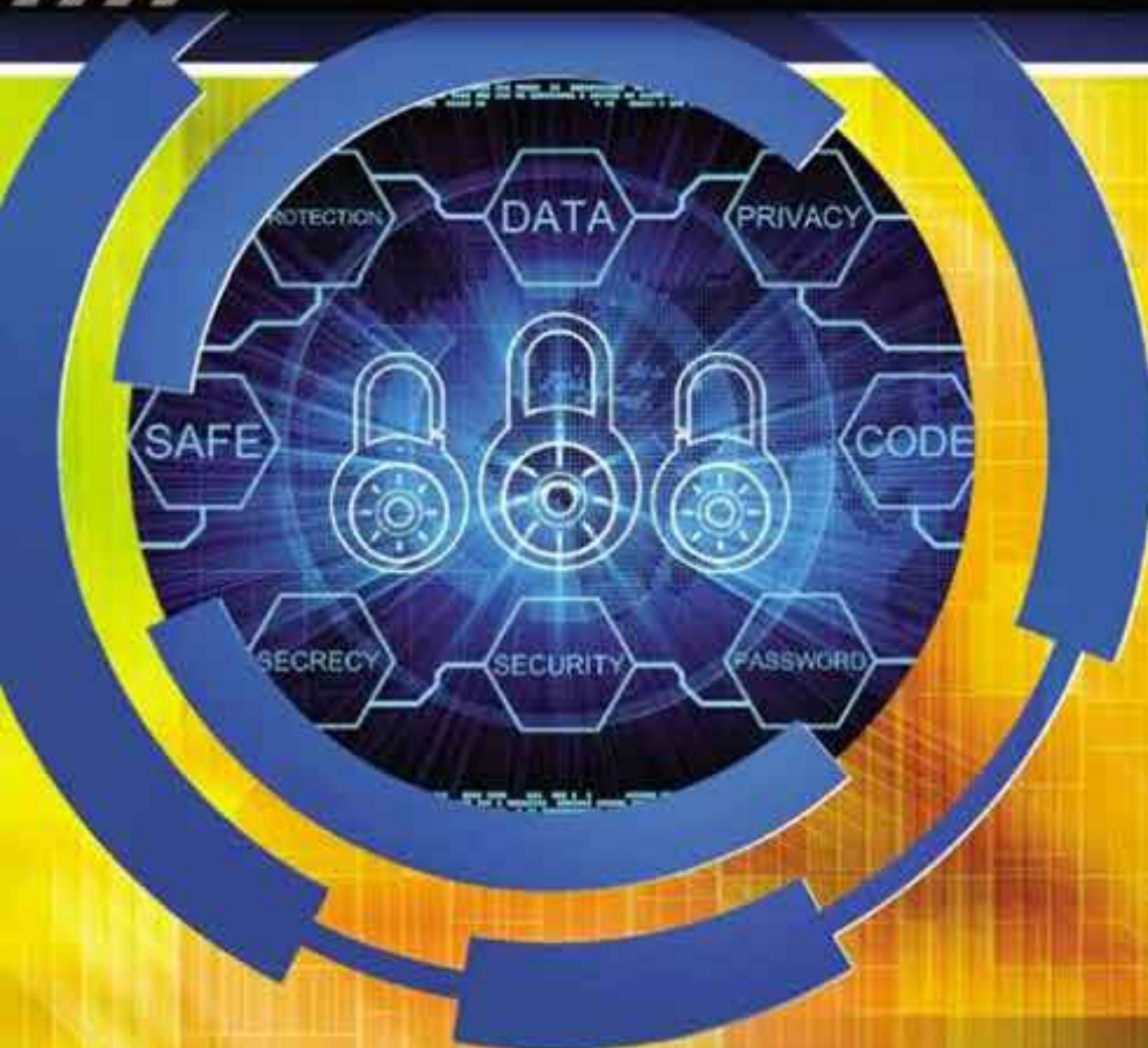


Fifth Edition

PRINCIPLES OF INFORMATION SECURITY

Michael E. Whitman and Herbert J. Mattord



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS



Principles of Information Security

Fifth Edition

Michael E. Whitman, *Ph.D., CISM, CISSP*

Herbert J. Mattord, *Ph.D., CISM, CISSP*
Kennesaw State University



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

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.

**Principles of Information Security,
Fifth Edition**

**Michael E. Whitman and
Herbert J. Mattord**

SVP, GM Skills & Global Product Management:
Dawn Gerrain

Product Development Manager: Leigh Hefferon

Senior Content Developer: Natalie Pashoukos

Development Editor: Dan Seiter

Product Assistant: Scott Finger

Vice President, Marketing Services:
Jennifer Ann Baker

Senior Marketing Manager: Eric La Scola

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/Vertigo3d

© 2016, 2012 Cengage Learning

WCN: 02-200-203

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means—graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act—without the prior written permission of the publisher.

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

Library of Congress Control Number: 2014944986

ISBN: 978-1-2854-4836-7

Cengage Learning

20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: www.cengage.com/global.

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: 2014

To Rhonda, Rachel, Alex, and Meghan, thank you for your loving support.
—MEW

To my granddaughter Ellie; the future is yours.
—HJM

Brief Table of Contents

PREFACE	xvii
CHAPTER 1 Introduction to Information Security	1
CHAPTER 2 The Need for Security	45
CHAPTER 3 Legal, Ethical, and Professional Issues in Information Security	109
CHAPTER 4 Planning for Security	153
CHAPTER 5 Risk Management	229
CHAPTER 6 Security Technology: Firewalls and VPNs	297
CHAPTER 7 Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools	355
CHAPTER 8 Cryptography	417
CHAPTER 9 Physical Security	467
CHAPTER 10 Implementing Information Security	505
CHAPTER 11 Security and Personnel	547
CHAPTER 12 Information Security Maintenance	591
GLOSSARY	657
INDEX	677

Table of Contents

PREFACE	xvii
CHAPTER 1	
Introduction to Information Security	1
Introduction.	3
The History of Information Security	3
The 1960s	4
The 1970s and 80s	5
The 1990s	9
2000 to Present	9
What Is Security?	10
Key Information Security Concepts	11
Critical Characteristics of Information	14
CNSS Security Model	17
Components of an Information System.	19
Software	19
Hardware	20
Data	20
People	20
Procedures	21
Networks	21
Balancing Information Security and Access	21
Approaches to Information Security Implementation	22
Security in the Systems Life Cycle	23
The Systems Development Life Cycle	24
The Security Systems Development Life Cycle	27
Software Assurance—Security in the SDLC	28
Software Design Principles	30
The NIST Approach to Securing the SDLC	31
Security Professionals and the Organization	34
Senior Management	35
Information Security Project Team	36
Data Responsibilities	37
Communities of Interest	37
Information Security Management and Professionals	37
Information Technology Management and Professionals	38
Organizational Management and Professionals	38
Information Security: Is It an Art or a Science?	38
Security as Art	38
Security as Science	39
Security as a Social Science	39
Selected Readings	39
Chapter Summary	40
Review Questions	40
Exercises	41
Case Exercises	42
Endnotes	42

