INFORMATION SECURITY

MANAGEMENT OF INFORMATION SECURITY

Sixth Edition

Michael E. Whitman
Herbert J. Mattord

INFORMATION SECURITY

MANAGEMENT OF INFORMATION SECURITY

Sixth Edition

Michael E. Whitman
Herbert J. Mattord

CENGAGE

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

CENGAGE

***Management of Information Security*, Sixth Edition**
Michael E. Whitman,
Herbert J. Mattord

SVP, GM Skills: Jonathan Lau

Product Director: Lauren Murphy

Product Team Manager: Kristin McNary

Product Manager: Amy Savino

Product Assistant: Jake Toth

Executive Director, Content Design: Marah Bellegarde

Director, Learning Design: Leigh Hefferon

Learning Designer: Natalie Onderdonk

Sr. Marketing Director: Michele McTighe

Assoc. Marketing Manager: Cassie Cloutier

Director, Content Delivery: Patty Stephan

Sr. Content Manager: Brooke Greenhouse

Digital Delivery Lead: Jim Vaughey

Senior Designer: Diana H. Graham

Production Service/Composition: SPi Global

Cover image: iStockPhoto.com/ValeryBrozhinsky

For product information and technology assistance, contact us at **Cengage Customer & Sales Support, 1-800-354-9706** or **support.cengage.com.**

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

Library of Congress Control Number: 2018936035

ISBN: 978-1-337-40571-3

Cengage
20 Channel Center Street
Boston, MA 02210
USA

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

To learn more about Cengage platforms and services, visit **www.cengage.com**.

To register or access your online learning solution or purchase materials for your course, visit **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: 2018

Brief Contents

PREFACE xv

CHAPTER 1
Introduction to the Management of Information Security 1

CHAPTER 2
Compliance: Law and Ethics 63

CHAPTER 3
Governance and Strategic Planning for Security 123

CHAPTER 4
Information Security Policy 169

CHAPTER 5
Developing the Security Program 219

CHAPTER 6
Risk Management: Assessing Risk 303

CHAPTER 7
Risk Management: Treating Risk 365

CHAPTER 8
Security Management Models 411

CHAPTER 9
Security Management Practices 457

CHAPTER 10
Planning for Contingencies 497

CHAPTER 11
Security Maintenance 567

CHAPTER 12
Protection Mechanisms 619

GLOSSARY 683

INDEX 709

Table of Contents

PREFACE xv

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 7

Key Concepts of Information Security: Threats and Attacks 11

- The 12 Categories of Threats 13

Management and Leadership 45

- Behavioral Types of Leaders 46
- Management Characteristics 47
- Governance 50
- Solving Problems 50

Principles of Information Security Management 52

- Planning 53
- Policy 54
- Programs 55
- Protection 55
- People 55
- Projects 55

Additional Reading 57

Chapter Summary 57

Review Questions 58

Exercises 59

Closing Case 60

- Discussion Questions 60
- Ethical Decision Making 60

Endnotes 61

CHAPTER 2

Compliance: Law and Ethics 63

Introduction to Law and Ethics 64

Ethics in InfoSec 66

Ethics and Education 70

Deterring Unethical and Illegal Behavior 72

Professional Organizations and Their Codes of Conduct 74

Association for Computing Machinery (ACM) 74

International Information Systems Security Certification Consortium, Inc. (ISC)² 75

SANS 75

Information Systems Audit and Control Association (ISACA).... 76

Information Systems Security Association (ISSA) 77

Information Security and Law....78

Types of Law 78

Relevant U.S. Laws 79

International Laws and Legal Bodies 95

State and Local Regulations.... 97

Standards Versus Law....101

Policy Versus Law 104

Organizational Liability and the Management of Digital Forensics 104

Key Law Enforcement Agencies 105

Managing Digital Forensics 109

Additional Reading 117

Chapter Summary.... 117

Review Questions 118

Exercises 119

Closing Case.... 120

Discussion Questions 120

Ethical Decision Making....120

Endnotes 120

CHAPTER 3

Governance and Strategic Planning for Security.... 123

The Role of Planning.... 125

Precursors to Planning.... 127

Strategic Planning.... 129

Creating a Strategic Plan....131

Planning Levels.... 132

Planning and the CISO.... 133

Information Security Governance 135

The ITGI Approach to Information Security Governance 136

NCSP Industry Framework for Information Security Governance 138

CERT Governing for Enterprise Security Implementation 140
ISO/IEC 27014:2013 Governance of Information Security 143
Security Convergence 145
Planning for Information Security Implementation 147
Implementing the Security Program using the SecSDLC 154
Additional Reading 163
Chapter Summary 164
Review Questions 165
Exercises 165
Closing Case 166
Discussion Questions 167
Ethical Decision Making 167
Endnotes 167

