIPP), 23•5
- National Institute of Standards and Technology (NIST):
  - awareness and training programs, guidelines for budgeting, 49•7
  - awareness program topics, recommendations for, 49•18
  - and CC Testing Labs, 51•28
  - Computer Security Incident Handling Guide*, 56•32
  - and development of the common language, 8•3
  - and Federal Information Security Management Act (FISMA), 71•8–71•9
  - FIPS Publication 199, 23•31
  - FIPS Publication 200, 23•31
  - premises security, 23•31
  - and public key systems, 7•35
  - and quantum cryptography, 7•42
  - risk framework, 54•18–54•19
  - security activities reference model, 1•17
- Security Configuration Checklists Program for IT Products, 40•22
- SP 800-16, 75•7
- SP 800-26, 54•16
- SP 800-48, “Wireless Network Security,” 35•15
- SP 800-50, awareness and training program, 49•9
- SP 800-53 Revision 1, “Recommended Security Controls for Federal Information Systems,” 54•15–54•16
- SP 800-55, 49•35
- SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, 54•15
- SP 800-61, *Computer Security Incident Handling Guide*, 40•24
- SP 800-66, 71•18–71•19
- SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, 40•24
- SP 800-98, RFID technology, 53•25
- SP 800 series, 38•6, 54•15
- special publications (SPs), 54•19
- storage unit standards, 4•4
- National Organization for Competency Assurance (NOCA), 74•4–74•5
- National Research Council (NRC), 1•13
- National Response Plan (NRP), 23•3–23•5, 23•7, 23•54
- National Security Agency (NSA):
  - and CC Testing Labs, 51•28
  - Centers of Academic Excellence in Information Assurance Education (CAE), 74•4–74•5, 75•4–75•5, 76•13
  - Computer Security Center, 24•13
  - Data Encryption Standard (DES). *See* Data Encryption Standard (DES)
  - and elliptic curve cryptography, 7•35
  - Information Assurance Courseware Evaluation (IACE) Program, 74•4
  - and Microsoft Vista, 25•12
  - Network Applications Team of the Systems and Network Attack Center, 54•15
  - Rainbow Series, 1•13–1•14, 54•14–54•15
  - Secure Hash Algorithms (SHA), 34•14
  - Security Guidelines Handbook*, 44•6–44•7
  - SPOCK program, 51•9
  - and TEMPEST compliance, 25•5
- National security and privacy law, 69•8–69•9
- National Security Telecommunications and Information Systems Security Committee, 71•9–71•10
- National Voluntary Laboratory Accreditation Program (NVLAP), 51•27
- National Vulnerability Database, 40•10, 40•23
- Natural hazards, 22•16–22•17. *See also* Physical threats
- Nearshoring, 68•4, 68•15

- Needs analysis, 66·12
  - Negligence:
    - contributory, 63·21–63·22
    - insurance and liability issues, 60·12–60·13
    - and physical site security, 22·8
  - Neighbor discovery (ND), 26·16
  - NetBIOS Extended User Interface (NetBEUI), 6·26
  - Netherlands, 76·10–76·11
  - Netscape Navigator, 7·26
  - Netstumbler, 33·36–33·38
  - Network access control (NAC), 32·7
  - Network Access Points (NAPs), 5·8
  - Network Access Protection, 25·11
  - Network activity files, 53·17
  - Network Address Translation (NAT), 5·3, 26·11, 26·17, 32·4, 34·12–34·13
  - Network anomaly detection (NAD), 16·11
  - Network Associates, 25·4
  - Network attached storage (NAS), 36·3, 36·5
  - Network File System (NFS), 36·7–36·8, 57·4
  - Network interface card (NIC), 5·3, 6·2, 25·4
  - Network intrusion prevention systems (N-IPS), 26·10
  - Network Monitor, 25·4
  - Network monitoring, 16·11
  - Network operating systems (NOS), 1·10–1·11, 6·3, 6·26–6·27, 25·8–25·15
  - Network proxy, 42·14–42·15
  - Network security:
    - acceleration, 26·15
    - allowed paths, 26·10–26·11
    - content control, 26·15–26·16
    - encryption, 26·14–26·15, 26·18–26·19. *See also* Encryption
    - evaluation of devices, 26·23–26·33
    - evaluation phase, security policy development, 66·9–66·10
    - firewalls. *See* Firewalls
    - intrusion detection and prevention, 26·11–26·14
    - IPv6, 26·16–26·17. *See also* IPv6
    - overview, 26·32–26·33
    - proxy servers. *See* Proxy servers
    - and virtual private networks. *See* Virtual private networks (VPNs)
    - and VoIP, 34·12
  - Networks:
    - application standards, 5·26–5·28
    - ARPANET, 1·8–1·9, 1·12, 77·15
    - Internet Protocol (IP). *See* Internet Protocol (IP)
    - local area networks. *See* Local area networks (LANs)
    - monitoring, 53·10–53·11
    - monitoring for intrusion detection, 27·5–27·7
    - orthogonal, 16·9, 16·11
    - penetration. *See* System and network penetration
    - protocol risks, 5·9, 21·10–21·12
    - public, 1·18
    - scanners, 40·16, 40·21, 46·3
    - security. *See* Network security
    - simple home PC network, 5·2–5·4
    - standards, 5·4–5·13, 5·23–5·28
    - terminology, 5·2
    - Transmission Control Protocol (TCP). *See* TCP/IP (Transmission Control Protocol/Internet Protocol); TCP (Transmission Control Protocol); Transmission Control Protocol (TCP)
    - User Datagram Protocol (UDP), 5·23
    - wide area networks (WANs), 1·12
    - wireless. *See* Wireless networks
  - NetZip, 48·13
  - Newsletters, certification exam preparation, 74·16–74·17
  - Nigerian 411/419 fraud (advance-fee fraud), 2·20, 16·10, 19·8
  - Nigerian 419 fraud, 16·10
  - Noncompetition agreements, 45·14–45·15
  - Noninterference security, 9·18–9·19
  - Nonpublic personal information (NPI), 54·5–54·6
  - Nonrepudiation, 3·12–3·13, 7·5, 28·5, 37·6
  - Norm of reciprocity, 50·19
  - North American Free Trade Agreement (NAFTA), 11·35
  - Norton Antivirus, 48·14
  - Norwich University, 75·13
  - Novell, 25·4, 42·5
    - NetWare, 1·10, 6·27, 25·8, 25·13
- O**
- Object Management Group (OMG), Common Object Request Broker Architecture (CORBA), 21·13
  - Observation, as means of information loss, 3·2, 3·16
  - Octet, 5·2, 5·19–5·20
  - Office of Management and Budget (OMB), 54·17–54·18, 71·9
  - Offshoring, 68·4, 68·15
  - Omnibus Crime Control and Safe Streets Act, 34·4
  - On-Line Certificate Status Protocol (OCSP), 37·20–37·21
  - Onion routing, 31·2, 31·11, 35·7, 42·15
  - Online auctions, 48·14, 48·25–48·26, 48·40
  - Online dating, 48·28, 48·37–48·39
  - Online files and databases, 52·2, 57·22–57·23
  - Online gambling, 48·14, 48·26, 48·40–48·41
  - Online shopping, 48·14, 48·23–48·26, 48·39–48·40
  - Online systems, 1·7
  - Open architecture, 1·9
  - Open design, 24·4
  - Open Shortest Path First (OSPF), 5·26
  - Open source code, 11·33–11·34, 51·10–51·11

## I • 36 INDEX

- Open Systems Interconnection (OSI) Reference Model, 5•10–5•11, 6•14–6•16
  - Open VMS, 17•13
  - Open Web Application Security Project (OWASP), 54•20
  - OpenVMS, 17•9–17•10
  - Operating system (OS):
    - access control, 24•2. *See also* Access control certification, 24•2
    - CTSS, 1•7
    - and data backups, 57•19–57•20
    - disk-based (DOS), 1•9–1•10
    - and e-commerce security, 21•20–21•21
    - erasing data, 57•24
    - and extranets, 32•13–32•14
    - file sharing, 24•10–24•11
    - fingerprinting, 15•22
    - and firewalls, 26•8–26•9
    - hidden operating systems and privacy protection, 42•15
    - information flow control, 24•2
    - known-good boot medium, 47•12
    - memory protection, 24•4–24•6
    - mode of processor execution, 24•9–24•10
    - monitoring for intrusion detection, 27•7
    - multiuser, 17•8–17•9
    - new versions, 47•12
    - operations staff responsibilities, 47•12–47•13
    - patches, 21•21, 47•12–47•13
    - performance (speed) errors, 38•12
    - program conflict errors, 38•10, 39•9
    - protection mechanisms, 24•4–24•10
    - protection policies, types of, 24•1–24•2
    - restricted, 17•8–17•9
    - security kernel, 38•5
    - security requirements, 24•2–24•4
    - sharing resources, 24•4–24•5
    - Trojan horse defense, 24•13–24•14. *See also* Trojan horses
    - trusted systems, 24•11–24•14
    - and Web applications, 21•7
    - Windows. *See* Microsoft Windows
    - and writing secure code, 38•5
  - Operation Sundevil, 2•25
  - Operations security:
    - access to operations center, 47•5
    - data protection, 47•13–47•15
    - data validation, 47•15–47•17
    - evaluation phase, security policy development, 66•8
    - operating system, 47•12–47•13
    - operations defined, 47•2–47•3
    - operations management, 47•4–47•12
    - overview, 47•1–47•3, 47•17
  - Opportunity, 4•21
  - Optical character recognition (OCR), 57•20
  - Optical fiber, 5•12, 6•2, 6•9–6•12, 6•18, 15•11, 25•5
  - Oracle, 36•13, 51•29
  - Orange Book*, 1•13–1•14, 17•9, 17•13, 25•11, 51•11, 51•14–51•15
  - Organization for Economic Cooperation and Development (OECD), 54•5, 69•2–69•4
  - Organizational culture, 15•2–15•3, 50•11–50•12, 65•15–65•16
  - Originator-controlled access control, 9•2, 9•6–9•7, 9•9
  - Orthogonal networks, 16•9, 16•11
  - OS/360, 17•9
  - OSI layers, 5•10–5•11
  - Output format errors, 38•12–38•13, 39•11–39•12
  - Output quality, monitoring, 47•12
  - Outsourcing:
    - and application service providers, 30•41–30•42
    - benefits of, 68•2
    - and changes in security landscape, 26•2
    - and collaboration tools, 35•19
    - computer security incident response, 56•6–56•7
    - defined, 68•3
    - degaussing, 57•25
    - and e-commerce, 30•25
    - failure, reasons for, 68•6–68•7
    - insourcing, 68•3–68•4, 68•15
    - intrusion detection and prevention, 27•15–27•16
    - issues and concerns, 68•2
    - managed security service provider (MSSP), 26•32
    - nearshoring, 68•4, 68•15
    - offshoring, 68•4, 68•15
    - overview, 68•21
    - process for outsourcing security functions, 68•18–68•21
    - reasons for, 68•2, 68•4–68•6, 68•15–68•17
    - and risk, 68•7–68•12, 68•18
    - risk management, 68•12–68•15, 68•21
    - SAS 70, *Reports on the Processing of Transactions by Service Organizations*, 54•7–54•10
    - security functions, 68•15–68•21
    - service-level agreements, 68•13, 68•19–68•21
    - terminology, 68•2–68•3
  - Overflow, 4•6
- ## P
- Packet analysis, 26•18
  - Packet filtering, 26•6
  - Packet sniffers, 6•2, 15•10–15•11, 15•25, 16•7, 25•4, 69•9
  - Packet-switching networks, 15•10
  - Packets, 5•7–5•8
  - Pairwise transient key, 33•46
  - Pandemics, 22•3, 22•17, 23•50–23•51. *See also* Physical threats
  - Paperwork Reduction Act of 1995, 54•17
  - Parameter-passing errors, 38•9, 39•8
  - Paravirtualization, 53•25