CHAPTER 2

The Need for Security	45
Introduction.	47
Business Needs First	47
Threats and Attacks	49
2.5 Billion Potential Hackers	49
Other Studies of Threats	50
Common Attack Pattern Enumeration and Classification (CAPEC)	52
The 12 Categories of Threats	52
Compromises to Intellectual Property.	52
Software Piracy	53
Copyright Protection and User Registration	53
Deviations in Quality of Service.	56
Internet Service Issues	56
Communications and Other Service Provider Issues	57
Power Irregularities	57
Espionage or Trespass	58
Hackers	59
Hacker Variants	64
Password Attacks	66
Forces of Nature	68
Fire	69
Floods	69
Earthquakes	69
Lightning	69
Landslides or Mudslides	69
Tornados or Severe Windstorms	69
Hurricanes, Typhoons, and Tropical Depressions	70
Tsunamis	70
Electrostatic Discharge	70
Dust Contamination	70
Human Error or Failure	71
Social Engineering	72
Information Extortion.	76
Sabotage or Vandalism	77
Online Activism	78
Software Attacks	80
Malware	80
Back Doors	87
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks	88
E-mail Attacks	89
Communications Interception Attacks	90
Technical Hardware Failures or Errors	92
The Intel Pentium CPU Failure	92
Mean Time Between Failure	93
Technical Software Failures or Errors	93
The OWASP Top 10	93
The Deadly Sins in Software Security	94
Technological Obsolescence	99
Theft.	101
Selected Readings.	101

Chapter Summary 101
 Review Questions. 102
 Exercises 104
 Case Exercises 104
 Endnotes 105

CHAPTER 3

Legal, Ethical, and Professional Issues in Information Security 109
 Introduction. 110
 Law and Ethics in Information Security 110
 Organizational Liability and the Need for Counsel 111
 Policy Versus Law 112
 Types of Law. 112
 Relevant U.S. Laws 113
 General Computer Crime Laws 113
 Export and Espionage Laws 122
 U.S. Copyright Law 124
 Financial Reporting 124
 Freedom of Information Act of 1966 124
 Payment Card Industry Data Security Standards (PCI DSS) 124
 State and Local Regulations 126
 International Laws and Legal Bodies 127
 U.K. Computer Security Laws 127
 Australian Computer Security Laws 127
 Council of Europe Convention on Cybercrime 128
 World Trade Organization and the Agreement on Trade-Related Aspects of Intellectual Property Rights . . 128
 Digital Millennium Copyright Act 129
 Ethics and Information Security. 129
 Ethical Differences Across Cultures 129
 Ethics and Education 135
 Deterring Unethical and Illegal Behavior 136
 Codes of Ethics at Professional Organizations. 137
 Major Information Security Professional Organizations 138
 Key U.S. Federal Agencies. 139
 Department of Homeland Security 139
 U.S. Secret Service 142
 Federal Bureau of Investigation (FBI) 142
 National Security Agency (NSA) 145
 Selected Readings. 146
 Chapter Summary 147
 Review Questions. 147
 Exercises 148
 Case Exercises 149
 Endnotes 149

CHAPTER 4

Planning for Security 153
 Introduction. 154
 Information Security Planning and Governance. 154

Planning Levels	155
Planning and the CISO	155
Information Security Governance	156
Information Security Governance Outcomes	157
Information Security Policy, Standards, and Practices	158
Policy as the Foundation for Planning	158
Enterprise Information Security Policy	163
Issue-Specific Security Policy	164
Systems-Specific Security Policy (SysSP)	167
Policy Management	172
The Information Security Blueprint	174
The ISO 27000 Series	175
NIST Security Models	179
Other Sources of Security Frameworks	185
Design of Security Architecture	185
Security Education, Training, and Awareness Program	189
Security Education	189
Security Training	190
Security Awareness	190
Continuity Strategies	191
The CP Policy	196
Business Impact Analysis	197
Incident Response Planning	200
Disaster Recovery Planning	214
Business Continuity Planning	215
Crisis Management	218
The Consolidated Contingency Plan	219
Law Enforcement Involvement	220
Selected Readings	221
Chapter Summary	221
Review Questions	222
Exercises	223
Case Exercises	224
Endnotes	225

CHAPTER 5

Risk Management	229
Introduction	230
An Overview of Risk Management	231
Know Yourself	232
Know the Enemy	233
The Roles of the Communities of Interest	233
Risk Appetite and Residual Risk	234
Risk Identification	236
Planning and Organizing the Process	236
Identifying, Inventorying, and Categorizing Assets	237
Classifying, Valuing, and Prioritizing Information Assets	241
Identifying and Prioritizing Threats	249
Specifying Asset Vulnerabilities	251
Risk Assessment	257
Planning and Organizing Risk Assessment	257

Determining the Loss Frequency 258
 Evaluating Loss Magnitude 260
 Calculating Risk 261
 Assessing Risk Acceptability 261
 The FAIR Approach to Risk Assessment 263
Risk Control 267
 Selecting Control Strategies 267
 Justifying Controls 272
 Implementation, Monitoring, and Assessment of Risk Controls 277
Quantitative Versus Qualitative Risk Management Practices 278
 Benchmarking and Best Practices 278
Recommended Risk Control Practices 285
 Documenting Results 286
 The NIST Risk Management Framework 287
Selected Readings 289
Chapter Summary 290
Review Questions 290
Exercises 291
Case Exercises 293
Endnotes 294

CHAPTER 6

Security Technology: Firewalls and VPNs 297
 Introduction 298
 Access Control 298
 Access Control Mechanisms 301
 Biometrics 305
 Access Control Architecture Models 308
 Firewalls 315
 Firewall Processing Modes 316
 Firewall Architectures 326
 Selecting the Right Firewall 331
 Configuring and Managing Firewalls 332
 Content Filters 341
 Protecting Remote Connections 342
 Remote Access 342
 Virtual Private Networks (VPNs) 346
 Selected Readings 349
 Chapter Summary 350
 Review Questions 351
 Exercises 352
 Case Exercises 352
 Endnotes 353

CHAPTER 7

Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools 355
 Introduction 357
 Intrusion Detection and Prevention Systems 357

IDPS Terminology	358
Why Use an IDPS?	360
Types of IDPSs	362
IDPS Detection Methods	371
IDPS Response Behavior	373
Selecting IDPS Approaches and Products	376
Strengths and Limitations of IDPSs	381
Deployment and Implementation of an IDPS	382
Measuring the Effectiveness of IDPSs	389
Honeybots, Honeynets, and Padded Cell Systems	391
Trap-and-Trace Systems	393
Active Intrusion Prevention	395
Scanning and Analysis Tools	395
Port Scanners	399
Firewall Analysis Tools	400
Operating System Detection Tools	401
Vulnerability Scanners	401
Packet Sniffers	407
Wireless Security Tools	408
Selected Readings	410
Chapter Summary	410
Review Questions	411
Exercises	412
Case Exercises	412
Endnotes	413
CHAPTER 8	
Cryptography	417
Introduction	418
Foundations of Cryptology	419
Terminology	422
Cipher Methods	422
Substitution Cipher	423
Transposition Cipher	426
Exclusive OR	428
Vernam Cipher	429
Book-Based Ciphers	431
Hash Functions	432
Cryptographic Algorithms	434
Symmetric Encryption	435
Asymmetric Encryption	437
Encryption Key Size	440
Cryptographic Tools	442
Public Key Infrastructure (PKI)	442
Digital Signatures	444
Digital Certificates	446
Hybrid Cryptography Systems	448
Steganography	450
Protocols for Secure Communications	451
Securing Internet Communication with S-HTTP and SSL	451
Securing E-mail with S/MIME, PEM, and PGP	453
Securing Web Transactions with SET, SSL, and S-HTTP	454