CHAPTER 4

Information Security Policy 169
Why Policy? 170
Policy, Standards, and Practices 175
Enterprise Information Security Policy 177
Integrating an Organization's Mission and Objectives into the EISP 178
EISP Elements 178
Example EISP Elements 180
Issue-Specific Security Policy 183
Elements of the ISSP 185
Implementing the ISSP 188
System-Specific Security Policy 190
Managerial Guidance SysSPs 191
Technical Specification SysSPs 192
Guidelines for Effective Policy Development and Implementation 197
Developing Information Security Policy 197
Policy Distribution 198
Policy Reading 199
Policy Comprehension 199
Policy Compliance 200
Policy Enforcement 201
Policy Development and Implementation Using the SDLC 201
Software Support for Policy Administration 206
Other Approaches to Information Security Policy Development 207
SP 800-18, Rev. 1: Guide for Developing Security Plans
for Federal Information Systems 209

A Final Note on Policy 212

Additional Reading 213

Chapter Summary 214

Review Questions 215

Exercises 216

Closing Case 217

- Discussion Questions 217
- Ethical Decision Making 217

Endnotes 218

CHAPTER 5

Developing the Security Program 219

Organizing for Security 220

- Security in Large Organizations 225
- Security in Medium-Sized Organizations 228
- Security in Small Organizations 229

Placing Information Security Within an Organization 230

Components of the Security Program 241

- Staffing the Security Function 244
- Information Security Professional Credentials 254
- Entering the Information Security Profession 265

Implementing Security Education, Training, and Awareness (SETA) Programs 267

- Security Education 269
- Security Training 271
- Security Awareness 278

Project Management in Information Security 286

- Projects Versus Processes 286
- Organizational Support for Project Management 288
- PMBOK Knowledge Areas 289
- Project Management Tools 292

Additional Reading 296

Chapter Summary 297

Review Questions 298

Exercises 299

Closing Case 299

- Discussion Questions 299
- Ethical Decision Making 300

Endnotes 300

CHAPTER 6

Risk Management: Assessing Risk

Risk Management: Assessing Risk 303
Introduction to the Management of Risk in Information Security 304
Knowing Yourself and Knowing the Enemy 305
The Information Security Risk Management Framework 305
Roles of Communities of Interest in Managing Risk 308
Executive Governance and Support 308
Framework Design 312
Framework Implementation 315
Framework Monitoring and Review 315
Continuous Improvement 316
The Risk Management Process 316
RM Process Preparation—Establishing the Context 317
Risk Assessment: Risk Identification 319
Risk Assessment: Risk Analysis 343
Risk Evaluation 355
Risk Treatment/Risk Control 359
Process Communications, Monitoring, and Review 359
Additional Reading 359
Chapter Summary 360
Review Questions 361
Exercises 361
Closing Case 362
Discussion Questions 362
Ethical Decision Making 362
Endnotes 363

CHAPTER 7

Risk Management: Treating Risk

Risk Management: Treating Risk 365
Introduction to Risk Treatment 366
Risk Treatment Strategies 368
Managing Risk 374
Feasibility and Cost-benefit Analysis 379
Other Methods of Establishing Feasibility 387
Alternatives to Feasibility Analysis 389
Recommended Alternative Risk Treatment Practices 392
Alternative Risk Management Methodologies 393
The OCTAVE Methods 393
Microsoft Risk Management Approach 394

FAIR 395
ISO Standards for InfoSec Risk Management 397
NIST Risk Management Framework (RMF) 399
Other Methods 403
Selecting the Best Risk Management Model 404
Additional Reading 405
Chapter Summary 405
Review Questions 406
Exercises 407
Closing Case 408
Discussion Questions 409
Ethical Decision Making 409
Endnotes 409

CHAPTER 8
Security Management Models 411
Introduction to Blueprints, Frameworks, and Security Models 412
Security Management Models 414
The ISO 27000 Series 414
NIST Security Publications 420
Control Objectives for Information and Related Technology 428
Committee of Sponsoring Organizations 430
Information Technology Infrastructure Library 431
Information Security Governance Framework 431
Security Architecture Models 434
TCSEC and the Trusted Computing Base 434
Information Technology System Evaluation Criteria 437
The Common Criteria 437
Access Control Models 438
Categories of Access Controls 440
Other Forms of Access Control 446
Academic Access Control Models 447
Bell-LaPadula Confidentiality Model 447
Biba Integrity Model 448
Clark-Wilson Integrity Model 449
Graham-Denning Access Control Model 450
Harrison-Ruzzo-Ullman Model 450
Brewer-Nash Model (Chinese Wall) 450