- Parental tools for Web content filtering, 31•9, 31•12, 48•34–48•35
- Paris Convention for the Protection of Industrial Properties, 11•19, 11•35
- Parity, 4•4–4•6, 4•9
- PASCAL, 38•8
- Passfaces software, 28•12–28•13
- Passwords:
  - access to by system administrators, 28•5
  - and authentication principles, 28•2–28•3, 28•5
  - bypass password, 23•26
  - changing, need for, 28•12
  - cracking, 15•24–15•25, 25•8, 25•10, 25•15, 28•6, 28•9, 46•4
  - and database security, 21•19–21•20
  - dictionary attacks, 28•9–28•10, 28•14
  - encryption, 7•5, 28•9–28•11. *See also* Encryption
  - failed attempts, 28•8
  - guessing, 15•17, 28•8–28•9
  - hashed, 28•9–28•10
  - and LANs, 25•8
  - and local area networks, 6•2
  - MacOS, 25•14
  - and nonrepudiation, 28•5
  - one-time, 28•7, 28•13–28•14
  - overview, 28•17
  - Passfaces software, 28•12–28•13
  - and Public Key Infrastructure (PKI), 28•7–28•8. *See also* Public Key Infrastructure (PKI)
  - same password at multiple sites, 28•7
  - and server spoofing, 28•11
  - sharing, 28•6–28•7
  - and smart cards, 28•14
  - sniffing, 28•9–28•11
  - and system penetration techniques, 15•15
  - theft, 28•5–28•6
  - and Trojan horses, 28•6
  - zero-knowledge password proofs, 28•10–28•11
- Patch and vulnerability group (PVG). *See* Software patches
- Patches:
  - collaboration tools, 35•19
  - firewalls and gateway security devices, 26•21
  - operating systems, 21•21, 47•12–47•13
  - software. *See* Software patches
  - and WLAN security, 33•22
- Patent Cooperation Treaty (PCT), 11•35
- Patent law:
  - disclosure requirement, 11•19
  - infringement, 11•19–11•20, 60•3–60•10
  - international, 11•19
  - overview, 11•18, 42•2
  - Patent Cooperation Treaty (PCT), 11•35
  - and TRIPS, 11•37–11•38
- Payment Card Industry Data Security Standards (PCIDSS), 21•8, 30•11, 53•5, 53•19
- Pdf (portable document format), 44•14, 48•20
- Pedophiles, 48•12–48•13
- Peer-to-peer (P2P) networking:
  - and application security, 5•28
  - BitTorrent, 35•6
  - business threats, 35•3–35•5
  - case study, 35•7–35•8
  - confidentiality, loss of, 35•4–35•5
  - illegal content, 35•4
  - and IP addresses, 5•25
  - Linux software distribution, 35•2, 35•6
  - and malware, 16•6
  - and music downloads, 42•6–42•8
  - Napster, 35•3, 35•5, 42•7–42•8
  - and need for security, 35•1
  - overview, 35•2, 35•20
  - safe messaging, 35•11–35•12
  - security breach prevention and mitigation, 35•5–35•7
  - security incident response, 35•7
  - uses of, 35•3
  - and video piracy, 42•8
  - and viruses, 41•5
- Penalties:
  - awareness programs, 49•14–49•17, 49•27
  - Gramm-Leach-Bliley Act (GLBA), 34•6
  - Health Insurance Portability and Accountability Act (HIPAA), 34•6, 71•13, 71•19–71•20, 71•24
  - Sarbanes-Oxley Act (SOX), 34•6
- Penetration of systems and networks. *See* System and network penetration
- Penetration testing:
  - best practices, 77•11–77•12
  - collaboration tools, 35•19
  - firewalls and gateway security devices, 26•20–26•21
  - red teams, 77•11–77•12
  - secure code, 38•13–38•14
  - and vulnerability assessment, 46•4, 46•7–46•10
- People, Processes, Tools, and Measures (PPTM) framework, 54•19–54•20
- Performance:
  - appraisals, 49•29
  - errors, 38•12, 39•11
  - monitoring, 47•10–47•11, 53•5–53•6
- Perl, 21•15, 21•19
- Personal computers (PCs):
  - history, 1•8–1•10
  - laptops, 1•18, 33•12–33•13, 36•10–36•11, 57•16–57•17
  - maintenance and repair, 4•24–4•25
  - and networks, 5•3
  - and productivity, 1•9
  - security issues, 4•20–4•25
  - spyware. *See* Spyware
- Personal Digital Assistants (PDAs), 17•1, 21•8, 33•13, 57•17

## I • 38 INDEX

- Personal identification number (PIN), 17•7, 23•23, 28•3, 28•8, 28•14
- Personality, 13•3–13•4, 50•4–50•7
- Personally identifiable information (PII), 1•18, 36•9, 53•5, 53•25, 60•14–60•16, 63•6–63•10. *See also* Identity theft
- Personnel. *See* Employees
- PestPatrol, 48•14, 48•42
- Pharming, 18•10, 19•3, 19•8–19•9, 20•29
- Phishing, 2•20, 5•27, 15•30, 16•8, 18•9–18•10, 19•3, 19•8, 19•16–19•17, 20•1–20•3, 20•26–20•29, 21•19, 32•14. *See also* Pharming
- Phone phreaking, 2•7–2•8
- Photodiodes, 6•10
- Phrack, 2•23–2•24, 15•33, 18•4
- Physical access:
  - biometric authentication. *See* Biometric authentication
  - control, 1•9, 1•11, 16•3, 53•18–53•19, 71•18
  - information infrastructure, 23•32–23•33
  - mantraps, 23•33
  - off-hour visitors, 22•23–22•24, 47•6
  - and social engineering, 19•5
  - and threats to information infrastructure, 22•18
  - visitor badges and log in, 23•22–23•23, 47•5–47•6
- Physical layer standards, 5•11–5•12
- Physical losses, 3•10, 3•17–3•18, 4•11–4•13, 4•22. *See also* Power failures and disturbances
- Physical security (infrastructure security), 22•9. *See also* Physical access; Physical site security; Physical threats
  - evaluation phase, security policy development, 66•6–66•7
  - HIPAA requirements, 71•17–71•18
- Physical site security:
  - access, 23•32–23•33. *See also* Access control; Physical access
  - alarms. *See* Alarms
  - and confidential design details, 23•12–23•13
  - construction issues, 23•12–23•13, 23•33–23•35
  - electrical power issues, 23•36–23•38
  - emergency power, 23•38–23•44
  - environmental control, 23•44–23•48
  - HIPAA requirements, 71•17–71•18
  - and information systems security, 22•9. *See also* Physical threats
  - liability issues, 22•7–22•8
  - local area network, 25•3
  - overview, 23•31
  - and physical threats. *See* Physical threats
  - remote spying devices, 23•49
  - responsibility for, 22•7
  - site selection, 23•31–23•32
  - and social engineering, 19•18
  - standards, 23•31
  - surveillance systems, 23•28–23•31
  - violence, 23•49–23•50
  - wiretaps and bugs. *See* Wiretapping
- Physical threats. *See also* Physical site security
  - assessment, 22•9–22•15
  - and backup media protection, 57•20–57•23
  - bombs, 23•49–23•50
  - and business continuity planning, 58•4–58•6
  - civil, political, and economic disruptions, 22•26
  - cleaning and maintenance, 22•24
  - confidential information regarding, 22•26–22•27
  - and control systems, 53•3–53•4
  - coordinated attacks, 22•26
  - costs, 22•6, 22•13–22•14
  - and e-commerce, 30•24
  - fire and smoke, 22•22
  - food and drink, 23•18
  - hazardous material incidents, 22•21
  - health threats, 22•3, 22•17, 22•25
  - high-energy radio-frequency (HERF) weapons, 22•21
  - humidity, 4•12, 22•23, 23•45–23•46, 53•11
  - illicit workstations, 22•25
  - and information infrastructure, 23•8
  - insurance coverage. *See* Insurance
  - leaks, 22•23, 53•11
  - liability issues, 22•7–22•8, 22•10
  - logical security, 22•9
  - man-made, 22•17–22•19
  - medical emergencies, 22•3, 22•17, 22•25, 23•50–23•51
  - mitigation, 23•48–23•52
  - monitoring and control systems, 53•11
  - natural hazards, 22•16–22•17
  - off-hour visitors and contractors, 22•23–22•24, 23•22
  - overview, 22•2–22•10, 22•27–22•28
  - physical security, 22•9
  - premises security, 22•9
  - and productivity, 22•4–22•6
  - responsibility for physical security, 22•7
  - rodents and insects, 23•18
  - and social engineering, 22•3–22•4. *See also* Social engineering
  - solar activity, 22•26
  - storage room, 22•24
  - targets, 22•4
  - temperature, 22•23
  - temperature as security hazard, 3•17, 4•11–4•12, 4•22, 22•23, 23•16–23•17, 23•44–23•46, 53•11, 57•20
  - terminology, 22•8–22•9
  - terrorism. *See* Terrorism and terrorists
  - threat information, sources of, 22•27, 23•51
  - toxic threats, 22•21
  - utility disruptions, 22•26
  - vandalism, 22•26