Securing Wireless Networks with WEP and WPA 455
 Securing TCP/IP with IPsec and PGP 457
Selected Readings 461
Chapter Summary 461
Review Questions 462
Exercises 463
Case Exercises 463
Endnotes 464

CHAPTER 9

Physical Security **467**
 Introduction 469
 Physical Access Controls 470
 Physical Security Controls 470
 Fire Security and Safety 479
 Fire Detection and Response 480
 Failure of Supporting Utilities and Structural Collapse 487
 Heating, Ventilation, and Air Conditioning 487
 Power Management and Conditioning 489
 Water Problems 493
 Structural Collapse 493
 Maintenance of Facility Systems 493
 Interception of Data 493
 Securing Mobile and Portable Systems 495
 Remote Computing Security 497
 Special Considerations for Physical Security 498
 Selected Readings 499
 Chapter Summary 499
 Review Questions 500
 Exercises 501
 Case Exercises 502
 Endnotes 503

CHAPTER 10

Implementing Information Security **505**
 Introduction 507
 Information Security Project Management 508
 Developing the Project Plan 508
 Project Planning Considerations 512
 The Need for Project Management 515
 Security Project Management Certifications 517
 Technical Aspects of Implementation 518
 Conversion Strategies 518
 The Bull’s-Eye Model 520
 To Outsource or Not 522
 Technology Governance and Change Control 522
 The SANS Top 20 Critical Security Controls 523

Nontechnical Aspects of Implementation	525
The Culture of Change Management	525
Considerations for Organizational Change	526
Information Systems Security Certification and Accreditation	527
Certification Versus Accreditation	527
The NIST Security Life Cycle Approach	527
NSTISS Certification and Accreditation	532
ISO 27001/27002 Systems Certification and Accreditation	539
Selected Readings	541
Chapter Summary	541
Review Questions	543
Exercises	544
Case Exercises	544
Endnotes	546
CHAPTER 11	
Security and Personnel	547
Introduction	548
Positioning and Staffing the Security Function	549
Staffing the Information Security Function	550
Credentials for Information Security Professionals	562
(ISC) ² Certifications	562
ISACA Certifications	565
SANS Certifications	567
EC Council Certifications	568
CompTIA Certifications	569
ISFCE Certifications	570
Certification Costs	571
Advice for Information Security Professionals	572
Employment Policies and Practices	573
Job Descriptions	573
Interviews	575
Background Checks	575
Employment Contracts	576
New Hire Orientation	576
On-the-Job Security Training	577
Evaluating Performance	577
Termination	577
Security Considerations for Temporary Employees, Consultants, and Other Workers	580
Temporary Employees	580
Contract Employees	580
Consultants	581
Business Partners	581
Internal Control Strategies	582
Privacy and the Security of Personnel Data	584
Selected Readings	584
Chapter Summary	584
Review Questions	586
Exercises	587

Case Exercises 588

Endnotes 588

CHAPTER 12

Information Security Maintenance 591

Introduction. 592

Security Management Maintenance Models 593

 NIST SP 800-100, Information Security Handbook: A Guide for Managers 593

 The Security Maintenance Model. 614

Digital Forensics. 641

 The Digital Forensics Team. 642

 Affidavits and Search Warrants 643

 Digital Forensics Methodology 643

 Evidentiary Procedures 649

Selected Readings. 650

Chapter Summary 650

Review Questions. 651

Exercises 652

Case Exercises 653

Endnotes 654

GLOSSARY **657**

INDEX **677**



As global networks expand the interconnection of the world's information systems, the smooth operation of communication and computing solutions becomes vital. However, recurring events such as malware and phishing attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems.

When attempting to secure their existing systems and networks, organizations must draw on the current pool of information security practitioners. But, to develop more secure computing environments in the future, these same organizations are counting on the next generation of professionals to have the correct mix of skills and experience to anticipate and manage the complex information security issues that are sure to arise. Thus, improved texts with supporting materials, along with the efforts of college and university faculty, are needed to prepare students of technology to recognize the threats and vulnerabilities in existing systems and to learn to design and develop the secure systems needed in the near future.

The purpose of *Principles of Information Security*, Fifth Edition, is to continue to meet the need for a current, high-quality academic textbook that surveys the discipline of information security. While dozens of good publications on information security are oriented to the practitioner, there remains a severe lack of textbooks that provide students with a balanced introduction to both security management and the technical components of information security. By creating a book specifically from the perspective of information security, we hope to close this gap. Further, there is a clear need to include principles from criminal justice, political science, computer science, information systems, and other related disciplines to

gain a clear understanding of information security principles and formulate interdisciplinary solutions for systems vulnerabilities. The essential tenet of this textbook is that information security in the modern organization is a problem for management to solve, and not one that technology alone can address. In other words, an organization's information security has important economic consequences for which management will be held accountable.

Approach

Principles of Information Security, Fifth Edition, provides a broad review of the entire field of information security, background on many related elements, and enough detail to facilitate an understanding of the topic as a whole. The book covers the terminology of the field, the history of the discipline, and strategies for managing an information security program.

Structure and Chapter Descriptions

Principles of Information Security, Fifth Edition, is structured to follow a model called the security systems development life cycle (or SecSDLC). This structured methodology can be used to implement information security in an organization that has little or no formal information security in place. The SecSDLC can also serve as a method for improving established information security programs. The SecSDLC provides a solid framework very similar to that used in application development, software engineering, traditional systems analysis and design, and networking. This textbook's use of a structured methodology is intended to provide a supportive but not overly dominant foundation that will guide instructors and students through the information domains of information security. To serve this end, the book is organized into six sections and 12 chapters.

› Section I—Introduction

Chapter 1—Introduction to Information Security The opening chapter establishes the foundation for understanding the broader field of information security. This is accomplished by defining key terms, explaining essential concepts, and reviewing the origins of the field and its impact on the understanding of information security.

› Section II—Security Investigation Phase

Chapter 2—The Need for Security Chapter 2 examines the business drivers behind the design process of information security analysis. It examines current organizational and technological security needs while emphasizing and building on the concepts presented in Chapter 1. One principal concept presented here is that information security is primarily a management issue rather than a technological one. To put it another way, the best practices within the field of information security involve applying technology only after considering the business needs.

The chapter also examines the various threats facing organizations and presents methods for ranking and prioritizing these threats as organizations begin their security planning process. The chapter continues with a detailed examination of the types of attacks that could result from these threats and how these attacks could affect the organization's information systems.

The chapter also provides further discussion of the key principles of information security,

some of which were introduced in Chapter 1: confidentiality, integrity, availability, authentication and identification, authorization, accountability, and privacy.