Additional Reading 451

Chapter Summary 451

Review Questions 452

Exercises 453

Closing Case 453

Discussion Questions 453

Ethical Decision Making 454

Endnotes 454

CHAPTER 9

Security Management Practices 457

Introduction to Security Practices 458

Security Employment Practices 459

Hiring 459

Contracts and Employment 462

Security Expectations in the Performance Evaluation 462

Termination Issues 463

Personnel Security Practices 464

Security of Personnel and Personal Data 466

Security Considerations for Temporary Employees, Consultants, and Other Workers 466

Information Security Performance Measurement 468

InfoSec Performance Management 469

Building the Performance Measurement Program 471

Specifying InfoSec Measurements 473

Collecting InfoSec Measurements 473

Implementing InfoSec Performance Measurement 478

Reporting InfoSec Performance Measurements 479

Benchmarking 481

Standards of Due Care/Due Diligence 482

Recommended Security Practices 483

Selecting Recommended Practices 484

Limitations to Benchmarking and Recommended Practices 485

Baselining 486

Support for Benchmarks and Baselines 487

ISO Certification 489

Additional Reading 490

Chapter Summary 491

Review Questions 492

Exercises 493
Closing Case 493
Discussion Questions 493
Ethical Decision Making 493
Endnotes 494

CHAPTER 10
Planning for Contingencies 497
Introduction to Contingency Planning 498
Fundamentals of Contingency Planning 500
Components of Contingency Planning 504
Business Impact Analysis 506
Contingency Planning Policies 513
Incident Response 513
Getting Started 514
Incident Response Policy 516
Incident Response Planning 517
Detecting Incidents 522
Reacting to Incidents 526
Recovering from Incidents 530
Disaster Recovery 538
The Disaster Recovery Process 540
Disaster Recovery Policy 541
Disaster Classification 542
Planning to Recover 545
Responding to the Disaster 546
Simple Disaster Recovery Plan 546
Business Continuity 549
Business Continuity Policy 550
Continuity Strategies 552
Timing and Sequence of CP Elements 554
Crisis Management 556
Business Resumption 558
Testing Contingency Plans 558
Final Thoughts on CP 560
Additional Reading 560
Chapter Summary 561
Review Questions 562

Exercises 563
Closing Case 563
Discussion Questions 564
Ethical Decision Making 564
Endnotes 564

CHAPTER 11

Security Maintenance 567
Introduction to Security Maintenance 568
Security Management Maintenance Models 569
NIST SP 800-100, Information Security Handbook: A Guide for Managers 569
The Security Maintenance Model 587
Additional Reading 614
Chapter Summary 614
Review Questions 615
Exercises 616
Closing Case 616
Discussion Questions 617
Ethical Decision Making 617
Endnotes 617

CHAPTER 12

Protection Mechanisms 619
Introduction to Protection Mechanisms 620
Access Controls and Biometrics 622
Managing Network Security 630
Firewalls 631
Intrusion Detection and Prevention Systems 643
Wireless Networking Protection 647
Scanning and Analysis Tools 651
Managing Server-Based Systems with Logging 655
Managing Security for Emerging Technologies 660
Cryptography 662
Encryption Operations 664
Using Cryptographic Controls 671
Managing Cryptographic Controls 674

Additional Reading 677

Chapter Summary........ 677

Review Questions 679

Exercises 679

Closing Case........ 680

Discussion Questions 681

Ethical Decision Making........681

Endnotes 681

GLOSSARY 683

INDEX........709

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. Global commerce is reliant on the Internet, which creates an increasing threat of attacks on information assets and a need for greater numbers of professionals capable of protecting those assets. With billions of Internet users capable of accessing and attacking online information from anywhere at any time, the threat of an attack from individuals, criminals, and government entities grows daily.

To secure commerce and 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

This textbook strives 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, few textbooks 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. In this edition, the discussion of digital forensics has been moved to Chapter 2 for better alignment with the primary subjects being covered.

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: 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: Treating 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—Security Maintenance

This chapter 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.

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.

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.

Additional Reading—Each chapter includes suggestions for reading outside resources that might augment or extend understanding of one or more aspects of the chapter.

New to This Edition

This sixth 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.

The material on personnel management has been consolidated and reorganized. Personnel placement, staffing, and credentials are now covered in Chapter 5, and employment practices are discussed in Chapter 9. Digital forensics is now covered in Chapter 2.

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*, *6e*, for their courses is a complete package of instructor resources. These resources are available from the Cengage 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.
- *Appendix*: The appendix has been relocated from the bound textbook and is available for instructor use. It describes methods for evaluating security, including (1) NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, (2) ISO 17799: 2005 Overview, (3) The OCTAVE Method of Risk Management, and (4) the Microsoft Risk Management Approach.
- *Lab Exercises*: Each chapter includes hands-on exercises designed to reinforce the theoretical concepts of the corresponding materials. Additional exercises and labs are available in the MindTap enhanced edition of the textbook.