- violence, 23-49-23-50
- wiretaps. *See* Wiretapping
- workplace violence, 22-6, 22-22
- Piggybacking, 19-7-19-8, 19-13, 19-18, 23-33, 46-9
- PING, 30-27
- Ping, 5-23
- Ping of Death, 18-7, 25-14
- Pinging, 5-23-5-24, 18-8, 18-13
- Piracy. *See also* Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)
  - antipiracy techniques, hardware-based, 42-5-42-12
  - antipiracy techniques, software-based, 42-3-42-5
  - database protection, 11-21
  - and digital rights, 42-2-42-12, 42-16
  - marketplace issues, 11-20-11-21
  - music downloads, 42-6-42-8, 42-10
  - overview, 11-20
  - policies on, 48-30
  - terminology, 42-17-42-20
  - types of, 42-2-42-3
- Plagiarism, 48-30-48-31
- Plain old telephone service (POTS), 4-14-4-15
- Plaintext, 7-2-7-3, 7-6. *See also* Encryption
- Plan, Design, Implement, and Operations (PDIO) framework, 54-20
- Plan-Do-Check-Act (PDCA), 54-5
- Point-to-Point Tunneling Protocol (PPTP), 25-7
- Points of presence (POPs), 1-12
- Policy and procedure:
  - anonymity, 70-18-70-19
  - antivirus technology, 41-13-41-14
  - awareness programs, 49-6
  - collaboration tools, 35-18
  - data classification. *See* Data
  - e-commerce security services, 30-6
  - gateway security device policy, 26-19-26-20
  - instant messaging, 35-9
  - judgment and adaptation, need for, 63-15-63-16
  - local area networks, 25-1-25-3
  - management's role, 63-12
  - peer-to-peer networking, 35-6
  - security incident response, 56-7-56-9
  - security policy, 44-1-44-15, 66-2-66-14
  - short message service (SMS), 35-14
  - writing secure code, 38-1-38-4
- Polymorphic viruses, 16-5
- Ponzi schemes, 48-9-48-10
- Pop-ups, 17-2, 19-18
- Pornography, 1-19, 48-12-48-13, 48-33-48-35, 48-37, 61-3, 72-3, 72-12-72-13
- Port Login (PLOGI), 36-7
- Port numbers, 5-20-5-21
- Port scanning, 15-20-15-21, 16-7, 46-4
- Portable data storage devices, 1-18
- Portable document format (PDF), 44-14, 48-20
- Portal machines, 23-25-23-26
- Ports, disabling, 30-27
- Positive-intrinsic-negative (PIN) photodiode, 6-10
- Possession as source of loss, 3-2, 3-7-3-14
- Post Office Protocol (POP), 5-27, 57-23
- Poulsen, Kevin, 2-8
- Power failures and disturbances, 4-11, 4-19-4-20, 4-23, 22-26, 23-36-23-44, 59-2. *See also* Disaster recovery
- Pre-shared key (PSK), 5-3, 33-46
- Prejudice, 50-9-50-10
- Preliminary evaluation phase, security policy development, 66-2-66-11
- Premises security. *See* Physical site security
- Presidential Directives, 23-3-23-6, 71-3, 71-10, 75-12
- Pretexting, 19-4
- Pretty Good Privacy (PGP), 7-26, 37-2, 37-13, 40-12
- Privacy. *See also* Confidentiality and anonymity, 70-11-70-15 and biometric authentication, 29-17, 29-19-29-21 checklist for implementation of privacy measures, 69-20 contract terms, 69-18-69-20 defined, 70-11 and Digital Rights Management (DRM), 42-3, 42-13-42-14, 42-16 and e-commerce, 21-8 and electronic communications, 11-29-11-33 Electronic Communications Privacy Act, 11-30 genetic discrimination, 69-16 and globalization, 69-1-69-2 Gramm-Leach-Bliley Act. *See* Gramm-Leach-Bliley Act (GLBA) insurance coverage for breaches of, 60-13-60-18 invasion of, remedies for, 11-29 and law enforcement, 69-8-69-9 laws. *See* Privacy law location privacy, 69-15-69-16 and mass e-mailing, 20-14 and national security, 69-8-69-9 and online monitoring, 69-15 and online shopping, 48-24-48-25, 48-40 proposed legislation, 71-10-71-11 and public directories, 21-18 regulatory compliance, 26-2 self-regulation approaches, 69-18 and social networking sites, 69-16 Stored Wire and Electronic Communications and Transactional Records Act (SCA), 11-30, 11-32-11-33 and surveillance systems, 23-19, 23-29, 69-8-69-9 terminology, 42-17-42-20 and Web monitoring, 31-11

## I • 40 INDEX

- Privacy (*Continued*)
  - Web site privacy policies, 30•19
  - and Web site security, 30•39–30•40
  - Wiretap Act, 11•30–11•32
  - workplace, 69•13–69•14
- Privacy Act of 1974, 67•3, 69•7–69•8, 71•8–71•10
- Privacy-enhancing technologies (PET), 31•2, 31•11, 42•14–42•15
- Privacy law. *See also* Privacy compliance, 60•14–60•16
  - compliance models, 69•17–69•20
  - Europe, 69•3–69•6
  - overview, 69•1–69•3
  - sources of, 69•3
  - United States, 69•6–69•17
- Private Branch Exchange (PBX), 51•21–51•22, 51•25
- Private keys, 7•5, 7•8, 7•26–7•27, 7•31–7•32, 7•43, 37•3, 37•5, 37•23. *See also* Encryption
- Privilege management:
  - access control privileges, 23•19–23•20
  - minimum necessary privilege, 17•12
  - operating system security, 24•4, 24•9–24•10, 24•12, 24•15–24•16, 24•18
  - Public Key Infrastructure, 37•24–37•25
- Procedural languages, 47•3
- Procedural statements, 47•3
- Procedures, 44•3. *See also* Policy and procedure
- Process activities, 53•12
- Process control table, 53•9
- Process flow, 53•10
- Process initiation log records, 53•15
- Process tables, 53•9
- Process termination log records, 53•15
- Product assessment:
  - consortium-based approaches, 51•7–51•10
  - hacking approaches, 51•7, 51•11
  - in-house proprietary assessments, 51•7–51•8
  - open source model, 51•7, 51•10–51•11
  - standards. *See* Standards
  - third-party commercial assessments, 51•7, 51•11–51•13
  - trade press, 51•7, 51•11
  - vendor self-declarations, 51•7
- Production system, 47•2, 47•8
- Productivity, 1•9, 22•4–22•6, 48•14–48•29
- Professional education:
  - business continuity management programs, 75•12–75•13
  - continuing education, 74•8, 74•10–74•12
  - distance learning, 75•9–75•12
  - growth of IA education programs in U.S., 75•4–75•5
  - learning continuum, 75•5–75•8
  - need for, 75•8–75•9
  - overview, 74•1, 74•3, 74•24
  - security certification examinations, preparing for, 74•16–74•20
  - TIE model, 75•1–75•4
- Program status word (PSW), 24•5–24•6
- Programmable logic controllers (PLCs), 53•5
- Programmable read-only memory (PROM), 4•9
- Programmer libraries, 47•3
- Programmers, production program access, 47•13
- Programming languages. *See* Computer languages
- Project Lightning, 7•3
- Projectiles as security hazard, 3•18
- Protected health information (PHI), 26•2, 60•16–60•17, 71•12–71•26. *See also* Health Insurance Portability and Accountability Act (HIPAA)
- Protection Profile (PP), 51•19–51•29, 51•31
- Protocol tunneling, 31•10
- Proximity cards, 23•22–23•23
- Proxy servers:
  - network proxy, 42•14–42•15
  - and network security, 26•10, 26•13
  - and Web monitoring, 31•2, 31•8, 31•12, 53•13
- Pseudonymity. *See* Anonymity
- Pseudospoofing, 70•8
- Psychological operations (PSYOP), 14•19–14•20
- Psychology:
  - computer criminals. *See* Computer criminals
  - dangerous information technology insiders. *See* Insiders, information technology
  - and social engineering, 19•10–19•12, 19•19
  - social psychology. *See* Social psychology
- PTR record spoofing, 18•9
- Public Company Accounting and Oversight Board (PCAOB):
  - Auditing Standard (AS) No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, 54•12
  - and COSO framework, 54•19
  - and SOX, 34•2
- Public directories and private documents, 21•18
- Public Key Infrastructure (PKI):
  - architecture, selecting, 37•13
  - background, 37•2–37•4
  - Certificate Policy (CP), 37•8–37•9, 37•17
  - Certificate Revocation List (CRL), 37•6, 37•13, 37•16–37•22, 37•25
  - Certification Authority (CA), 17•5, 21•10–21•11, 37•5–37•22. *See also* Digital certificates
  - certification practice statement (CPS), 37•8–37•9
  - costs, 37•26
  - cross-certification, 37•13–37•14
  - and cross-domain authentication, 28•16
  - encryption, 7•32–7•35
  - enterprise PKI, 37•7–37•8
  - interoperability, 37•14–37•17
  - key expiration and rekeying, 37•21–37•22

key recovery, 37·22–37·24  
 and mobile code, 17·5  
 need for, 37·4–37·5  
 and passwords, 28·7–28·8  
 privilege management, 37·24–37·25  
 proofing (vetting), 37·10  
 recertification, 37·22  
 registration authority (RA), 37·7–37·9  
 revocation, 37·6, 37·13, 37·16–32·21  
 and secure client VPNs, 32·5  
 and signed code, 17·4, 17·6  
 and soft tokens, 28·15, 37·23  
 trust, levels of, 37·9–37·10  
 trust models, 37·11–37·13  
 trusted archival services, 37·25–37·26  
 trusted paths, 37·10–37·11  
 trusted time stamp, 37·26  
 Public keys. *See also* Encryption  
 and digital signatures. *See* Digital signatures  
 encryption, 7·5, 7·22–7·27, 7·36–7·37,  
 7·43  
 key recovery, 37·22–37·24  
 and onion routing, 31·2  
 public key cryptosystems (PKCs), 37·2–37·4  
 Public Key Infrastructure. *See* Public Key  
 Infrastructure (PKI)  
 rekeying, 37·21–37·22  
 and server spoofing, 28·11  
 smart cards, 28·14  
 and soft tokens, 28·14–28·15  
 validity period, 37·21–37·22  
 X.509 standard. *See* X.509 certificate format  
 Public relations, 56·30, 58·14, 60·17  
 Publications, product reviews, 51·11  
 Punched-card systems, 1·3–1·4  
 Python, 21·15

**Q**

Quality assurance, software, 39·2–39·3,  
 47·10–47·12. *See also* Software  
 development  
 Quality control, 47·10  
 Quality of service (QoS), 34·12, 34·14  
 Quantitative risk model, 58·29–58·31  
 Quantum cryptography, 7·38–7·42  
 Quarantines, 20·32  
 Quicken, 17·7  
 QuickTime, 26·16

**R**

Race condition errors, 38·9–38·10, 39·9, 39·14,  
 48·22, 52·4  
 Radiation, 4·12–4·13  
 Radio-frequency identification (RFID), 23·19,  
 23·21–23·23, 23·25, 53·25, 69·17  
 Radio Regulatory Technical Advisory Group  
 (RR-TAG), 6·18  
 Radio signals, 5·12, 22·21  
 RADIUS, 32·5, 33·46, 34·11

Radon, 22·21  
 RAID. *See* Redundant Array of Independent  
 Disks (RAID)  
 Rainbow Series, 1·13–1·14, 54·14–54·15  
 Rainbow Technologies, 7·30  
 RAMAC (Random Access Method of Accounting  
 and Control), 1·5  
 Random access memory (RAM), 4·8,  
 15·16–15·17, 36·2, 38·10, 39·9  
 Random sampling, 10·5–10·6, 10·8  
 Range checks, 52·10  
 Rapid application development (RAD), 39·7,  
 52·2  
 Rapid Spanning Tree Protocol (RSTP), 5·12  
 Raw sockets, 25·11  
 RC4. *See* Rivest Cipher 4 (RC4)  
 Read-after-write, 4·6, 4·9  
 Read-only access, 36·8  
 Read-only memory (ROM), 4·8–4·9  
 Readers, specialized, 42·6–42·10  
 Real-only file security, 30·36–30·37  
 Real-time systems, 1·7  
 Real-time Transport Protocol (RTP), 34·8–34·10,  
 34·13  
 Recording Industry Association of America  
 (RIAA), 42·6–42·8, 42·19  
 Recovery procedures, 4·20, 36·9–36·10, 52·6,  
 57·6  
 Redundancy, as security element, 23·14–23·15  
 Redundancy checks, 4·4–4·6, 4·9, 4·16  
 Redundant Array of Independent Disks (RAID),  
 23·15, 36·3, 57·4–57·5, 57·22  
 Reference Model of Open Systems  
 Interconnection (OSI). *See* Open Systems  
 Interconnection (OSI) Reference Model  
 Reference monitor concept, 24·12–24·13  
 Registered Jack (RJ), 5·3  
 Registration authority (RA), 37·7–37·9  
 Registry keys, 17·11  
 Regression testing, 39·15, 39·17  
 Regulatory compliance. *See* Legal and regulatory  
 compliance  
 Rekeying, 37·21–37·22  
 Reliability:  
 information assurance, importance of,  
 77·14–77·15  
 protocols, 5·19  
 UDP, 5·23  
 Remote Access Dial-In User Service (RADIUS),  
 25·7  
 Remote Authentication Dial-in User Service  
 (RADIUS). *See* RADIUS  
 Reordering of data, 3·15  
 Replacement of data, 3·2, 3·15  
 Replaying, 33·9  
 Replication, 4·6–4·7  
 Reporting:  
 chief information security officer (CISO),  
 65·12–65·13, 65·17