Chapter 3—Legal, Ethical, and Professional Issues in Information Security

In addition to being a fundamental part of the SecSDLC investigation process, a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities provides important insights into the regulatory constraints that govern business. This chapter examines several key laws that shape the field of information security and examines the computer ethics to which those who implement security must adhere. Although ignorance of the law is no excuse, it's considered better than negligence (that is, knowing the law but doing nothing to comply with it). This chapter also presents several common legal and ethical issues found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

› Section III—Security Analysis

Chapter 4—Planning for Security This chapter presents a number of widely accepted security models and frameworks. It examines best business practices and standards of due care and due diligence, and offers an overview of the development of security policy. This chapter details the major components, scope, and target audience for each level of security policy. It also explains data classification schemes, both military and private, as well as the security education training and awareness (SETA) program. The chapter examines the planning process that supports business continuity, disaster recovery, and incident response; it also describes the organization's role during incidents and specifies when the organization should involve outside law enforcement agencies.

Chapter 5—Risk Management Before the design of a new information security solution can begin, information security analysts must first understand the current state of the organization and its relationship to information security. Does the organization have any formal information security mechanisms in place? How effective are they? What policies and procedures have been published and distributed to security managers and end users? This chapter describes how to conduct a fundamental information security assessment by describing procedures for identifying and prioritizing threats and assets as well as procedures for identifying what controls are in place to protect these assets from threats. The chapter also discusses the various types of control mechanisms and identifies the steps involved in performing the initial risk assessment. It continues by defining risk management as the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. The chapter concludes with a discussion of risk analysis and various types of feasibility analyses.

› Section IV—Design

The material in this section is sequenced to introduce students of information systems to the information security aspects of various technology topics. If you are not familiar with networking technology and TCP/IP, the material in Chapters 6, 7, 8, and 9 may prove difficult. Students who do not have a grounding in network protocols should prepare for their study of the chapters in this section by reading a chapter or two from a networking textbook on TCP/IP.

Chapter 6—Security Technology: Firewalls and VPNs Chapter 6 provides a detailed overview of the configuration and use of technologies designed to segregate the organization's systems from the insecure Internet. This chapter examines the various definitions and categorizations of firewall technologies and the architectures under which firewalls may be deployed. The chapter discusses the rules and guidelines associated with the proper configuration and use of firewalls. It also discusses remote dial-up services and the security precautions necessary to secure access points for organizations still deploying this older technology. The chapter continues by presenting content-filtering capabilities and considerations, and concludes by examining technologies designed to provide remote access to authorized users through virtual private networks.

Chapter 7—Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools Chapter 7 continues the discussion of security technologies by examining the concept of intrusion and the technologies necessary to prevent, detect, react to, and recover from intrusions. Specific types of intrusion detection and prevention systems (IDPSs)—the host IDPS, network IDPS, and application IDPS—and their respective configurations and uses are presented and discussed. The chapter examines specialized detection technologies that are designed to entice attackers into decoy systems (and thus away from critical systems) or simply to identify the attackers' entry into these decoy areas. Such systems are known as honeypots, honeynets, and padded cell systems. The discussion also examines trace-back systems, which are designed to track down the true addresses of attackers who were lured into decoy systems. The chapter then examines key security tools that information security professionals can use to examine the current state of their organization's systems and identify potential vulnerabilities or weaknesses in the organization's overall security posture. The chapter concludes with a discussion of access control devices commonly deployed by modern operating systems and new technologies in the area of biometrics that can provide strong authentication to existing implementations.

Chapter 8—Cryptography Chapter 8 continues the section on security technologies by describing the underlying foundations of modern cryptosystems as well as their architectures and implementations. The chapter begins by summarizing the history of modern cryptography and discussing the various types of ciphers that played key roles in that history. The chapter also examines some of the mathematical techniques that comprise cryptosystems, including hash functions. The chapter then extends this discussion by comparing traditional symmetric encryption systems with more modern asymmetric encryption systems and examining the role of asymmetric systems as the foundation of public-key encryption systems. Also covered are the cryptography-based protocols used in secure communications, including S-HTTP, S/MIME, SET, and SSH. The chapter then discusses steganography and its emerging role as an effective means of hiding information. The chapter concludes by revisiting attacks on information security that are specifically targeted at cryptosystems.

Chapter 9—Physical Security A vital part of any information security process, physical security includes the management of physical facilities, the implementation of physical access control, and the oversight of environmental controls. Physical security involves a wide range of special considerations that encompass designing a secure data center, assessing the relative value of guards and watchdogs, and resolving technical issues in fire suppression

and power conditioning. Chapter 9 examines these considerations by factoring in the physical security threats that modern organizations face.

› Section V—Implementation

Chapter 10—Implementing Information Security The preceding chapters provide guidelines for how an organization might design its information security program. Chapter 10 examines the elements critical to *implementing* this design. Key areas in this chapter include the bull’s-eye model for implementing information security and a discussion of whether an organization should outsource components of its information security program. The chapter also discusses change management, program improvement, and additional planning for business continuity efforts.

Chapter 11—Security and Personnel The next area in the implementation stage addresses personnel issues. Chapter 11 examines both sides of the personnel coin: security personnel and security of personnel. It examines staffing issues, professional security credentials, and the implementation of employment policies and practices. The chapter also discusses how information security policy affects and is affected by consultants, temporary workers, and outside business partners.

› Section VI—Maintenance and Change

Chapter 12—Information Security Maintenance Last and most important is the discussion of maintenance and change. Chapter 12 describes the ongoing technical and administrative evaluation of the information security program that an organization must perform to maintain the security of its information systems. This chapter explores ongoing risk analysis, risk evaluation, and measurement, all of which are part of risk management. It also explores special considerations needed for the varieties of vulnerability analysis in modern organizations, from Internet penetration testing to wireless network risk assessment. The chapter and the book conclude by covering the subject of digital forensics.

Features

Here are some features of the book’s approach to information security:

Information Security Professionals’ Common Bodies of Knowledge—Because the authors hold both the Certified Information Security Manager (CISM) and Certified Information Systems Security Professional (CISSP) credentials, those knowledge domains have had an influence in the design of the text. Although care was taken to avoid producing a certification study guide, the authors’ backgrounds ensure that the book’s treatment of information security integrates the CISM and CISSP Common Bodies of Knowledge (CBKs).

Chapter Scenarios—Each chapter opens and closes with a short story that features the same fictional company as it encounters information security issues commonly found in real-life organizations. At the end of each chapter, a set of discussion questions provides students and instructors with opportunities to discuss the issues suggested by the story and explore the ethical dimensions of those issues.

Offline and Technical Details Boxes—Interspersed throughout the textbook, these sections highlight interesting topics and detailed technical issues, giving students the option of delving into information security topics more deeply.

Hands-On Learning—At the end of each chapter, students will find a chapter summary and review questions as well as exercises. In the exercises, students are asked to research, analyze, and write responses to reinforce learning objectives, deepen their understanding of the text, and examine the information security arena outside the classroom.

New to This Edition

- Additional discussion questions at the end of each chapter to explore ethical dimensions of the content
- Coverage of the newest laws and industry trends
- Key Terms boxes that provide increased visibility for terminology used in the industry
- “For More Information” features that provide Web locations where students can find additional information about the subject covered
- Additional figures to illustrate important topics

Additional Resources

To access additional course materials, please visit www.cengagebrain.com. Note the ISBN on the back cover of your book, and then search for the book’s ISBN using the search box at the top of the CengageBrain home page.