- *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*). 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 policy and planning and in 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 *Journal of Cybersecurity Education, Research and Practice*, and he continually solicits relevant and well-written articles of interest to faculty teaching and researching cybersecurity 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 and soldier 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.

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:

- Paul D. Witman, Ph.D., Associate Professor, Information Technology Management, California Lutheran University, School of Management, Thousand Oaks, CA
- Michael Moorman, Ph.D., Professor of Computer Science, Department of Computer Science and Information Systems, St. Leo University, St. Leo, FL

Special Thanks

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

Natalie Onderdonk, Learning Designer

Dan Seiter, Developmental Editor

Kristin McNary, Product Team Manager

Amy Savino, Product Manager

Brooke Greenhouse, Senior Content 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:

David Rowan

Charles Cresson Wood

Clearwater Compliance

The View Point authors:

- Henry Bonin
- Lee Imrey
- Robert Hayes and Kathleen Kotwicka
- David Lineman
- Paul D. Witman & Scott Mackelprang
- Alison Gunnels
- George V. Hulme
- Tim Callahan
- Mark Reardon
- Martin Lee
- Karen Scarfone
- Donald "Mac" McCarthy
- 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 at *infosec@kennesaw.edu*.

Foreword

By David Rowan, retired 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.

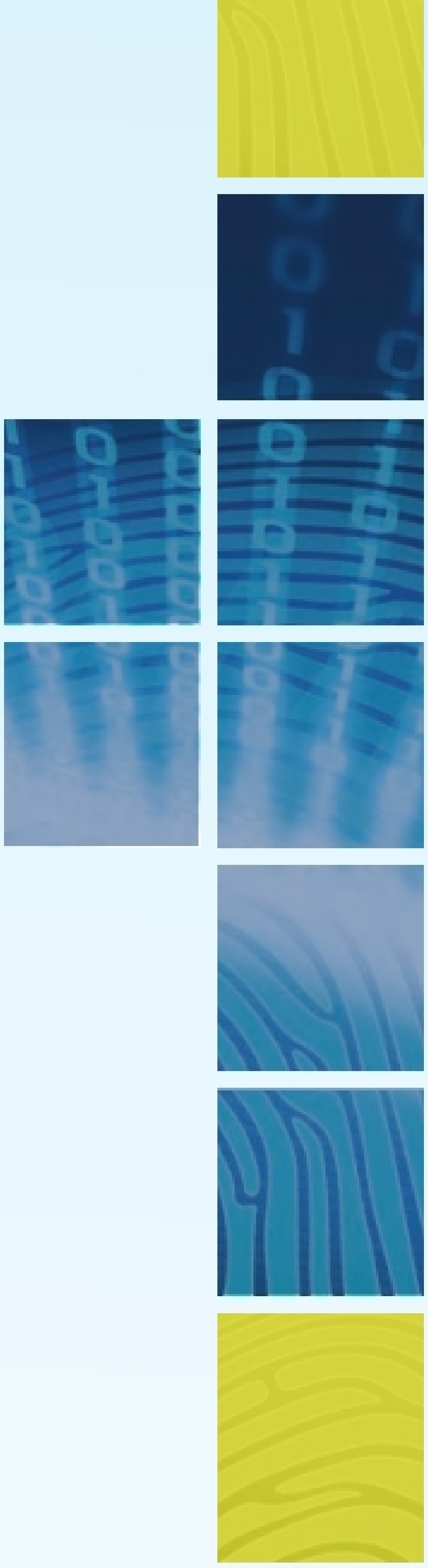
The motives of these actors matter, but regardless of why they threaten what technology gives us, the actions we take to safeguard it is up to us. That's why I am glad you are reading this. We need guardians of the trust we place in technology and the information flow it enables.

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 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 2018



CHAPTER 1

INTRODUCTION TO THE MANAGEMENT OF INFORMATION SECURITY

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

—HENRY MINTZBERG

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

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

Describe the importance of the manager's role in securing an organization's information assets

Differentiate information security management from general business management

Case Opener

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 manager of information risk 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 Sequential Label and Supply (SLS), the company she used to work for. 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 senior 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 I bring up 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 anytime soon. 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 wasting their time, and they don't seem to take our 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 get together for coffee."

Introduction to Security

Key Terms

asset An organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible object. Assets, particularly information assets, are the focus of what security efforts are attempting to protect.

information asset The focus of information security; information that has value to the organization, and the systems that store, process, and transmit the information.

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. In addition, 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 and whatever 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 must 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 recommendations to executive management 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.