## I • 42 INDEX

### Reports:

- exception reports, 53•23
- Repudiation, 3•2, 3•12–3•13, 3•15–3•16, 28•5.  
*See also* Nonrepudiation
- Reputation, damage to, 48•2–48•11, 60•16, 65•16
- Requests for Comments (RFCs). *See* Internet Engineering Task Force (IETF)
- Requirements analysis, 38•4–38•5, 39•6
- Research methodology, computer crime, 10•3–10•11
- Resilient Packet Ring (RPR), 6•18
- Resource exhaustion errors, 38•10, 39•9
- Resource starvation, 18•11
- Resource utilization logs, 53•17
- Reverse engineering, 42•12
- Reverse-path filtering, 31•10
- Reverse social engineering, 19•10
- Revocation:
  - Authority Revocation List (ARL), 37•19
  - Certificate Revocation List (CRL), 37•6, 37•13, 37•16–37•21
  - public key, 37•18–37•21
- Reward and punishment, 50•13, 50•15, 63•13
- RFC (Request for Comment). *See* Internet Engineering Task Force (IETF)
- Rich text format (rtf), 44•14, 48•19
- Right to Financial Privacy Act of 1978, 69•8
- Ring topology, 6•4–6•5
- Risk assessment:
  - algorithms, 62•17–62•18, 62•22
  - annualized loss expectancy (ALE), 62•3–62•18, 62•22–62•24
  - and due diligence, 63•20–63•21
  - e-commerce Web sites, 30•22–30•24
  - and future of information assurance, 77•9
  - loss potential, 62•17–62•23, 63•19
  - objective, 62•5–62•6
  - occurrence rate, 62•22, 63•19
  - outage duration, 62•22
  - and outsourcing, 68•7–68•12
  - questionnaires, use of, 62•6–62•7
  - return on investment (ROI), 62•5–62•6, 62•11, 62•13–62•16, 62•21, 62•23–62•24
  - risk model, 62•7–62•10, 62•16
  - risk reduction, assurance-based, 77•13–77•16
  - sensitivity testing, 62•23–62•24
  - techniques, 62•16–62•24
  - and Trusted Information Environment, 75•3
- Risk management. *See also* Risk assessment
  - annualized loss expectancy (ALE), 62•3–62•18, 62•22–62•24
  - DHS/FEMA methodology for, 23•55–23•56
  - legal and regulatory compliance, 62•4
  - mitigation of risk, 62•10–62•16, 62•24
  - and outsourcing, 68•12–68•15
  - overview, 62•2, 63•3
  - risk classification, 63•18–63•19
  - risk defined, 62•1–62•2

- risk reduction, assurance-based, 77•13–77•16
- standards, 62•3–62•4
- Rivest Cipher 4 (RC4), 7•29–7•30, 25•7, 37•2
- RJ-11 connectors, 5•3
- RJ-45 connectors, 5•3
- Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988, 23•6
- Robust Security Network Associations (RSNAs), 33•25–33•36, 33•47
- Robust Security Network (RSN), 33•25–33•32, 33•46
- Role-based access controls, 9•2, 9•7–9•9
- Root capability, 21•5
- Rootkits, 8•14, 15•24–15•25, 16•7, 17•3, 20•30–20•31, 21•4, 41•2, 55•13–55•14
- Router solicitation/advertisement (RS/RA), 26•16
- Routers:
  - and access control lists, 26•5–26•6, 26•8, 26•17
  - access router, 5•2–5•3
  - additional modules, 26•8
  - denial-of-service attacks (DoS), 18•12
  - dynamic routing protocols, 5•26
  - and layered defense, 16•10
  - and network interconnection, 6•25
  - and network security, 16•10, 26•8, 26•17
  - onion routers, 31•2, 31•11, 35•7
  - terminology, 5•7
- Routing and Domain Name System attacks, 18•9–18•10
- Routing Information Protocol (RIP), 5•26
- RSA Data Security Company:
  - cryptographic toolkits, 38•8
  - CSIRT management conferences, 56•34
  - password generators, 28•13
  - RSA algorithm, 7•24–7•27, 7•35–7•37, 7•41, 37•16, 37•22. *See also* Encryption
  - SecurID, 28•13, 28•16
- RST (Reset + Restart) message, 5•9, 5•18–5•19, 26•12

## S

- S/HTTP, 21•10
- S/MIME. *See* Secure/Multipurpose Internal Mail Extensions (S/MIME)
- \*-property (star property), 24•12, 24•14
- Safes, 57•21
- Salami fraud, 2•10
- Saliency effect, 50•9–50•10
- Sandboxes, 17•4, 17•8–17•9, 38•8
- Sarbanes-Oxley Act (SOX):
  - audits, 54•13–54•14
  - and business continuity planning, 58•3
  - certification requirements, 54•14
  - and COBIT, 54•12–54•13
  - and code security, 38•4, 39•9–39•10
  - compliance, 54•13, 54•19, 64•11–64•14
  - and computer security, 60•3
  - control framework, 54•11–54•12

- and data classification, 67-5
- and data management, 57-17
- and documentation, 39-15, 39-18
- and information protection, 71-1
- insurance industry compliance, 34-2
- internal control weaknesses, 38-4, 39-9-39-10
- and ISO/IEC 27001 ISMS certification, 54-5, 54-15
- management perspective on, 64-5-64-6
- metrics, 49-35
- and monitoring and control systems, 53-5
- and need for network level centralized control, 26-3
- overview, 54-10-54-11, 54-14, 64-2-64-4, 64-11, 64-14
- penalties, 34-6
- and physical threats to infrastructure, 22-6-22-7
- provisions of (list of titles), 64-3
- and risk management, 62-4
- and role of CISO, 65-13, 65&
- schedule for compliance activities, 54-14
- section 404, internal control over financial reporting, 54-11, 64-4-64-5, 67-5
- security awareness and training, 49-4
- and security planning, 23-6
- and VoIP compliance, 34-2-34-3, 34-6-34-7
- SATAN (Security Analysis Tool for Auditing Networks), 15-19, 15-21, 46-3
- Saudi Arabia Internet content regulation, 72-6
- SCADA. *See* Supervisory control and data acquisition (SCADA)
- Scanners, 15-20-15-23, 40-15-40-16, 46-5. *See also* Antivirus programs; Networks
- Schema and schemata, 50-3-50-4, 50-11-50-13
- Schneider, Jerry Neal, 2-5
- Schools. *See also* Colleges and universities
  - Web monitoring and content filtering, 31-3, 31-11, 72-14, 72-16-72-17
- Screened subnet firewall, 26-17
- Screensavers, 20-30-20-31
- Scriptlet.typlib, 25-10
- Script kiddies, 16-2, 18-1, 55-13
- Scripting languages, 21-15
- Search engines, 19-7, 31-6, 31-12
- Search warrants, 61-9, 70-9
- Secure Hash Algorithms (SHA), 34-14
- Secure/Multipurpose Internal Mail Extensions (S/MIME), 5-27, 20-18, 21-10, 37-6, 37-16
- Secure Real-Time Protocol (SRTP), 34-13-34-14
- Secure remote access, 32-2, 32-11-32-15. *See also* Virtual private networks (VPNs)
- Secure Session Initiation Protocol (SSIP), 34-9, 34-13
- Secure Shell (SSH), 5-27, 25-4, 28-10, 31-10
- Secure Sockets Layer (SSL). *See also* Transport Layer Security (TLS)
  - application standards, 5-27
  - and e-commerce, 21-10, 30-11-30-12
  - encryption, 26-15, 26-18
  - and encryption, 7-28-7-30
  - and extranets, 32-12
  - firewalls, 30-38
  - and mobile code, 17-3
  - and password encryption, 28-10-28-11
  - SSL/TLS. *See* Secure Sockets Layer/Transport Layer Security (SSL/TLS)
  - testing, 51-8-51-9
  - and Transport Layer Security (TLS), 34-13
  - and trust chain, 37-4-37-5
- Secure Sockets Layer/Transport Layer Security (SSL/TLS), 5-27, 32-3-32-6
- SecurID, 28-13, 28-16
- Securities and Exchange Commission (SEC), 26-3, 60-14
- Security administration, 63-26-63-29
- Security administrators, 47-4-47-5, 63-26-63-29
- Security Assertion Markup Language (SAML), 28-15-28-16
- Security assurance requirements, 51-19-51-21
- Security awareness. *See* Awareness programs
- Security Breach Information Act (California), 71-9
- Security by wandering around (SBWA), 49-35
- Security conferences, 63-13
- Security descriptor, 24-16-24-19
- Security functions, outsourcing, 68-15-68-21. *See also* Outsourcing
- Security Guidelines Handbook*, 44-6-44-7
- Security ID (SID), 24-14-24-18
- Security Impact Analysis (SIA), 51-28
- Security incidents:
  - attacks, 8-12-8-16
  - awareness programs. *See* Awareness programs
  - common language for, 8-1-8-20
  - defined, 8-1
  - Department of Veterans Affairs, 63-6-63-10
  - evaluation phase, security policy development, 66-10-66-11
  - events, 8-4-8-11
  - incident defined, 8-15
  - overview, 56-2-56-3
  - reporting, 49-20
  - reputation damage, 60-16
  - response team. *See* Computer security incident response team (CSIRT)
  - victims, notifying, 63-4, 63-6-63-7
  - virus detection, policies and strategies, 41-13-41-14
- Security kernel database, 24-12-24-13
- Security officer, 47-4-47-5
- Security planning:
  - All-Hazard Mitigation Plan, 23-6, 23-52
  - auditing standards, 23-7
  - cost-benefit analysis, 23-53
  - defensive strategies, 23-8-23-9