Instructor Resources

› Instructor Companion Site

A variety of teaching tools have been prepared to support this textbook and enhance classroom learning:

Instructor’s Manual—The Instructor’s Manual includes suggestions and strategies for using this text, and even suggestions for lecture topics. It also includes answers to the review questions and suggested solutions to the exercises at the end of each chapter.

Solutions—The instructor resources include solutions to all end-of-chapter material, including review questions and exercises.

Figure Files—Figure files allow instructors to create their own presentations using figures taken from the text.

PowerPoint Presentations—This book comes with Microsoft PowerPoint slides for each chapter. These slides are included as a teaching aid to be used for classroom presentation, to be made available to students on the network for chapter review, or to be printed for classroom

distribution. Instructors can add their own slides for additional topics they introduce to the class.

Lab Manual—Cengage Learning has developed a lab manual to accompany this and other books: *The Hands-On Information Security Lab Manual*, Fourth Edition (ISBN-13: 9781285167572). The lab manual provides hands-on security exercises on footprinting, enumeration, and firewall configuration, as well as detailed exercises and cases that can supplement the book as laboratory components or in-class projects. Contact your Cengage Learning sales representative for more information.

Cognero—Cengage Learning Testing Powered by Cognero is a flexible, online system that allows you to:

- Author, edit, and manage test bank content from multiple Cengage Learning solutions
- Create multiple test versions in an instant
- Deliver tests from your LMS, your classroom, or anywhere you want

Author Team

Michael Whitman and Herbert Mattord have jointly developed this text 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, Michael J. Coles College of Business at Kennesaw State University, Kennesaw, Georgia, where he is also the Director of the KSU Center for Information Security Education (infosec.kennesaw.edu). Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, Ethical Computing, and Curriculum Development Methodologies. He currently teaches graduate and undergraduate courses in Information Security and Contingency Planning. He has published articles in the top journals in his field, including *Information Systems Research*, *Communications of the ACM*, *Information and Management*, *Journal of International Business Studies*, and *Journal of Computer Information Systems*. Dr. Whitman is also the Editor-in-Chief of the *Information Security Education Journal*. He is a member of the Information Systems Security Association, the Association for Computing Machinery, and the Association for Information Systems. Dr. Whitman is also the co-author of *Management of Information Security*, *Principles of Incident Response and Disaster Recovery*, *Readings and Cases in the Management of Information Security*, *The Guide to Firewalls and VPNs*, *The Guide to Network Security*, and *The Hands-On Information Security Lab Manual*, among others, all published by Cengage Learning. Prior to his career in academia, Dr. Whitman was an Armored Cavalry 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 before joining the faculty of Kennesaw State University in 2002. Professor Mattord is the Coordinator of the Bachelor of Business Administration in Information Security and Assurance degree and the Associate Director of the KSU Center for Information Security Education and Awareness (infosec.kennesaw.edu). He is also an Associate Editor of the *Information Security Education Journal*. During his career as an IT practitioner, he 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, Data Communications, Local Area Networks, Database Technology, Project Management, Systems Analysis and Design, and Information Resources Management and Policy. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this textbook was acquired. Professor Mattord is also the co-author of *Management of Information Security*, *Principles of Incident Response and Disaster Recovery*, *Readings and Cases in the Management of Information Security*, *The Guide to Firewalls and VPNs*, *The Guide to Network Security*, and *The Hands-On Information Security Lab Manual*, among others, all published by Cengage Learning.

Acknowledgments

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

› Contributors

Several people and organizations also provided materials for this textbook, and we thank them for their contributions. For example, the National Institute of Standards and Technology (NIST) is the source of many references, tables, figures, and other content used throughout the textbook.

› Reviewers

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

- Paul Witman, California Lutheran University
- Pam Schmelz, Ivy Tech Community College of Indiana
- Donald McCracken, ECPI University, Virginia
- Michelle Ramim, Nova Southeastern University, Florida

› 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, Development Editor
- Nick Lombardi, Product Manager
- Brooke Baker, Senior Content Project Manager

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

- Charles Cresson Wood
- Donn Parker
- Our colleagues in the Department of Information Systems and the Coles College of Business at Kennesaw State University

› Our Commitment

The authors are committed to serving the needs of adopters and readers of this book. We would be pleased and honored to receive feedback on the textbook and its supporting materials. You can contact us through Cengage Learning via e-mail at mis@course.com.

Foreword

Information security is an art more than a science, and the mastery of protecting information requires multidisciplinary knowledge of a huge quantity of information plus experience and skill. You will find much of what you need here in this book as the authors take you through the security systems development life cycle using real-life scenarios to introduce each topic. The authors provide their perspective from many years of real-life experience, combined with their academic approach for a rich learning experience expertly presented in this book. You have chosen the authors and the book well.

Since you are reading this book, you are most likely working toward a career in information security or at least have serious interest in information security. You must anticipate that just about everybody hates the constraints that security puts on their work. This includes both the good guys and the bad guys—except for malicious hackers who love the security we install as a challenge to be beaten. We concentrate on stopping the intentional wrongdoers because it applies to stopping the accidental ones as well. Security to protect against accidental wrongdoers is not good enough against those with intent.

I have spent 40 years of my life in a field that I found to be exciting and rewarding, working with computers and pitting my wits against malicious people, and you will too. Security controls and practices include logging on and off, using passwords, encrypting and backing up vital information, locking doors and drawers, motivating stakeholders to support security, and installing antivirus software. These means of protection have no benefit except rarely, when adversities occur. Good security is in effect when nothing bad happens, and when nothing bad happens, who needs security? Nowadays, in addition to loss experience, we need it because the law, regulations, and auditors say so—especially if we deal with the personal information of others, electronic money, intellectual property, and keeping ahead of the competition.

There is great satisfaction in knowing that your employer's information and systems are reasonably secure and that you are paid a good salary, are the center of attention in emergencies, and are applying your wits against the bad guys. This makes up for the downside of your security work. It is no job for perfectionists because you will almost never be fully successful,

and there will always be vulnerabilities that you aren't aware of or that the bad guys discover first. Our enemies have a great advantage over us. They have to find only one vulnerability and one target to attack in a known place, electronically or physically at a time of their choosing, while we must defend from potentially millions of attacks against assets and vulnerabilities that are no longer in one computer room but are spread all over the world. It's like playing a game in which you don't know your opponents and where they are, what they are doing, or why they are doing it, and they are secretly changing the rules as they play. You must be highly ethical, defensive, secretive, and cautious. Bragging about the great security you are employing might tip off the enemy. Enjoy the few successes that you experience, for you will not even know about some of them.

There is a story that describes the kind of war you are entering into. A small country inducted a young man into its ill-equipped army. The army had no guns, so it issued a broom to the new recruit for training purposes. In basic training, the young man asked, "What do I do with this broom?"

The instructor took him to the rifle range and told him to pretend the broom is a gun, aim it at the target, and say, "Bang, bang, bang." He did that. Then the instructor took him to bayonet practice, and the recruit said, "What do I do with this broom?"

The instructor said, "Pretend it is a gun with a bayonet and say, 'Stab, stab, stab.'"

The recruit did that as well. Then the war started and the army still didn't have guns; the young man found himself on the front line with enemy soldiers running toward him across a field. All he had was his trusty broom. So he could only do what he was trained to do. He aimed the broom at the enemy soldiers and said, "Bang, bang, bang." Some of the enemy soldiers fell down, but many kept coming. Some got so close that he had to say, "Stab, stab, stab," and more enemy soldiers fell down. However, there was one stubborn enemy soldier (there always is in these stories) running toward him. The recruit said, "Bang, bang, bang," but to no effect. The enemy continued to get closer and the recruit said, "Stab, stab, stab," but it still had no effect. In fact, the enemy soldier ran right over the recruit, broke his broom in half, and left him lying in the dirt. As the enemy soldier ran by, the recruit heard him muttering under his breath, "Tank, tank, tank."

I tell this story at the end of my many lectures on computer crime and security to impress on my audience that if you are going to win against crime, you must know the rules, and it is the criminal who is making up his secret rules as he goes along. This makes winning very difficult.

When I was lecturing in Rio de Janeiro, a young lady performed simultaneous translation into Portuguese for my audience of several hundred people, all with earphones clapped over their ears. In such situations, I have no idea what my audience is hearing, and after telling my joke nobody laughed. They just sat there with puzzled looks on their faces. After the lecture, I asked the translator what had happened. She had translated "tank, tank, tank" into "water tank, water tank, water tank." The recruit and I were both deceived that time.

Three weeks later, I was lecturing to an audience of French bankers at the George V Hotel in Paris. I had a bilingual friend listen to the translation of my talk. The same thing happened as in Rio. Nobody laughed. Afterward, I asked my friend what had happened. He said, "You will never believe this, but the translator translated 'tank, tank, tank' into 'merci, merci, merci' (thanks)." Even in telling the joke, like the recruit, I didn't know the rules to the game.

Remember that when working in security, you are in a virtual army defending your employer and stakeholders from their enemies. From your point of view the enemies will probably think and act irrationally, but from their perspective they are perfectly rational, with serious personal problems to solve and gains to be made by violating your security. You are no longer just a techie with the challenging job of installing technological controls in systems and networks. Most of your work should be in assisting potential victims to protect themselves from information adversities and dealing with your smart but often irrational enemies, even though you rarely see or even identify them. I spent a major part of my security career hunting down computer criminals and interviewing them and their victims, trying to obtain insights to do a better job of defending from their attacks. Likewise, you should use every opportunity to seek them out and get to know them. This experience gives you great cachet as a real and unique expert, even with minimal exposure to only a few enemies.

Comprehensiveness is an important part of the game you play for real stakes because the enemy will likely seek the easiest way to attack vulnerabilities and assets that you haven't fully protected yet or even know exist. For example, a threat that is rarely found on threat lists is endangerment of assets—putting information assets in harm's way. Endangerment is also one of the most common violations by security professionals; it occurs when they reveal too much about their security and loss experience.

You must be thorough and meticulous and document everything pertinent, in case your competence is questioned and to meet the requirements of the Sarbanes–Oxley Law. Keep your documents safely locked away. Documentation is important so that when adversity hits and you lose the game, you will have proof of being diligent in spite of the loss. Otherwise, your career could be damaged, or at least your effectiveness will be diminished. For example, if the loss occurred because management failed to give you an adequate budget and support for security you knew you required, you need to have documented that failure before the incident occurred. Don't brag about how great your security is, because it can always be beaten. Keep and expand checklists for everything: threats, vulnerabilities, assets, key potential victims, suspects of wrongdoing, security supporters and nonsupporters, attacks, enemies, criminal justice resources, auditors, regulators, and legal counsel. To assist your stakeholders, who are the front-line defenders of their information and systems, identify what they must protect and know the real extent of their security. Make sure that upper management and other people to whom you report understand the nature of your job and its limitations.

Use the best possible security practices yourself to set a good example. You will have a huge collection of sensitive passwords to do your job. Write them down, and keep the list safely in your wallet next to your credit card. Know as much as possible about the systems and networks in your organization and have access to experts who know the rest. Make good friends of local and national criminal justice officials, your organization's lawyers, insurance risk managers, human resources people, facilities managers, and auditors. Audits are one of the most powerful controls your organization has. Remember that people hate security and must be properly motivated by penalties and rewards to make it work. Seek ways to make security invisible or transparent to stakeholders while keeping it effective. Don't recommend or install controls or practices that stakeholders won't support, because they will beat you every time by making it look like the controls are effective when they are not—a situation worse than no security at all.

One of the most exciting parts of the job is the insight you gain about the inner workings and secrets of your organization, its business, and its culture. As an information security consultant, I was privileged to learn about the culture and secrets of more than 250 of the largest corporations throughout the world. I had the opportunity to interview and advise the most powerful business executives, if only for a few minutes of their valuable time. You should always be ready with a “silver bullet” to use in your short time with top management for the greatest benefit of enterprise security. Carefully learn the limits of management’s security appetites. Know the nature of the business, whether it is a government department or a hotly competitive company. I once found myself in a meeting with a board of directors intensely discussing the protection of their greatest trade secret, the manufacturing process of their new disposable diapers.

Finally, we come to the last important bit of advice. Be trustworthy and develop mutual trust among your peers. Your most important objectives are not just risk reduction and increased security. They also include diligence to avoid negligence and endangerment, compliance with all laws and standards, and enablement when security becomes a competitive or budget issue. To achieve these objectives, you must develop a trusting exchange of the most sensitive security intelligence among your peers so you’ll know where your organization stands relative to other enterprises. But be discreet and careful about it. You need to know the generally accepted and current security solutions. If the information you exchange is exposed, it could ruin your career and others, and could create a disaster for your organization. Your personal and ethical performance must be spotless, and you must protect your reputation at all costs. Pay particular attention to the ethics section of this book. I recommend that you join the Information Systems Security Association, become active in it, and become professionally certified as soon as you are qualified. My favorite certification is the Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium.

Donn B. Parker, CISSP
Los Altos, California

PROTECTION

DATA

PRIVACY

chapter

1

SAFE

CODE

Introduction to Information Security

PASSWORD

Do not figure on opponents not attacking; worry about your own lack of preparation.

BOOK OF THE FIVE RINGS

For Amy, the day began like any other at the Sequential Label and Supply Company (SLS) help desk. Taking calls and helping office workers with computer problems was not glamorous, but she enjoyed the work; it was challenging and paid well enough. Some of her friends in the industry worked at bigger companies, some at cutting-edge tech companies, but they all agreed that jobs in information technology were a good way to pay the bills.

The phone rang, as it did about four times an hour. The first call of the day, from a worried user hoping Amy could help him out of a jam, seemed typical. The call display on her monitor showed some of the facts: the user's name, his phone number and department, where his office was on the company campus, and a list of his past calls to the help desk.

"Hi, Bob," she said. "Did you get that document formatting problem squared away?"

"Sure did, Amy. Hope we can figure out what's going on this time."

"We'll try, Bob. Tell me about it."

"Well, my PC is acting weird," Bob said. "When I go to the screen that has my e-mail program running, it doesn't respond to the mouse or the keyboard."

"Did you try a reboot yet?"

“Sure did. But the window wouldn’t close, and I had to turn my PC off. After it restarted, I opened the e-mail program, and it’s just like it was before—no response at all. The other stuff is working OK, but really, really slowly. Even my Internet browser is sluggish.”