## I • 44 INDEX

- Security planning (*Continued*)
  - federal guidelines, 23•10–23•11, 23•52. *See also* Legal and regulatory compliance
  - implementation, accountability, and follow-up, 23•54–23•55
  - legal and regulatory compliance. *See* Legal and regulatory compliance
  - management responsibilities, 63•23–63•25
  - security response plan, 23•54
  - strategic planning, 23•7–23•11
- Security policy:
  - collaboration in developing, 66•2
  - development phases, 66•2–66•14
  - implementation, 66•12–66•14
  - maintenance, 44•14–44•15, 66•14
  - management support, 66•11–66•12
  - need for, 66•2–66•3
  - needs analysis, 66•12
  - organization, 44•11–44•12
  - overview, 66•14
  - policy development group, 66•3
  - preliminary evaluation phase of policy
    - development, 66•2–66•11
  - publishing, 44•12–44•14
  - recommendations for creating and implementing, 44•15
  - resources for policy writers, 44•3
  - review of, 44•15
  - standards, 44•3–44•9
  - templates, 44•9–44•10
  - terminology, 44•2–44•3
  - updating, 44•15
  - and Web application systems, 21•5–21•6
  - writing, 44•10–44•11, 66•12
- Security Proof of Concept Keystone (SPOCK), 51•8–51•9
- Security response plan, 23•54
- Security services, 30•5–30•9
- Security Target (ST), 51•19–51•21, 51•23–51•26, 51•31
- Security through obscurity, 5•6
- Security University, 74•5, 74•20–74•22
- Seduction, 19•5
- Seeding, 39•15
- SEEK, 7•27
- Segmentation, secrets, 23•11–23•12
- Self-Monitoring, Analysis, and Reporting Technology (SMART), 4•10
- Semiconductor Chip Protection Act of 1984 (SCPA), 11•12
- Sendmail*, 16•5, 17•13
- Sensitive compartmented information facilities (SCIFs), 15•13
- Separation of duties, 45•9–45•10, 47•4
- September 11, 2001 attacks, 14•20–14•21, 22•2, 22•6, 58•4, 59•3, 59•5, 59•21, 62•12–62•13. *See also* Terrorism and terrorists
- Serial broadcast, 6•5
- Server Message Block (SMB), 36•3, 36•8
- Server-Side Includes (SSIs), 15•29, 21•17–21•18
- Servers:
  - antivirus scanners, 41•12–41•13
  - buffer overflow attacks, 21•4
  - dial-up server and LANs, 25•6
  - and extranet systems, 32•15
  - and extranets, 32•13–32•14
  - local area network, 1•11
  - mix server, 31•2
  - and mobile code, 17•12–17•13. *See also* Mobile code
  - proxy servers. *See* Proxy servers
  - revocation protocols, 37•20–37•21
  - root servers, 5•25
  - server spoofing, 28•11
  - Web Server security, 21•16–21•19, 27•14
  - Web servers. *See* Web servers
- Service-level agreements (SLAs), 47•10, 68•13, 68•19–68•21. *See also* Outsourcing
- Service organizations, 54•7–54•10. *See also* Outsourcing
- Service-oriented architecture (SOA), 5•28, 30•23
- Service set identifier (SSID), 15•12
- Services, 6•26
- Session border control (SBC), 34•14
- Session hijacking, 36•7, 36•9
- Session initiation log records, 53•15
- Session Initiation Protocol (SIP), 34•9, 34•13
- Session termination log records, 53•15
- SET, 21•10
- Shadowcrew, 2•26
- Sharing resources, 24•4–24•5
- Shielded twisted pair (STP), 6•9
- Shiftwork, 56•29–56•30
- Short message service (SMS):
  - and BlackBerrys, 35•14–35•15
  - business threats, 35•12–35•13
  - guidelines for security planning, 35•15
  - and need for security, 35•1
  - overview, 35•2–35•3, 35•12, 35•20
  - security breach prevention and mitigation, 35•13–35•15
  - security incident response, 35•16
- Shoulder surfing, 15•19, 46•9
- Simple Certificate Validation Protocol (SCVP), 37•20–37•21
- Simple Mail Transfer Protocol (SMTP), 5•27, 17•12–17•13, 20•3–20•5, 20•24, 21•7, 21•12, 26•15–26•16
- Simple Network Management Protocol (SNMP), 5•22, 5•26, 25•9
- Simple security property, 24•12
- Simultaneous broadcast, 6•6
- Site security, 25•3
- Site Security Handbook*, 44•8–44•9
- Site-to-site (S2S) VPNs, 32•6–32•7
- Skype, 32•10–32•11
- Slashes, 15•29

- Small Computer System Interface (SCSI), 57·4
- Small to medium business (SMB) appliances, 26·10
- Smart Card Security Users Group, 51·9–51·10
- Smart cards, 7·30, 7·38, 25·11, 28·2–28·4, 28·13–28·14, 32·5
- Smoke. *See* Fire and smoke
- SMURF, 18·8, 18·13, 25·14
- Snapshots, 53·7
- SnifferPro, 25·4
- Sniffit, 25·4
- Snopes.com, 48·6
- Snort, 25·4
- Social engineering:
  - and awareness programs, 49·40. *See also*
    - Awareness programs
    - background, 19·2–19·4
    - and computer security incident response, 56·27
    - consequences of, 19·12–19·13
    - detection, 19·15–19·16
    - employee training and awareness, 19·17
    - examples, 19·13–19·14
    - frequency of use, 19·3
    - insiders, dangerous. *See* Insiders, information technology
    - and Kevin Mitnick, 2·5–2·6
    - low-tech attacks, 19·4, 19·6–19·8
    - and malicious code, 16·6, 41·5
    - methods, 19·4–19·10
    - overview, 19·18–19·19
    - and penetration testing, 46·8–46·10
    - pharming. *See* Pharming
    - phishing. *See* Phishing
    - pretexting, 54·6
    - prevention of, 19·16–19·19
    - profile of social engineer, 19·12
    - psychology of, 19·10, 19·19
    - responding to, 19·16
    - small business versus large organizations, 19·14–19·15
    - social psychology, 19·11–19·12
    - and spam, 48·9
    - success rate, 19·14
    - and system penetration, 15·3–15·7
    - targets of, 19·4
    - trends, 19·15
    - and Trojan horses, 19·2
- Social Engineering Defense Architecture (SEDA), 19·16
- Social networking, 48·5, 69·16
- Social psychology:
  - anonymity and aggression, 70·6–70·7
  - anonymity and prosocial behavior, 70·7–70·8
  - attribution errors, 50·7–50·10
  - behavior, explanations of, 50·7
  - beliefs and attitudes, 50·13–50·16
  - cultural differences, 50·10–50·11
  - deindividuation theory, 70·5–70·7
  - group behavior, 50·20–50·21
- identity in cyberspace, 70·8–70·10
- and implementation of security practices, 50·1–50·2
- initiative, encouraging, 50·16–50·19
- personality, theories of, 50·4–50·7
- rationality, 50·2
- reality, framing, 50·11–50·12
- recommendations, 50·22–50·24
- reward versus punishment, 50·13, 50·15, 63·13
- schema, 50·3–50·4
- security policies, explaining, 50·12–50·13
- and technological generation gap, 50·21–50·22
- Sockets, 5·21–5·22
- Software. *See also* Applications
  - agents, 53·11
  - antivirus. *See* Antivirus programs
  - commercial off-the-shelf (COTS) software, 14·3, 17·3, 21·13, 21·21, 47·9
  - communications software, 6·26
  - component-based software (CBS), 21·13
  - computer programs, 47·3
  - and data backups, 57·19–57·20
  - data classification, 67·7–67·8
  - data integrity, 47·16
  - development. *See* Software development
  - downloading, 48·13
  - early development of, 1·9–1·10
  - errors, types of, 38·8–38·13, 39·7–39·12
  - externally supplied, 47·9
  - and indispensable employees, 45·4–45·6
  - keys, 42·11–42·12
  - misconfiguration, 21·16–21·17, 21·21
  - network operating system. *See* Network operating systems (NOS)
  - new versions of, responsibilities of operations staff, 47·6–47·8
  - Passfaces, 28·12–28·13
  - password crackers, 15·24
  - patches. *See* Software patches
  - piracy, 48·30
  - purchase criteria, 40·22–40·23
  - threats to, 24·3
  - tokens (soft tokens), 28·14–28·15
  - tracking versions of, 47·6–47·7
  - uninstalling, 40·13
  - usage counters, 42·4–42·5
- Software & Information Association, 42·3
- Software development:
  - automated testing, 39·15–39·16
  - best practices, 77·10–77·11
  - bugs, tracking and removal, 39·16
  - bugs and debugging, 39·5, 39·18–39·20
  - change management, 39·16–39·18
  - data corruption, 39·19
  - design flaws, 39·18
  - design phase, 39·6
  - documentation, 38·11, 39·10, 39·17–39·18
  - errors, types of, 39·7–39·12

## I • 46 INDEX

- Software development (*Continued*)
  - evaluation phase, security policy development, 66•7–66•8
  - hacking, 39•19–39•20
  - implementation flaws, 39•18
  - implementation phase, 39•6
  - joint application design (JAD), 39•7, 52•2
  - life cycle. *See* Software development life cycle (SDLC)
  - maintenance phase, 39•6
  - overview, 39•2
  - rapid application development (RAD), 39•7, 52•2
  - regression testing, 39•15
  - requirements analysis, 39•6
  - secure code, writing. *See* Codes and coding
  - software development life cycle (SDLC), 39•3–39•7
  - software quality assurance (SQA), 39•2–39•3, 39•18–39•19
  - standards for assessing competency of developers, 51•13–51•14
  - test cases, designing, 39•12–39•15
  - testing, 39•5–39•6, 39•15–39•16
  - unauthorized changes, 39•18
  - Web sites for secure coding information, 38•13
- Software development life cycle (SDLC):
  - joint application design (JAD), 39•7, 52•2
  - overview, 39•3–39•4
  - phases, 39•4–39•5
  - rapid application development (RAD), 39•7, 52•2
  - security integration, 39•7
  - waterfall model, 39•5–39•7
- Software Engineering Institute, 44•8, 56•4. *See also* Computer Emergency Response Team Coordination Center (CERT/CC)
- Software patches. *See also* Updates
  - after security compromise, 40•24
  - automated, 40•2–40•4, 40•13–40•14
  - distributing to administrators, 40•15
  - enterprise patching solutions, 40•18–40•22
  - operating system, 47•12–47•13
  - overview, 40•1–40•2, 40•24–40•25
  - patch and vulnerability group (PVG), creation of, 40•4–40•6
  - patch logs, 40•16–40•17
  - process for patch and vulnerability management, 40•4–40•17
  - remediation database, 40•11
  - and software purchase considerations, 40•22–40•23
  - standardized configurations, use of, 40•23–40•24
  - testing, 40•15
  - uninstall, 40•13
- Software total quality management, 38•2–38•3
- Solar activity, 22•26
- Solsniff, 25•4
- Sony Music, 17•3
- Source code. *See* Codes and coding
- Source libraries, 47•3
- Spam:
  - antispam router, 20•23–20•24
  - appending services, 20•16–20•17
  - CAN-SPAM Act of 2003, 20•15, 20•25–20•26
  - costs of, 20•6–20•7, 20•10–20•13
  - criminal prosecution, 20•9
  - defined, 48•3
  - e-mail content filtering, 5•27
  - filters, 20•20–20•23
  - forged headers, 48•8
  - fraudulent return addresses, 70•3
  - history, 2•19–2•20
  - impact of, 20•7–20•8, 20•11–20•13
  - and IRC bots, 16•8
  - and ISPs, 20•19–20•20
  - origin of term, 20•7–20•8
  - overview, 20•1–20•3
  - and permissions, 20•16–20•17
  - preventing, 20•17–20•26
  - productivity, effect on, 48•14
  - profitability of, 20•9
  - recommendations for protecting against, 48•42
  - scams, 20•9–20•10
  - versus SPAM™, 48•3
  - SPam over Internet Telephony (SPIT), 34•9
  - and Trojan horses, 20•32. *See also* Trojan horses
  - as unsolicited commercial e-mail (UCE), 20•8
- Spamhaus Project, 20•17, 20•20
- Spanning Tree Protocol (STP), 5•12
- Spear phishing, 19•8, 20•29. *See also* Phishing
- SpectorSoft, 21•9
- SPI Dynamics, 21•16
- Spim, 19•8–19•9
- Spit, 19•8–19•9
- SPIT (SPam over Internet Telephony), 34•9
- SPOCK (Security Proof of Concept Keystone), 51•8–51•9
- Spoofing:
  - antispoofing, 26•11
  - defined, 8•10
  - examples of, 8•8
  - IP address, 5•15, 18•24, 18•26–18•27, 26•11, 30•30–30•31, 31•9–31•10, 36•7, 36•9
  - PTR record spoofing, 18•9
  - public key spoofing, 37•4
  - server spoofing, 28•11
  - and social engineering, 19•8
  - socket spoofing, 5•21–5•22
- Spread spectrum radio transmission, 5•12
- Spybots, 17•11. *See also* Bots
- Spyware:
  - and e-commerce, 21•9
  - and Internet use, 48•13–48•14, 48•41–48•42
  - overview, 16•6–16•7
  - personal computers, 65•2