“OK, Bob. We’ve tried the usual stuff we can do over the phone. Let me open a case, and I’ll dispatch a tech over as soon as possible.”

Amy looked up at the LED tally board on the wall at the end of the room. She saw that only two technicians were dispatched to user support at the moment, and since it was the day shift, four technicians were available. “Shouldn’t be long at all, Bob.”

She hung up and typed her notes into ISIS, the company’s Information Status and Issues System. She assigned the newly generated case to the user dispatch queue, which would page the roving user support technician with the details in a few minutes.

A moment later, Amy looked up to see Charlie Moody, the senior manager of the server administration team, walking briskly down the hall. He was being trailed by three of his senior technicians as he made a beeline from his office to the room where the company servers were kept in a carefully controlled environment. They all looked worried.

Just then, Amy’s screen beeped to alert her of a new e-mail. She glanced down. The screen beeped again—and again. It started beeping constantly. She clicked the envelope icon and, after a short delay, the mail window opened. She had 47 new e-mails in her inbox. She opened one from Davey Martinez in the Accounting Department. The subject line said, “Wait till you see this.” The message body read, “Funniest joke you’ll see today.” Davey often sent her interesting and funny e-mails, and she clicked the file attachment icon to open the latest joke.

After that click, her PC showed the hourglass pointer icon for a second and then the normal pointer reappeared. Nothing happened. She clicked the next e-mail message in the queue. Nothing happened. Her phone rang again. She clicked the ISIS icon on her computer desktop to activate the call management software and activated her headset. “Hello, Help Desk, how can I help you?” She couldn’t greet the caller by name because ISIS had not responded. “Hello, this is Erin Williams in Receiving.”

Amy glanced down at her screen. Still no ISIS. She glanced up to the tally board and was surprised to see the inbound-call counter tallying up waiting calls like digits on a stopwatch. Amy had never seen so many calls come in at one time.

“Hi, Erin,” Amy said. “What’s up?”

“Nothing,” Erin answered. “That’s the problem.” The rest of the call was a replay of Bob’s, except that Amy had to jot notes down on a legal pad. She couldn’t dispatch the user support team either. She looked at the tally board. It had gone dark. No numbers at all.

Then she saw Charlie running down the hall from the server room. His expression had changed from worried to frantic.

Amy picked up the phone again. She wanted to check with her supervisor about what to do now. There was no dial tone.



LEARNING OBJECTIVES:

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

- Define information security
- Recount the history of computer security, and explain how it evolved into information security
- Define key terms and critical concepts of information security
- List the phases of the security systems development life cycle
- Describe the information security roles of professionals within an organization

Introduction

James Anderson, executive consultant at Emagined Security, Inc., believes information security in an enterprise is a “well-informed sense of assurance that the information risks and controls are in balance.” He is not alone in his perspective. Many information security practitioners recognize that aligning information security needs with business objectives must be the top priority.



For more information on Emagined Security Consulting, visit www.emagined.com.

This chapter’s opening scenario illustrates that information risks and controls may not be in balance at SLS. Though Amy works in a technical support role to help users with their problems, she did not recall her training about malicious e-mail attachments, such as worms or viruses, and fell victim to this form of attack herself. Understanding how malware might be the cause of a company’s problems is an important skill for information technology (IT) support staff as well as users. SLS’s management also shows signs of confusion and seems to have no idea how to contain this kind of incident. If you were in Amy’s place and were faced with a similar situation, what would you do? How would you react? Would it occur to you that something far more insidious than a technical malfunction was happening at your company? As you explore the chapters of this book and learn more about information security, you will become more capable of answering these questions. But, before you can begin studying details about the discipline of information security, you must first know its history and evolution.

The History of Information Security

Key Term

computer security In the early days of computers, this term specified the need to secure the physical location of computer technology from outside threats. This term later came to represent all actions taken to preserve computer systems from losses. It has evolved into the current concept of information security as the scope of protecting information in an organization has expanded.

The history of information security begins with the concept of **computer security**. The need for computer security arose during World War II when the first mainframe computers were developed and used to aid computations for communication code breaking, as shown in



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Figure 1-1 The Enigma¹

Source: National Security Agency. Used with permission.²

Figure 1-1. Multiple levels of security were implemented to protect these devices and the missions they served. This required new processes as well as tried-and-true methods needed to maintain data confidentiality. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and technologically sophisticated computer security safeguards.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on a MOTD (message of the day) file and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.³

› The 1960s

During the Cold War, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks. These mainframes required a less cumbersome process of communication than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. In 1968, Dr. Larry Roberts developed the ARPANET

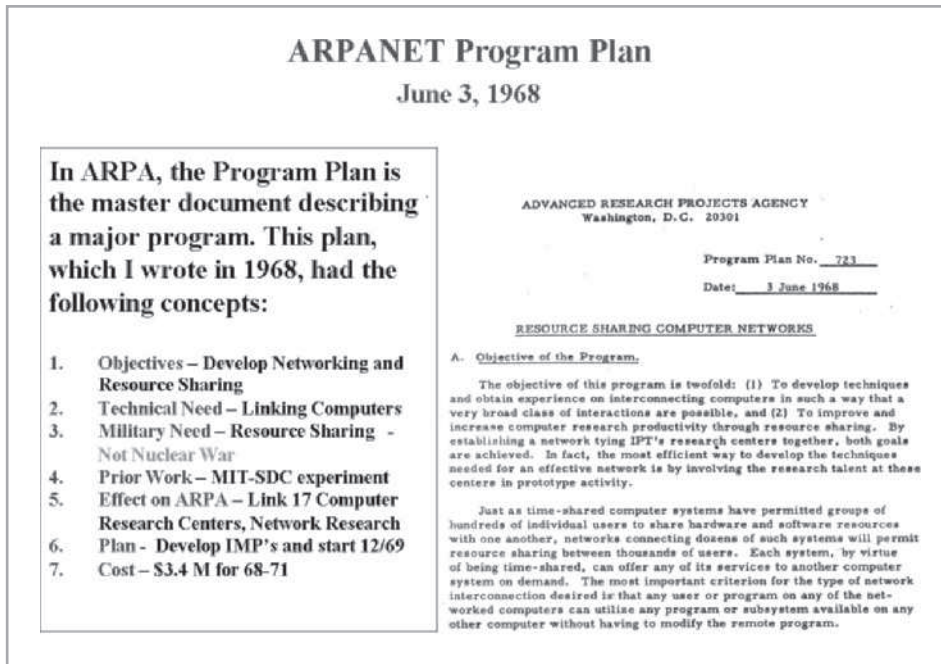



Figure 1-2 Development of the ARPANET

Source: Courtesy of Dr. Lawrence Roberts. Used with permission.⁴

project. Figure 1-2 is an excerpt from his Program Plan. ARPANET evolved into what we now know as the Internet, and Roberts became known as its founder.

 For more information on Dr. Roberts and the history of the Internet, visit his Web site at www.packet.cc.