- SQL Slammer worm, 16·5–16·6, 53·12
- SSH. *See* Secure Shell (SSH)
- SSH Communications Security, 25·4
- SSL. *See* Secure Sockets Layer (SSL)
- SSL/HTTP-based tunnels, 30·32
- Stakeholders, 63·20
- Standard for Interoperable LAN Security (SILS), 6·17
- Standard of care, 65·6–65·8, 65·13–65·14, 65·18
- Standards:
  - alternatives to, 51·7–51·13
  - American National Standards Institute (ANSI), 6·22, 37·16
  - British Standard 7799 (BS7799), 44·3–44·4, 54·3–54·4, 62·3
  - Capability Assessment for Readiness (CAR) Report, 23·7
  - Capability Maturity Model (CMM), 51·13–51·14
  - classes of security standards, 51·5
  - COBIT. *See* Control Objectives for Information and Related Technology (COBIT)
  - combined standards, product and product builder assessment, 15·15–15·16, 51·14
  - Committee for National Security Systems (CNSS), 75·5, 75·7
  - Common Criteria (CC), 51·10, 51·12, 51·15–51·31
  - Common Criteria Evaluation and Validation Scheme (CCEVS), 1·13, 51·15, 51·17–51·18, 51·25–51·30
  - Common Evaluation Methodology (CEM), 51·26
  - and core layers, 5·9–5·10
  - and data classification, 67·5–67·6
  - disaster/emergency preparedness, 22·10
  - due diligence, 3·14, 3·20
  - Emergency Management Assessment Program (EMAP), 23·7
  - federal government identity cards, 28·15
  - goals of standardization, 51·6
  - IEEE. *See* IEEE 802 standards
  - informal security standards, 44·5–44·9
  - information security governance, 65·8
  - Information Security Standard (ISO) 17799, 23·7
  - Information Technology Infrastructure Library (ITIL), 54·15, 65·8
  - International Organization for Standardization. *See* International Organization for Standardization (ISO)
  - International Telecommunications Union – Telecommunications Standards Sector. *See* International Telecommunications Union – Telecommunications Standards Sector (ITU-T)
  - Internet Engineering Task Force. *See* Internet Engineering Task Force (IETF)
  - ISO. *See* International Organization for Standardization (ISO)
  - ISO/IEC 17799:2005, 44·3
  - IT Infrastructure Library (ITIL), 65·8
  - layered standards architectures, 5·10–5·11
  - local area networks, 6·14–6·23. *See also* Local area networks (LANs)
  - National Electric Code (NEC), 23·14
  - National Institute of Standards and Technology (NIST). *See* National Institute of Standards and Technology (NIST)
  - OSI, 5·10
  - overview, 1·13, 44·2–44·3, 51·2, 51·30–51·31
  - physical site security, 23·31. *See also* Physical site security
  - product builders, standards for assessing, 51·13–51·14
  - products, 51·2–51·6, 51·13–51·16
  - Public Key Cryptography Standards (PKCS), 37·16
  - Rainbow Series, 1·13–1·14, 54·14–54·15
  - recommendations, 1·1·16·1·17, 1·14–1·15
  - risk assessment and management, 62·3–62·4 and risk management, 51·3–51·4
  - security auditing, 23·7
  - security-enabled products, 51·5
  - security products, 51·5
  - single network, 5·11–5·12
  - sources of, 51·4–51·5
  - Telecommunications Industry Association/Electronic Industry Alliance (TIA/EIA), 23·14
  - and trust, 51·3–51·4, 51·6
  - types of product-oriented standards, 51·5–51·6
  - value of, 51·2–51·3
  - writing secure code, 38·15
  - X.509. *See* X.509 certificate format
- Star property (\*-property), 24·12, 24·14
- Star topology, 6·4
- Star-wired bus, 6·6–6·7, 6·9, 6·23
- Star-wired ring, 6·6–6·7, 6·9
- State emergency operations plan, 23·54
- State law:
  - admissibility of expert testimony, 73·4
  - customers, advising of information security breaches, 63·4
  - information security, personal data, 71·9
  - privacy laws, 34·8, 69·6, 69·17
  - and VoIP, 34·5
- State University of New York (SUNY), 75·10–75·11
- Stateful inspection, 26·5–26·7, 26·10
- Statement of work (SOW), 68·18–68·19
- Statements on Auditing Standards (SAS):
  - SAS 70, *Reports on the Processing of Transactions by Service Organizations*, 54·7–54·10
- Static electricity, 4·23–4·24, 23·46

## I • 48 INDEX

- Statistics, and computer crime studies, 10•2–10•9
  - Stay Safe On-Line, 75•8
  - Steganography, 31•11
  - Steve Jackson Games, 2•25
  - Stopbadware.org initiative, 51•12–51•13
  - Storage area network (SAN), 18•12, 36•2–36•5, 57•4, 64•16, 74•5, 74•15
  - Storage media:
    - and data backups. *See* Data backups
    - and data leakage, 1•18
    - degradation, 57•19
    - destruction, 57•24–57•25
    - discarding, 15•18, 36•13, 57•23–57•25
    - environmental protection of, 57•20
    - jukeboxes, 57•8
    - longevity, 57•18–57•19
    - nonvolatile media, 36•1
    - off-site storage, 57•21–57•23
    - on-site protection, 57•20–57•21
    - rotation, 57•18
    - secondary storage, 4•9–4•10
    - theft, 4•22
    - transportation of, 57•21
    - volatile storage, 36•1–36•2
  - Storage Networking Industry Association (SNIA), 57•2
  - Storage rooms, 22•24
  - Stored Wire and Electronic Communications and Transactional Records Act (SCA), 11•30, 11•32–11•33
  - STRIDE framework, 54•20
  - Structured Query Language (SQL) injection, 26•13, 32•14
  - Subnetwork Access Protocol (SNAP), 6•23
  - Subversion, 17•11, 21•15–21•16
  - Sun Microsystems, 17•9, 51•29. *See also* Java
  - Supervisory control and data acquisition (SCADA), 53•11, 53•24
  - Surveillance systems, 23•14, 23•18, 23•26–23•32, 69•8–69•9, 70•12–70•13. *See also* Privacy
  - Surveys as computer crime research method, 10•6, 10•9–10•10
  - Switched network services, 5•5
  - Switches, 5•4–5•5, 5•12, 6•24–6•25
  - Switzerland, 76•10
  - Sybase, product validation, 51•29
  - Symantec, product validation, 51•29
  - SYN flooding, 18•10–18•11
  - Synchronous communications, 15•9
  - Synchronous dynamic random access memory (SDRAM), 4•8
  - Synchronous time, 4•10–4•11
  - SysAdmin, Audit, Network, Security Institute (SANS). *See* System Administration and Network Security (SANS) Institute
  - System Access Control List (SACL), 24•16
  - System Administration and Network Security (SANS) Institute, 44•10, 49•35, 74•16
  - System administrators:
    - password access, 28•5
    - software patches, responsibility for, 40•6
  - System and network penetration:
    - exchange of information on, issues with, 15•31–15•34
    - factors, 15•1–15•3
    - information availability issues, 15•30–15•34
    - and Internet information, 15•30
    - nontechnical methods, 15•3–15•7
    - overview, 15•34–15•35
    - sources of information on, 15•32–15•34
    - technical methods, 15•7–15•30
    - testing, tools, and techniques, 15•19–15•25
    - through Web sites, 15•25–15•29
    - trends, 15•34
  - System boot log record, 53•14
  - System components, monitoring and control, 53•11–53•12
  - System console activity file log, 53•16–53•17
  - System development life cycle (SDLC), 63•4–63•5
  - System mode, 24•9
  - System requirements, monitoring and control, 53•4
  - System response, monitoring and control, 53•2
  - System shutdown log record, 53•14–53•15
  - System start-up, 4•8
  - System state, 53•11
  - System tables, 53•9
  - Systems Security Certified Practitioner (SSCP), 74•14, 74•22
  - Systems Security Engineering Capability Maturity Model (SSE-CMM), 51•13–51•14
- ## T
- 2600: *The Hacker Quarterly*, 2•23, 15•33, 18•4
  - Tables of values or codes, validity checks using, 52•10–52•11
  - Tailgating, 19•7–19•8, 19•18
  - Taking as means of information loss, 3•2, 3•17
  - Taxonomy, computer security incident information, 8•4–8•16
  - TCP/IP (Transmission Control Protocol/Internet Protocol):
    - and data communications, 5•8, 7•28
    - and denial-of-service attacks, 18•1. *See also* Denial-of-service attacks (DoS)
    - Domain Name System. *See* Domain Name System (DNS)
    - Dynamic Host Configuration Protocol (DHCP), 5•25
    - dynamic routing protocols, 5•26
    - and e-commerce, 21•10, 30•25
    - history, 1•12
    - Internet Control Message Protocol (ICMP), 5•23–5•24
    - and layered standards architectures, 5•10–5•11, 7•28

- and network operating systems, 6•27
- packet sniffers. *See* Packet sniffers
- and protecting Web applications, 21•6–21•7
- Simple Network Management Protocol (SNMP). *See* Simple Network Management Protocol (SNMP)
- and wiretapping, 15•10
- TCP port 80, 15•22, 18•21, 30•32
- TCP port 443, 30•32, 30•38
- TCP (Transmission Control Protocol), 5•17–5•22. *See also* TCP/IP (Transmission Control Protocol/Internet Protocol)
- Tcpdump, 25•4
- Teardrop, 25•14
- Teardrop attacks, 18•9
- Tebibytes, 4•4
- Telecommunications Industry Association/Electronic Industry Alliance (TIA/EIA), Standard 606, *Administration Standard for the Telecommunications Infrastructure of Commercial Buildings*, 23•14
- Telecommuting, 1•12
- Telephone Consumer Protection Act of 1991, 11•29
- Television, piracy, 42•8–42•10
- Telnet, 5•27
- Temperature:
  - and HVAC systems, 23•16–23•17, 23•44–23•46
  - as security hazard, 3•17, 4•11–4•12, 4•22, 22•23, 53•11, 57•20
- TEMPEST (Transient ElectroMagnetic Pulse Emission Standard), 15•13, 25•5
- Temporal key integrity protocol (TKIP), 33•30–33•33, 33•36, 33•39, 33•47
- Terms of use, 11•25–11•26
- Terrorism and terrorists. *See also* September 11, 2001 attacks
  - computer crime, trends, 2•26
  - cyberterrorism, 12•3
  - information infrastructure, protecting against threats, 23•49
  - physical threats, 22•4, 22•6, 22•20, 22•22–22•23, 22•26
  - reporting activities, 61•4
  - taxonomy, 8•16
- Testimony, expert witnesses. *See* Expert witnesses
- Testing:
  - automated, 39•15–39•16
  - backup plans, 4•20
  - best practices, 38•15
  - CC Testing Labs, 51•27–51•28
  - disaster recovery plan, 59•20–59•21
  - and internal controls, 54•13
  - penetration testing. *See* Penetration testing
  - race conditions, testing for, 39•14
  - regression testing, 39•15, 39•17
  - software development, 39•5–39•6, 39•12–39•16
  - software patches, 40•11–40•13, 40•15
  - and standards, 51•8–51•9. *See also* Standards
  - test-coverage monitors, 39•14
  - test data, 47•13–47•14
  - test libraries, 47•14
  - third-party commercial product assessments, 51•7, 51•11–51•12
- Theft, 4•22, 19•6
- Theft-of-service attacks, 34•10
- Threat analysis, 3•14–3•18, 22•2, 22•9–22•15, 30•24, 51•21–51•22. *See also* Physical threats; Risk assessment
- Threats:
  - and business continuity planning, 58•4–58•6. *See also* Business continuity planning (BCP); Disaster recovery
  - classification of damage, 59•3–59•6
  - and disaster recovery, 59•1–59•2
  - list of, 59•2
  - malicious code threat model, 16•2–16•3
  - management awareness of, 63•16–63•19
  - physical threats. *See* Physical threats
  - threat occurrence rate, 62•17–62•18. *See also* Risk assessment
  - understanding of and awareness programs, 49•19
  - unified threat management (UTM), 53•2
  - Voice over Internet Protocol (VoIP), 34•9–34•11
  - wireless local area networks, 33•9–33•14
- Threats, assets, vulnerabilities model, 3•2, 3•20–3•22
- Thumb drives. *See* Flash drives
- Time, synchronous and asynchronous, 4•10–4•11
- Time bombs, 2•10–2•11
- Time sharing, 1•7
- Time stamps, 47•14
- TLS. *See* Transport Layer Security (TLS)
- Token bus, 6•17
- Token passing, 6•14
- Token ring, 6•17, 6•20–6•22, 6•24
- Token ring network, 6•14, 25•5
- Tokens:
  - and authentication principles, 28•2–28•4
  - dongles. *See* Dongles
  - hardware, 7•30, 28•14
  - one-time password generators, 28•13–28•14
  - private key, 37•23
  - smart cards. *See* Smart cards
  - soft tokens, 28•14–28•15
  - types of, 28•3–28•4, 28•13
  - and virtual private networks, 32•5
- Toolkits, 8•14, 15•20–15•21
- Topology, local area networks, 6•3–6•7
- TOR (the onion router). *See* Onion routing
- Total quality management (TQM), 38•2
- Touch cards, 23•22–23•23



## I • 50 INDEX

- Traceroute (tracert), 5•24
- Trade press, product reviews, 51•11
- Trade-Related Aspects of Intellectual Property Rights (TRIPS). *See* Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)
- Trade secrets, 11•5–11•8, 11•36–11•37, 45•3, 60•11
- Trademarks, 42•2
- Traducement, 9•18
- Training. *See also* Certification; Professional education
- antivirus technology, 41•13
  - and awareness programs, 49•4. *See also* Awareness programs
  - Computer Security Act requirements, 75•5
  - computer security incident response team, 56•14–56•15
  - versus education, 74•2–74•3
  - employees, 63•28–63•29
  - Federal Information Security Management Act requirements, 75•7
  - Getronics Security University, 74•22–74•23
  - Honeynet Project, 63•13
  - International Council of Electronic Commerce Consultants (EC-Council), 74•23–74•24
  - malicious code awareness, 16•9–16•10
  - mobile workforce, 19•18
  - security policy, 66•13–66•14
  - security response plan, 23•54–23•55
  - Security University, 74•5, 74•20–74•22
  - social engineering attacks, awareness of, 19•17
  - and Trusted Information Environment model, 75•3–75•4
- Transient security network (TSN), 33•47
- Transistors, 1•7
- Transition security network (TSN), 33•25
- Transmission Control Protocol/Internet Protocol (TCP/IP). *See* TCP/IP (Transmission Control Protocol/Internet Protocol)
- Transmission Control Protocol (TCP), 5•17–5•22. *See also* TCP/IP (Transmission Control Protocol/Internet Protocol)
- Transport Layer Security/Secure Sockets Layer (TLS/SSL). *See* Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Transport Layer Security (TLS), 5•25, 7•28–7•30, 30•11, 32•4–32•5, 33•47, 34•13. *See also* Secure Sockets Layer (SSL)
- Trapping, 4•8
- Treaties:
- intellectual property, 11•34–11•39
  - Patent Cooperation Treaty (PCT), 11•35
  - World Intellectual Property Organization Copyright Treaty, 11•14–11•15
- Trespass, 11•24–11•25
- Trinoo (Trin00), 18•13, 18•17–18•19
- TRIPS. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)
- Trojan horses. *See also* Social engineering
- antivirus programs. *See* Antivirus programs
  - attacks, 20•1–20•3, 20•29–20•30
  - Back Orifice (BO) and Back Orifice 2000 (BO2K), 2•23, 21•4, 21•10, 25•10
  - background, 19•2
  - computer crime, 2•11–2•14
  - and cyber investigation, 55•13–55•14
  - defenses, 20•31–20•33, 24•13–24•14
  - history, 2•11–2•14
  - and information warfare, 14•18
  - and malicious Web servers, 16•8
  - malware, 15•29–15•30
  - and mobile code, 17•2
  - overview, 16•6
  - and passwords, 28•6
  - and porn sites, 48•34
  - and role of CISO, 65•2
  - and screensavers, 20•30–20•31
  - and social engineering attacks, 19•9–19•10
  - system penetration, 15•13–15•14, 15•25
  - taxonomy, 8•13
- Truncated binary exponential backoff, 6•13
- Trust:
- asymmetric trust, 17•10
  - B2C security services trust levels, 30•4
  - chain of trust, 37•4–37•5
  - derivative trust, 17•10
  - domain ranges, trusted and untrusted, 21•7
  - levels of, 37•9–37•10
  - models, 37•11–37•13
  - path, 37•15
  - and PKI interoperability, 37•14–37•15
  - Pretty Good Privacy (PGP), 7•26, 37•2, 37•13, 40•12
  - proofing, 37•10–37•11
  - and public key cryptosystems, 7•25
  - and rekeying, 37•22
  - and signed code, 17•4–17•8. *See also* Mobile code
  - transitive trust, 17•10
  - trusted archival services, 37•25–37•26
  - trusted paths, 37•10–37•11
  - trusted time stamp, 37•26
  - trustworthiness and future of information assurance, 77•2–77•5
  - web of trust, 7•26, 37•5, 37•12–37•13
- TRUSTe, 30•19
- Trusted archival services, 37•25–37•26
- Trusted communication, 30•6
- Trusted Computer Systems Evaluation Criteria* (TCSEC) (*Orange Book*), 1•13–1•14, 17•9, 17•13, 25•11, 51•11, 51•14–51•15
- Trusted paths, 37•10–37•11
- Trusted systems, 24•11–24•14, 54•15
- Trusted time stamp, 37•26
- TSADBOT, 48•14
- Tunneling, 26•10–26•11, 30•36, 30•38, 31•9–31•10, 32•3–32•4, 32•10

Turkey, Internet content regulation, 72·7  
 Turnitin.org, 48·31  
 Twisted pair cable, 6·9, 6·12  
 Two-factor authentication, 25·6, 28·3, 28·8, 28·13  
 Two-phase commit, 52·5  
 Typed access control model, 9·6

**U**  
 UA control, 25·10  
 Unicode, 4·3  
 Unified Modeling Language (UML), 21·14  
 Unified Threat Management (UTM), 31·9  
 Uniform resource locator (URL), 31·4–31·5, 31·7–31·8  
 Uniform Trade Secrets Act (UTSA), 11·6–11·8  
 Uninterruptible power supply (UPS), 4·23  
 Unions, 49·12–49·13  
 Uniqueness constraints, 52·4  
 United Arab Emirates (UAE), Internet content regulation, 72·6  
 United Kingdom, 48·27, 72·2, 76·10  
 United States:  
     First Amendment rights and Internet censorship, 72·2, 72·7–72·17  
     privacy law, 69·6–69·20  
 United States Federal Chief Information Officers (CIO) Council:  
     Best Practices Committee, documentation for policy makers, 44·7–44·8  
 UNIVAC (Universal Automatic Computer), 1·5  
 Universal Plug and Play (UPnP), 26·8  
 Universal Serial Bus (USB) tokens, 4·9  
 Universities. *See* Colleges and universities  
 UNIX, 6·27, 16·5, 17·9–17·10, 17·13, 21·7, 25·8, 25·11, 25·13–25·14  
 Unmanned undersea vehicles (UUVs), 53·7  
 Unshielded twisted pair (UTP) wire, 5·3, 5·11, 6·2, 6·9, 6·18–6·19, 25·4–25·5  
 Unsolicited commercial e-mail (UCE). *See* Spam  
 Unwired generation, 50·21  
 Updates:  
     antivirus software, 26·9  
     automatic, 16·10, 17·11  
     and database management, 52·4  
     firewalls and gateway security devices, 26·21  
     importance of, 5·3  
     and preventing Trojans, 20·32  
     software patches. *See* Software patches  
 Urban myths, 48·6–48·7  
 U.S. Constitution, First Amendment rights, 48·4, 72·2, 72·7–72·17  
 U.S. Postal Inspection Service, 61·7  
 U.S. Secret Service, 61·6–61·7  
 US-CERT Cyber Security Alerts, 40·10  
 USB drives. *See* Flash drives  
 USENET, 20·7–20·8, 48·4, 48·23, 48·30  
 User Account Control (UAC), 25·11

User Datagram Protocol (UDP), 5·23, 15·21, 16·5, 30·34, 33·47, 34·8–34·9, 34·13  
 User identifiers (IDs), 28·2  
 User interface, 38·11, 39·10, 77·15–77·16  
 User name, 7·4–7·5  
 User virtual machine (UVM), 38·11, 39·10  
 Utilities:  
     diagnostic utilities, 52·11, 53·8  
     exploratory utilities, 53·9  
     log record analysis, 53·20  
     power outages and disruptions. *See* Power failures and disturbances  
 Utility as source of loss, 3·2, 3·4–3·5, 3·8–3·12  
 Utilization Review Accreditation Commission (URAC), 71·26  
 UUCP, 30·32

**V**  
 Validation, 4·6, 4·9, 47·15–47·17, 52·2, 52·9–52·11  
 Van Eck freaking (monitoring devices), 5·12, 15·13, 25·5  
 Vandalism, 22·26  
 VB-Script, 14·18, 26·16  
 Vendors:  
     accountability, 68·8, 68·20–68·21  
     contracts with, 11·4–11·5  
     gateway security devices, 26·30–26·31  
     product validation, 51·29  
     selection criteria for outsourcing, 68·19  
     self-declarations, product assessment, 51·7  
 Verification of identity, 29·5–29·6  
 VeriSign, 17·8  
 Video:  
     awareness training programs, 49·32  
     piracy, 42·842·8, 48·30. *See also* Piracy training videos, 63·28  
     videocassettes, watermarking, 42·11  
 Video Privacy Protection Act, 69·12  
 Violence:  
     physical threats, 22·26, 23·49–23·50  
     prevention and mitigation, 23·13–23·14  
     threats of, 48·36  
     video games, 48·29  
     workplace, 22·3, 22·6, 22·22  
 Virtual appliance, 26·10  
 Virtual firewalls, 26·9–26·10  
 Virtual local area networks (VLANS), 16·10–16·11, 40·17  
 Virtual Machine technology, 17·12  
 Virtual machines, 42·15  
 Virtual Private Network (VPN) Consortium, 51·8–51·9  
 Virtual private networks (VPNs):  
     background, 32·1–32·2  
     client management, 32·8  
     costs, 32·10  
     and e-commerce, 30·15  
     and encryption, 31·11

## I • 52 INDEX

Virtual private networks (VPNs) (*Continued*)  
malicious, 32•10–32•11  
and mobile access, 47•14–47•15  
network traffic inspection, 32•9  
overview, 32•2–32•3, 32•15  
processing power requirements, 32•9  
protection, 32•8–32•9  
secure client VPNs, 32•3–32•6  
trusted, 32•6–32•11  
and tunneling, 31•10  
and wireless local area network security, 1•18,  
25•7, 26•14–26•15, 33•22–33•24, 33•39

Virtual reality, 48•29

Virtualization:  
and extranets, 32•14  
monitoring and control issues, 53•25–53•26  
and monitoring and control systems, 53•12  
paravirtualization, 53•25  
virtual machine (VM), 53•25–53•26  
virtualization interface (VI), 53•25

VirtualPC, 42•15

Viruses:  
antivirus technology. *See* Antivirus programs  
boot sector, 16•4  
complexity of, 41•3  
Creeper virus, 2•14–2•15  
defined, 16•4–16•5  
e-mail content filtering, 5•27  
financial motivation, 41•1–41•2  
history, 41•4–41•5  
history of computer crime, 2•14–2•19  
hoaxes and Internet myths, 48•7–48•8  
and intrusion detection response, 27•11  
Jerusalem virus (Friday the 13th virus), 2•11,  
2•15  
and LANs, 25•10  
logic bombs. *See* Logic bombs  
MacOS, 25•14  
malware, 15•29–15•30  
Melissa virus, 1•3, 2•17–2•18, 18•4, 25•10  
naming, 41•6  
new threats (2007), 20•2  
and social engineering attacks, 19•9–19•10  
taxonomy, 8•13, 8•18  
time bombs, 2•10–2•11  
types of, 16•4–16•5  
virus creators, 12•19–12•21  
WildList, 48•13

Vishing, 19•8–19•9

Visitors, 23•22, 47•5–47•6

Visitors, controlling, 22•18, 47•6

Visual Basic for Applications (VBA), 16•4

Visual BASIC (VB), 41•4, 47•3

VMware, 42•15

Voice over Internet Protocol (VoIP):  
and application security, 5•27  
audio stream protocols, 34•8–34•9  
eavesdropping, 34•10  
encryption, 34•13–34•14

and Enhanced 911, 34•3  
infrastructure protection, 34•11–34•13  
man-in-the-middle attacks, 34•10–34•11  
overview, 34•1–34•2, 34•14  
regulatory compliance, 34•2–34•6  
risk analysis, 34•6–34•8  
signaling protocols, 34•9  
SPIT (SPam over Internet Telephony), 19•9,  
34•9  
theft of service, 34•10  
threats, 34•9–34•11  
and user datagram protocol, 5•22, 5•23  
and wiretapping, 15•10

Vulnerability:  
allowed path vulnerabilities, 21•7  
analysis, 51•21–51•22  
analysis tools, 15•20–15•21  
assessment, 46•2–46•6, 47•7  
class analysis, 15•28  
credentialed monitoring, 46•5  
and malware, 41•2  
management, 46•1–46•3  
noncredentialed monitoring, 46•5–46•6  
penetration testing. *See* Penetration testing  
reporting, 49•20  
scanning, 40•15–40•16, 40•21, 46•4, 53•2,  
53•18, 55•14  
and security incident common language,  
8•12–8•15  
and segmented secrets, 23•11–23•12  
and software patches, 40•1, 40•9. *See also*  
Software patches  
understanding of and awareness programs,  
49•29  
wired versus wireless networks, 33•10

## W

WANK worm, 30•36

War-chalking, 33•12

War dialing (demon dialing), 4•14–4•15, 15•15,  
21•12, 25•6, 46•4

War driving, 15•12, 15•19, 33•10–33•12, 33•23,  
33•36, 46•4

Water damage, 4•12, 53•11

Watermarking, 42•11–42•12

Weapons of mass destruction (WMD),  
22•22–22•23, 23•50

Weather as security threat, 22•13, 22•16–22•17

Web 2.0, 35•16, 41•11

Web application system security, 21•5–21•8

Web beacons (Web bugs), 69•15

Web browsers, 1•12, 15•17, 16•10, 17•10, 17•12

Web crawlers, 11•23

Web monitoring:  
anonymity and privacy concerns, 31•11  
block lists, 31•7–31•8  
and caching services, 31•12  
and encryption, 31•11  
filtering methods, 31•4–31•7

- firewalls, 26•15, 31•8–31•9
- implementation, 31•7–31•8
- and IP spoofing, 31•9–31•10
- and language translation sites, 31•11–31•12
- need for, 31•1–31•2
- overview, 31•13
- parental tools, 31•9, 31•12
- and pornography, 48•35
- proxy servers, 31•2, 31•8, 31•12
- reasons for, 31•2–31•4
- terminology, 31•2
- trends, 31•12
- tunneling, 31•9–31•10
- vulnerabilities, 31•9–31•12
- Web of trust, 7•26, 37•5, 37•12–37•13
- Web proxy, 16•10
- Web servers, 16•8, 21•16–21•19, 30•27–30•29
- Web sites:
  - annoy.com, 48•
  - CCCure.org, 63•28, 74•18
  - certification exams, resources for preparing, 74•17–74•19
  - customer monitoring, 30•39
  - defacement of Web pages, 15•26–15•27
  - law enforcement, 61•6
  - maintenance and updating, 30•29
  - personal, 48•5
  - privacy policies, 30•19
  - protection of and e-commerce, 30•17–30•21
  - secure coding resources, 38•13
  - security, 30•29–30•30
  - servers. *See* Web servers
  - Snopes.com, 48•6
  - system and network penetration through Web sites, 15•25–15•29
  - term paper analysis, 48•31
  - WildList, 48•13
- WebInspect, 21•16, 39•13
- Wellenreiter, 33•37–33•39
- WEPCrack, 33•20
- West Coast Labs, 51•12
- White box testing, 38•13–38•14
- Wi-Fi Protected Access (WPA), 5•3, 33•24–33•25, 33•35–33•36, 33•43, 33•47
- Wide area networks (WANs), 1•12, 5•5–5•6, 6•2, 6•10, 6•23–6•225, 32•6–32•11
- WiFi, 4•16, 15•12–15•13
- Wildfires, 22•17. *See also* Physical threats
- WildList, 41•3, 41•6, 48•13
- WiMAX Forum, 51•9
- Window field, 5•20
- Windows. *See* Microsoft Windows
- WinDump, 25•4
- Wired Equivalent Privacy (WEP), 25•7, 33•14–33•25, 33•39, 33•47
- Wired generation, 50•21
- Wireless access point (WAP), 5•3
- Wireless devices, 6•2, 6•10–6•12, 21•8, 71•11
- Wireless local area network (WLAN):
  - abbreviations, 33•44–33•47
  - architecture, 33•4–33•9
  - business use of, 33•3–33•4
  - components, 33•4–33•5
  - home use of, 33•4, 33•7
  - IEEE 802.11, original security functionality, 33•14–33•25
  - IEEE 802.11 standards, 33•40–33•43. *See also* IEEE 802 standards
  - IEEE 802.11i, 33•25–33•36
  - intrusion detection and prevention systems (WIDPS), 27•14
  - and laptops, 33•12–33•13
  - neighbors, threats from, 33•13
  - network architecture, 33•6
  - network detection, 33•14–33•15
  - network penetration techniques, 15•11–15•13
  - overview, 6•10–6•12, 33•2–33•3, 33•39–33•40
  - physical layer, 33•6–33•7
  - products, types of, 33•7–33•8
  - public (hot spots), 33•13–33•14
  - security auditing tools, 33•36–33•39
  - security issues, 4•16, 25•6–25•7
  - security threats, 33•9–33•14
  - terminology, 33•43–33•47
  - uses of, 33•3–33•4
  - war-chalking, 33•12
  - war-driving, 33•10–33•12, 33•23, 33•37
  - wireless switch/access controller architecture, 33•7–33•9
- Wireless networks, 5•13, 15•12, 15•19, 53•10–53•11, 53•24–53•25
- Wireless Personal Area Networks (WPAN), 6•17–6•18
- Wireless phones, 15•11
- Wireless Regional Area Network (WRAN), 6•18
- Wires, 22•18. *See also* Cables; Unshielded twisted pair (UTP) wire
- Wiretap Act, 11•30–11•32
- Wiretapping, 5•4, 5•12, 15•8, 15•10, 22•19–22•20, 23•48–23•49
- Witnesses, expert. *See* Expert witnesses
- Workplace violence, 22•6, 22•22
- Workstations, 22•18, 22•25
- World Intellectual Property Organization
  - Copyright Treaty, 11•14–11•15
- World Trade Organization (WTO) Agreement, 11•35–11•36
- World Wide Name (WWN) service, 36•7
- World Wide Web (WWW), history, 1•8–1•9, 1•12
- Worms:
  - Bagel worm, 16•6
  - Christmas Tree worm, 2•15, 18•2, 18•4
  - Code Red Worm, 18•21, 18•25–18•26
  - and cyber investigation, 55•13

## I • 54 INDEX

### Worms (*Continued*)

- first worm, 1•9
- and history of computer crime, 2•10,  
2•15–2•16, 2•19
- ILOVEYOU worm, 2•17
- and intrusion detection response, 27•11
- and LANs, 25•10
- MacOS, 25•14
- and malicious code, 16•5–16•6
- malware, 15•29–15•30
- Melissa virus/worm, 1•3, 2•17–2•18, 18•4,  
25•10
- Morris Worm, 2•15–2•16, 16•5, 18•2–18•4,  
30•36, 56•4, 65•2
- new threats (2007), 20•2
- Nimda worm, 16•5
- PrettyPark worm, 16•7
- SQL Slammer, 16•5–16•6, 53•12
- taxonomy, 8•18
- WANK worm, 30•36
- Warhol Worms, 16•5
- Write-once, read-many (WORM) media,  
53•18
- Write protection, 4•9–4•10

### X

- X.25 carriers, 15•10
- X.509 certificate format, 7•31–7•35, 17•4–17•5,  
30•36, 37•5–37•6, 37•8, 37•15–37•19,  
37•24
- Xerox:
  - antipiracy programs, 42•5
  - and Digital Rights Management, 42•14
  - and Ethernet standard, 6•19
  - product validation, 51•29
- XOR (Exclusive-Or), 7•15–7•16, 33•18, 33•45,  
53•19

### Y

- Yahoo!, 48•21, 72•2
- Yellow Book*, 54•15
- Yemen, Internet content regulation, 72•7

### Z

- ZBubbles, 48•13
- Zero-day attacks, 15•23
- Zero latency, 30•23
- Zigbee, 53•10–53•11
- ZoneAlarm, 48•14, 48•42