› The 1970s and 80s

During the next decade, ARPANET became more popular and saw wider use, increasing the potential for its misuse. In 1973, Internet pioneer Robert M. Metcalfe (pictured in Figure 1-3) identified fundamental problems with ARPANET security. As one of the creators of Ethernet, a dominant local area networking protocol, he knew that individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorizations. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was commonly referred to as network insecurity.⁵ In 1978, Richard Bisbey and Dennis Hollingworth, two researchers in the Information Sciences Institute at the University of Southern California, published a study entitled “Protection Analysis: Final Report.” It focused on a project undertaken by ARPA to understand and detect



Figure 1-3 Dr. Metcalfe receiving the National Medal of Technology

Source: U.S. Department of Commerce. Used with permission.

vulnerabilities in operating system security. For a timeline that includes this and other seminal studies of computer security, see Table 1-1.

Security that went beyond protecting the physical location of computing devices began with a single paper sponsored by the Department of Defense. Rand Report R-609 attempted to define the multiple controls and mechanisms necessary for the protection of a computerized data processing system. The document was classified for almost ten years, and is now considered to be the paper that started the study of computer security.

The security—or lack thereof—of systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern both for the military and defense contractors.

In June 1967, ARPA formed a task force to study the process of securing classified information systems. The task force was assembled in October 1967 and met regularly to formulate recommendations, which ultimately became the contents of Rand Report R-609.⁶ The document was declassified in 1979 and released as Rand Report R-609-1. The content of the two documents is identical with the exception of two transmittal memorandums.



For more information on the Rand Report, visit www.rand.org/pubs/reports/R609-1.html and click the Read Online Version button.



Date	Document
1968	Maurice Wilkes discusses password security in <i>Time-Sharing Computer Systems</i> .
1970	Willis H. Ware authors the report <i>Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609</i> , which was not declassified until 1979. It became known as the seminal work identifying the need for computer security.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in <i>Preliminary Notes on the Design of Secure Military Computer Systems</i> .
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the <i>Federal Register</i> .
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software. ⁷
1979	Morris and Thompson author "Password Security: A Case History," published in the <i>Communications of the Association for Computing Machinery</i> (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1984	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report, the authors examined four "important handles to computer security:" physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security. ⁸
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the system administrator or other privileged users...the naive user has no chance." ⁹
1992	Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

Table 1-1 Key Dates in Information Security

© Cengage Learning 2015

Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide use of networking components in military information systems introduced security risks that could not be mitigated by the routine practices then used to secure these systems. Figure 1-4 shows an illustration of computer network vulnerabilities from the 1979 release of this document. This paper signaled a pivotal moment in computer security history—the scope of computer security expanded significantly from the safety of physical locations and hardware to include:

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in information security

MULTICS Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS). Although it is now obsolete,

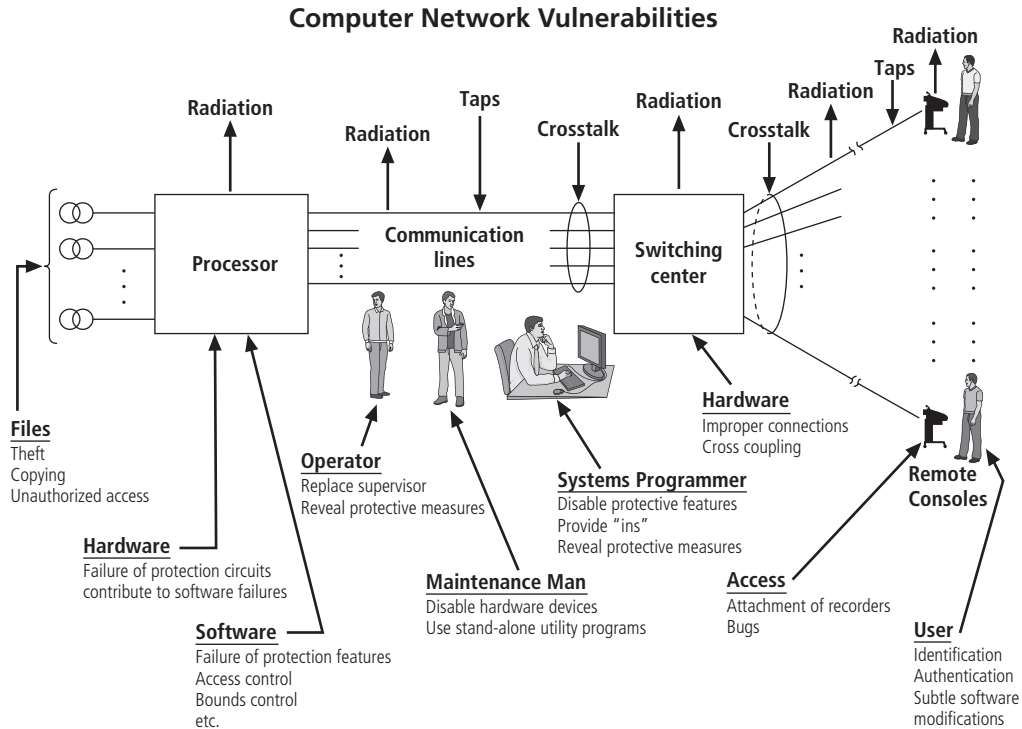


Figure 1-4 Illustration of computer network vulnerabilities from Rand Report R-609

Source: Rand Report R-609. Used with permission.¹⁰

MULTICS is noteworthy because it was the first operating system to integrate security into its core functions. It was a mainframe, time-sharing operating system developed in the mid-1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).

i For more information on the MULTICS project, visit web.mit.edu/multics-history.

In 1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlroy) created a new operating system called UNIX. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not. Its primary function, text processing, did not require the same level of security as that of its predecessor. Not until the early 1970s did even the simplest component of security, the password function, become a component of UNIX.

In the late 1970s, the microprocessor brought the personal computer (PC) and a new age of computing. The PC became the workhorse of modern computing, moving it out of the data center. This decentralization of data processing systems in the 1980s gave rise to networking—the interconnecting of PCs and mainframe computers, which enabled the entire computing community to make all its resources work together.



In the mid-1980s, the U.S. Government passed several key pieces of legislation that formalized the recognition of computer security as a critical issue for federal information systems. The Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987 defined computer security and specified responsibilities and associated penalties. These laws and others are covered in Chapter 3, “Legal, Ethical, and Professional Issues in Information Security.”

In 1988, the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense created the Computer Emergency Response Team (CERT) to address network security.

› The 1990s

At the close of the 20th century, networks of computers became more common, as did the need to connect them to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s after decades of being the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks. At first, these connections were based on de facto standards because industry standards for interconnected networks did not exist. These de facto standards did little to ensure the security of information, though some degree of security was introduced as precursor technologies were widely adopted and became industry standards. However, early Internet deployment treated security as a low priority. In fact, many problems that plague e-mail on the Internet today result from this early lack of security. At that time, when all Internet and e-mail users were presumably trustworthy computer scientists, mail server authentication and e-mail encryption did not seem necessary. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

In 1993, the first DEFCON conference was held in Las Vegas. Originally it was established as a gathering for people interested in information security, including authors, lawyers, government employees, and law enforcement officials. A compelling topic was the involvement of hackers in creating an interesting venue for the exchange of information between two adversarial groups—the “white hats” of law enforcement and security professionals and the “black hats” of hackers and computer criminals.

In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations. Antivirus products became extremely popular.

› 2000 to Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer’s stored information is contingent on the security level of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized