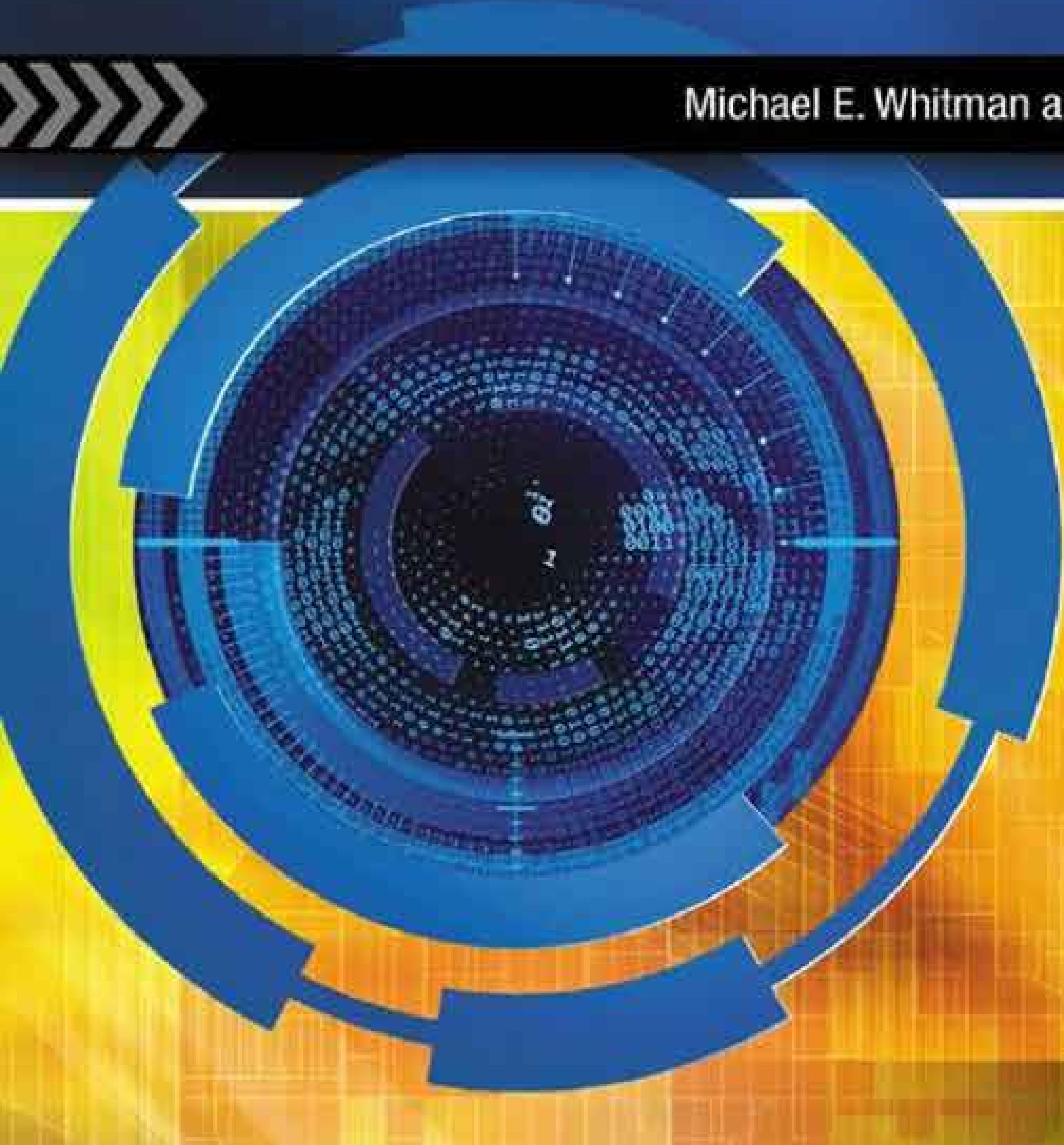
Fourth Edition

MANAGEMENT OF INFORMATION SECURITY

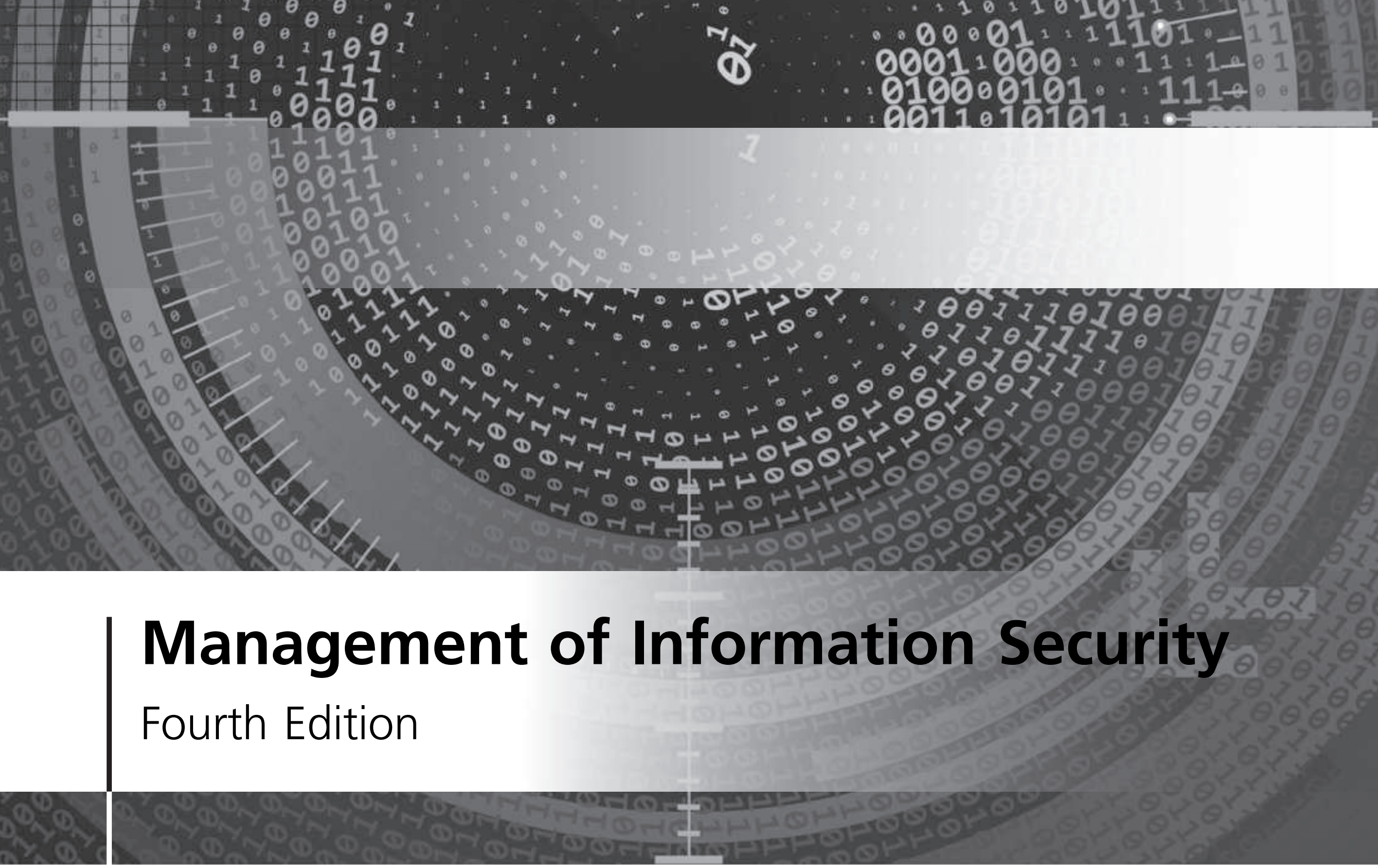
Michael E. Whitman and Herbert J. Mattord



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Management of Information Security

Fourth Edition



Management of Information Security

Fourth Edition

Michael E. Whitman, Ph.D., CISM, CISSP
Herbert J. Mattord, Ph.D., CISM, CISSP
Kennesaw State University

CENGAGE
Learning®

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

CENGAGE
Learning®

Management of Information Security, Fourth Edition

Michael E. Whitman and Herbert J. Mattord

General Manager: Dawn Gerrain

Product Manager: Nick Lombardi

Senior Director, Development: Marah Bellegarde

Product Development Manager: Leigh Hefferon

Senior Content Developer: Natalie Pashoukos

Developmental Editor: Kent Williams

Product Assistant: Torey Schantz

Brand Manager: Kristin McNary

Market Development Manager: Gretchen Swann

Senior Production Director: Wendy A. Troeger

Production Manager: Andrew Crouth

Content Project Manager: Allyson Bozeth

Art Director: GEX

Media Editor: Debbie Bordeaux

Cover Photo: ©iStockphoto.com/polygraphus

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Microsoft and the Office logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Any fictional data related to persons or companies or URLs used throughout this book is intended for instructional purposes only. At the time this book was printed, any such data was fictional and not belonging to any real persons or companies.

The programs in this book are for instructional purposes only. They have been tested with care, but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities with respect to the programs.

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

For permission to use material from this text or product,
submit all requests online at **www.cengage.com/permissions**
Further permissions questions can be emailed to
permissionrequest@cengage.com

Library of Congress Control Number: 2013945552

ISBN-13: 978-1-285-06229-7

ISBN-10: 1-285-06229-9

Cengage Learning

200 First Stamford Place, 4th Floor
Stamford, CT 06902
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
1 2 3 4 5 6 7 17 16 15 14 13

Brief Table of Contents

Table of Contents

CHAPTER 3

Planning for Contingencies 73

CHAPTER 4

Information Security Policy 123

Preface

As global networks continue to expand, the interconnections among them become ever more vital to the smooth operation of commerce, which depends on communication and computing systems. However, escalating attacks on information assets and the success of criminal attackers illustrate the weaknesses in current information technologies and the need for heightened information security.

To secure systems and networks, organizations must draw on the available pool of information security practitioners. These same organizations will in future count on the next generation of professionals to have the correct mix of skills and experiences to develop more secure computing environments. Students of technology must learn to recognize the threats and vulnerabilities present in existing systems. They must also learn how to design and implement secure systems that will address these threats in the future.

Why This Text Was Written

The purpose of this textbook is to fulfill the need for a quality academic textbook in the discipline of information security management. While there are dozens of quality publications on information security and assurance for the practitioner, there are few textbooks that provide the student with an in-depth study of information security management. Specifically, those in disciplines such as information systems, 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 management overview of information security and a thorough treatment of the administration of information security. It can be used to support course delivery for information security programs for information technology students, as well as for IT management and technology management curricula aimed at business or technical management 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 Technologies (NIST, at *csrc.nist.gov*), the authors have also tapped into 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, 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. This chapter also provides an overview of project management, a necessary skill in any IT/information security professional's portfolio.

Chapter 2—Planning for Security

This chapter explains the importance of planning and describes the principal components of organizational planning and information security system implementation planning.

Chapter 3—Planning for Contingencies

This chapter describes the need for contingency planning and explores the major components of contingency planning. It illustrates how to create a simple set of contingency plans using business impact analysis, and how to prepare and execute a test of contingency plans.

Chapter 4—Information Security Policy

This chapter defines information security policy and describes its central role in a successful information security program. Research has shown that there are 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 the information security program. Students learn how to plan and staff 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.

Chapter 6—Security Management Models

This chapter describes the components of the dominant information security management models, including U.S. government-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 7—Security Management Practices

This chapter describes the fundamentals of and emerging trends in information security management practices and explains how these practices help organizations meet U.S. and international compliance standards. It also covers the certification and accreditation of U.S. federal IT systems.

Chapter 8—Risk Management: Identifying and Assessing Risk

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

Chapter 9—Risk Management: Controlling Risk

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

Chapter 10—Protection Mechanisms

This chapter introduces students to the world of technical risk 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.

Chapter 11—Personnel and Security

This chapter expands upon the discussion of the skills and requirements for information security positions introduced in Chapter 5. It explores the various information security professional certifications and identifies which skills are encompassed by each. The second half of the chapter explores the integration of information security constraints—to control employee behavior and prevent misuse of information—into an organization's human resources processes.

Chapter 12—Law and Ethics

In this chapter, students learn about the legal 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.

Appendix

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

Features

Chapter Scenarios—Each chapter opens with a short story 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 and offers a few discussion questions to round out each scenario. These questions give the student and the instructor an opportunity to discuss the issues that underlie the content.

Viewpoints—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 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 Case Exercises, which give them the opportunity to examine the information security arena outside the classroom. Using the Exercises, students can research, analyze, and write to reinforce learning objectives and deepen their understanding of the text. The Case Exercises require that students use professional judgment, powers of observation, and elementary research to create solutions for simple information security scenarios.

New to This Edition

This fourth 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, the fourth edition has fewer technical examples, in-depth discussions, and Offline boxes. This edition also has additional coverage in key managerial areas: risk management, information security governance, access control models, and information security program assessment and metrics. Chapter 1 consolidates all the introductory and general IT managerial material.

In general, the entire text has been updated 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.

Instructor Resources

The following supplemental materials are available when this book is used in a classroom setting. All the supplements available with this book are provided to the instructor on the Instructor Companion Site at www.cengage.com. Instructors can access these resources through one single sign-on experience. If you do not already have a Cengage SSO account, click on "Click HERE to register" in the Faculty single sign-on box to get started right away.

- **Electronic Instructor's Manual**—The Instructor's Manual that accompanies this book includes additional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional activities.
- **Solutions**—The instructor resources include solutions to all end-of-chapter material, including review questions and case projects.
- **ExamView®**—ExamView®, the ultimate tool for objective-based testing needs, is a powerful test generator that enables instructors to create paper, LAN, or Web-based tests from test banks designed specifically for their Cengage Learning text. Instructors can utilize the ultra-efficient Quick Test Wizard to create tests in less than five minutes by taking advantage of Cengage Learning's question banks, or customize their own exams from scratch.
- **PowerPoint Presentations**—This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make 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.
- **Figure files**—All figures and tables in the book are reproduced on the Instructor Companion Site. Similar to the PowerPoint presentations, they are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

Additional Resources

Lab Manual—Cengage Learning has produced a lab manual (*Hands-On Information Security Lab Manual, Fourth Edition*) written by the authors that can be used to provide technical hands-on exercises in conjunction with this book. Contact your Cengage Learning sales representative for more information.

Readings and Cases—Cengage Learning also produced two texts—*Readings and Cases in the Management of Information Security* (ISBN-13: 978-0-619-21627-6) and *Readings & Cases in Information Security: Law & Ethics* (ISBN-13: 978-1-435-44157-6)—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 and Assurance—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 and Awareness (*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 Director of the Coles 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 and Cases in Information Security: Law and 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 Course Technology. Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, Ethical Computing, and Information Systems Research Methods. 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 three times.

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 Assistant Professor of Information Security at Kennesaw State University, where he serves as the program coordinator for the Information Security and Assurance degree programs. 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; Readings & Cases in Information Security: Law & Ethics; Guide to Network Security; and Hands-On Information Security Lab Manual*, all from Cengage Course Technology. 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 also an active member of the Information Systems Security Association and Information Systems Audit and Control Association. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this and his earlier textbooks was acquired.

Acknowledgments

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

Reviewers

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

Wasim A. Al-Hamdani, Ph.D.
Professor of Cryptography and Information Security
Information Security Lab, Kentucky State University
Frankfort, KY

Michelle Ramim, Ph.D.
Instructor and IS consultant
Nova Southeastern University
Wayne Huizenga School of Business and Entrepreneurship
Fort Lauderdale, FL

James Rust, MSIS
Technical Services Engineer
Buford, GA

Dale Suggs, BBA, MA, MS
Instructor, Information Technology and Security
Campbell University
Buies Creek, NC

Paul Witman, Ph.D.
Associate Professor, IT Management
Director, Undergraduate Programs, School of Management
California Lutheran University
Thousand Oaks, CA

Special Thanks

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

Natalie Pashoukos, Senior Content Developer

Kent Williams, Developmental Editor

Nick Lombardi, Product Manager

Allyson Bozeth, Content Project Manager

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

Charles Cresson Wood

NetIQ Corporation

The Viewpoint authors:

Henry Bonin

Robert Lang

Karen Scarfone

David Lineman

Paul D. Witman & Scott Mackelprang

Mark Reardon

Martin Lee

George V. Hulme

Tim Callahan

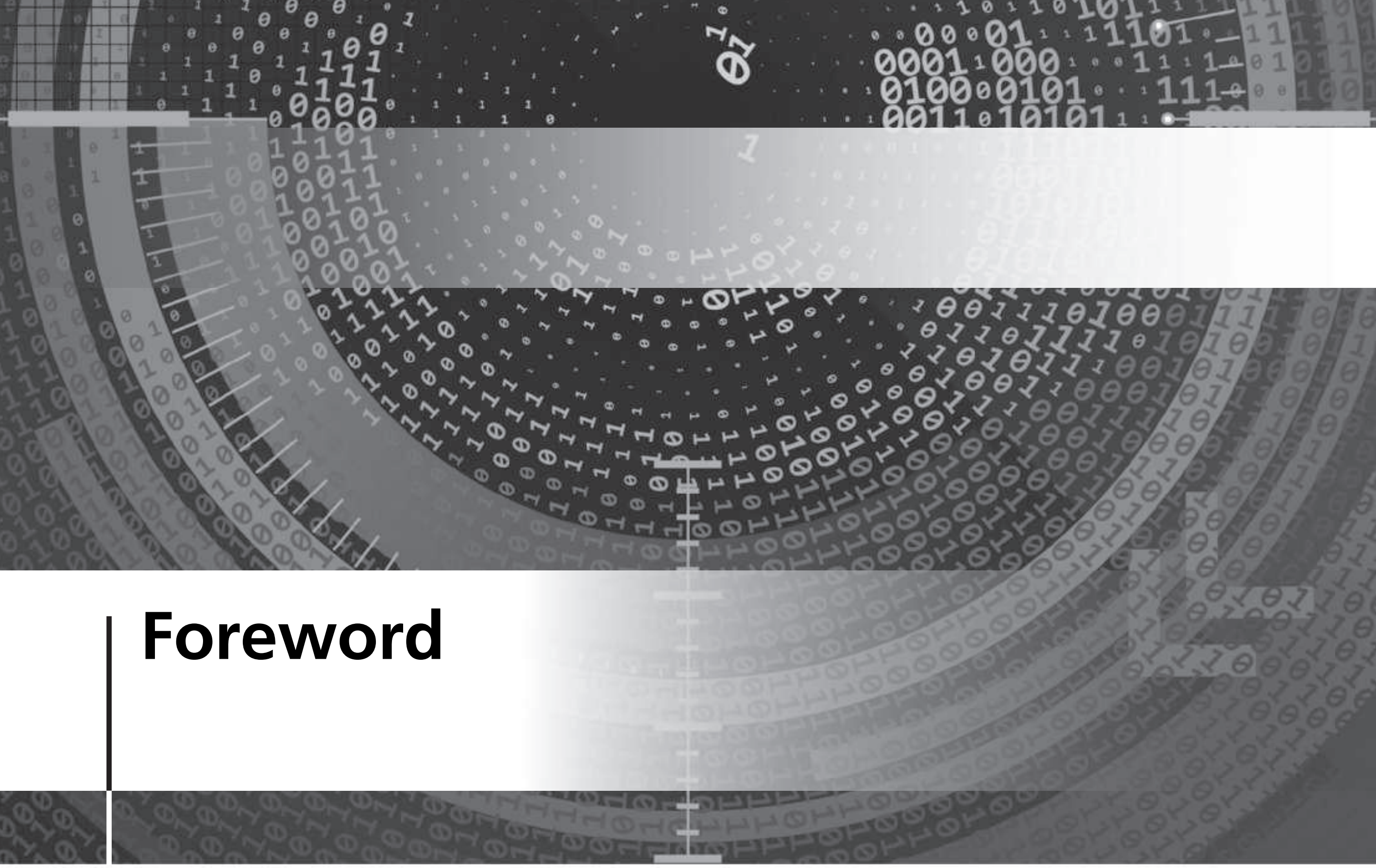
Todd E. Tucker

Alison Gunnels

Lee Imrey

Our Commitment

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



Foreword

By Charles Cresson Wood

Over the last 30+ years that I've worked in the information security field, I've had an opportunity to perform risk assessments for over 125 different organizations around the world. No matter how large the organization, no matter how well-respected it is in the public's eyes, and no matter how much high-tech gear it employs, in all cases I find that management doesn't take information security seriously enough.

In part, this is because information security is still a relatively new field and the long-run implications of doing it well or poorly are still being discovered (recent industrial espionage attacks originating in China provide a good example). In part, this lack of seriousness is because information security is a rapidly emerging multidisciplinary field and cross-domain creative thinking is in critically short supply. In part, this is also because top management often doesn't know much, and doesn't care to know much, about information systems technology. In part, this is additionally because top management has been making traditional tradeoff decisions, where information security loses when up against other recognized-as-important objectives such as lowered costs, greater user-friendliness, accelerated time to market with a new product, etc. If top management accurately understood the modern-day importance of information security, they would be spending much more money on it as well as giving it much more of their personal attention.

Times have changed dramatically, except top management in most cases hasn't yet appreciated how different things now are. For example, consider the case of Arthur Andersen, once one of the largest and most-highly-regarded public accounting firms in the world. Andersen did some auditing and consulting work for Enron, now a discredited and defunct energy trading concern. A U.S. Securities and Exchange Commission investigation into Enron's accounting practices caused certain Andersen employees to destroy documents that might have been relevant to the investigation. Aside from the fact that Andersen staff may have been involved in "cooking the books" along with Enron accounting staff, there was a major misunderstanding about the document destruction policy at Andersen. Certain staff believed they were doing the right thing when they destroyed thousands of pounds of Enron documents.

Of course, document destruction is an important part of the information security field. If these staff members had received much better training about this document destruction policy, Andersen might still be in existence. So, here we have a misunderstanding about and a lack of adequate training in information security, leading to the downfall of one the world's largest accounting firms. But in spite of this case and a host of other publicly revealed and very serious cases, top management at most organizations still believes that information security is a relatively unimportant issue, not worthy of considerable top management attention.

Additionally, please consider a recent poll conducted by Harris Interactive that indicated fully 79 percent of the American public believes that their personal information will be shared with other organizations without their permission. Apparently, Americans don't believe businesses and government agencies when they publish privacy policies. Apparently, Americans think these policies are just "window dressing" or something to please the auditors and regulators. What we have here is a major trust problem, where customers don't believe what businesses and government agencies say about the handling of private data. This is indicative of a serious failure on the part of these organizations; they have failed to convince customers that they will dutifully respect customer privacy rights.

An earlier study, performed by the same organization (then called Louis Harris Associates), indicated that the take-up or adoption rate for new electronic services, such as Internet merchant credit card sales, would double when adequate privacy safeguards were added. In other words, customers will be twice as likely to place an order online if they feel comfortable that their personal information will be adequately protected. Yet, top management so often doesn't allocate sufficient resources to information security—for instance by establishing a Chief Privacy Officer—and the net result is that sales suffer. Top management so often doesn't appreciate how doing a good job in the information security realm will lead to a variety of tangible business benefits, like increased sales and competitive advantage. If being able to double the level of sales isn't important to top management, what is?

So, information security very pressingly now needs to be recognized as a regular part of every modern organization. People need to have information security tasks expressly identified in their job descriptions, several departments need to have information security expressly stated in their mission statements, and outsourcing firms need to have information security expressly stated in their service-level agreements. Likewise, if it is used with employer-provided data, every worker's portable computer needs to be outfitted with a standard suite of software that includes a malware/spyware detection package, a hard drive encryption routine, a data wipe routine for use when the device is lost, and an automated software update program. End users also need to be well trained about information security. For instance, they need to know how to construct a fixed password that is difficult for others to guess but is, at the same time, easy for the user to remember. End users are now on the front line of the information security war. And a war is what it is because new, more complex, and more aggressive ways to compromise information systems security are being developed every day.

Information security cannot be something that is left to the technologists within the Information Technology Department. End users, for example, must deal with telephone callers who are seeking to get information through what is called social engineering. Also known as masquerading or spoofing, this technique involves leading users to believe that the caller is somebody other than who he really is. A caller could say he was from the IT Department, that he needed to have the user's user-ID and fixed password in order to correct a problem with the network. While it may sound unbelievable, unless users are told not to divulge such information, studies have shown that a large percentage of the user population will simply reveal their user-ID and password.

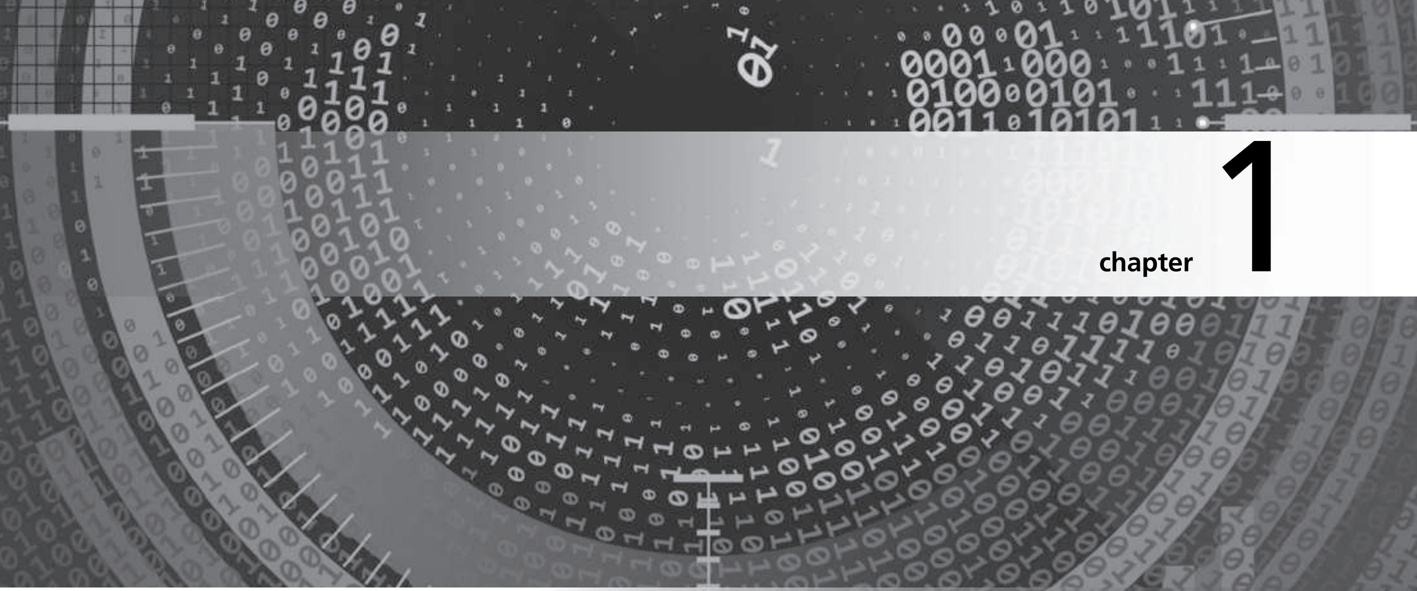
Everybody who comes into contact with sensitive, valuable, or critical information needs to know about information security. This means that the janitor needs to know how to dispose of confidential documents that may have been thrown away in the trash. This means that the temporary staff person who is answering the telephone at the front desk needs to know what information he or she can divulge to outsiders. This means that outsourcing firms must know how to respond to a hacker break-in so that losses are minimized, so that the subscribing organization's good reputation is maintained, and so that the subscribing firm's business activity can proceed without undue interruption.

In other words, information security must be approached with a team of individuals, all consistently using the same approaches to security, each with her own special part to play. In this context, I welcome the fourth edition of this textbook to train our future leaders. Every person working in modern businesses and/or government agencies will need to know a good deal about the management issues related to practical information security. If they cover information security at all, too many of the current college classes get bogged down in the technology. While the technology is interesting, it is an overview, a holistic perspective, that is needed so that these future leaders can understand the importance of and the ways to use information security. It is an overview like that provided by this textbook that can acquaint workers with the objectives of information security, and that will then assist them in making good judgment calls in the arena of information security.

Information security is multidisciplinary, multidepartmental, and increasingly multiorganizational in its scope. Future business leaders must appreciate how information security fits in with the other activities performed by the organizations where they will work.

The need for this information security knowledge gets more pressing every year. The U.S. Federal Bureau of Investigation teams up with the Computer Security Institute every year to do a survey about computer crime. In a recent year, some 50 percent of the respondents to this survey indicated that their organization doesn't have a policy informing them where they should report information security violations and incidents. If workers at an organization don't even know to whom, and when, they should report a violation or an incident, then there is no chance that top management will know what is really happening when it comes to information security. If top management doesn't know what's happening, then there will be no hope that they will be able to adequately manage the problem. In the interests of adequately managing this serious problem, this book helps by talking about best practices, which can help management figure out what's happening, and from there determine the best way to address the problems.

Charles Cresson Wood, MBA, MSE, CISA, CISSP, CISM
Independent Information Security Consultant
Mendocino, California



chapter 1

Introduction to the Management of Information Security

If this is the information superhighway, it's going through a lot of bad, bad neighborhoods.

DORIAN BERGER, *1997*

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

This occasion marked Iris's first ISSA meeting. With a mountain of pressing matters on her cluttered desk, Iris wasn't certain of exactly 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 firm.

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

"Hi, Charley," she said.

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

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

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

Charley 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 number—call me tomorrow and we'll arrange to get together for coffee."

LEARNING OBJECTIVES

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

- Describe the importance of the manager's role in securing an organization's use of information technology and explain who is responsible for protecting an organization's information assets
- List and discuss the key characteristics of information security
- Discuss the key characteristics of leadership and management
- Differentiate information security management from general business management
- Identify and describe basic project management practices and techniques

Introduction

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 20 years, however, technology has permeated 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," which covers a broader range of issues, from the protection of data to the protection of human resources. 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 technical managers—like Iris in the opening scenario of this chapter—allows for the creation of professionally managed information security teams whose main objective is the protection of information assets.

Organizations must realize that information security funding and planning decisions involve more than just technical managers, such as information security managers or members of the information security team. Altogether, they should involve three distinct groups of decision makers, or **communities of interest**:

- Managers and professionals in the field of information security
- Managers and professionals in the field of IT
- Managers and professionals from the rest of the organization

These three groups should engage in constructive debate 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 **information technology community** supports the business objectives of the organization by supplying and supporting IT that is appropriate to the organization's needs.
- The **general business community** articulates and communicates organizational policy and objectives and allocates resources to the other groups.

Working together, these communities of interest make decisions about how to secure an organization's information assets most effectively. As the discussion between Iris and Charley 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 documenting) the risk associated with operating information assets. 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.

What Is Security?

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

In general, **security** is the quality or state of being secure—being free from danger. To be secure is to be protected from the risk of loss, damage, or 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—**Protecting people, physical assets, and the workplace from various threats, including fire, unauthorized access, and natural disasters
- **Operations security—**Protecting the organization's ability to carry out its operational activities without interruption or compromise
- **Communications security—**Protecting the organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives
- **Network security—**Protecting the organization's data networking devices, connections, and contents as well as protecting the ability to use that network to accomplish the organization's data communication functions

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

Information security (InfoSec) is the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology. Figure 1-1 shows that InfoSec includes the broad areas of InfoSec management (the topic of this book), computer and data security, and network

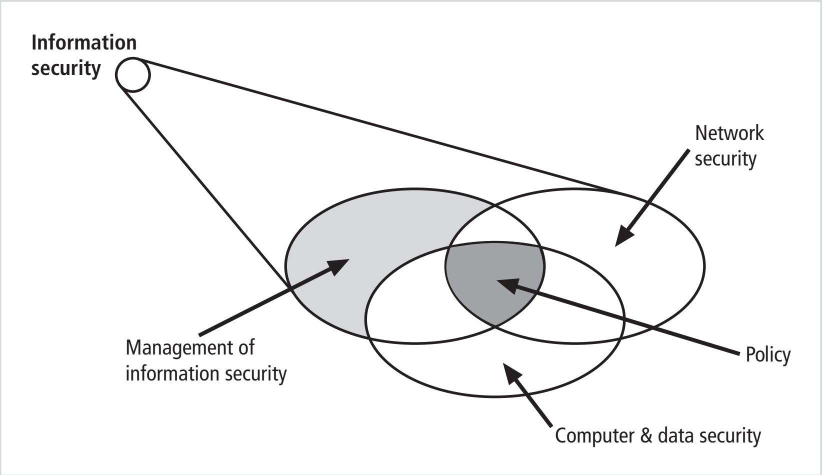


Figure 1-1 Components of information security

Copyright © 2014 Cengage Learning®.

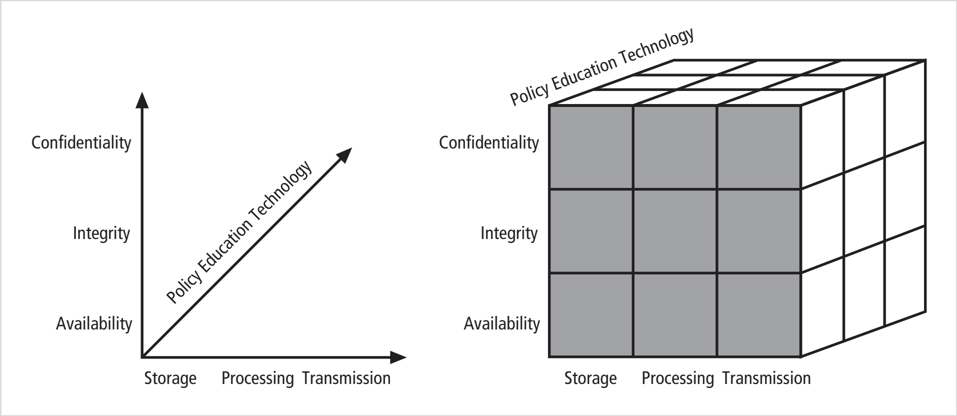


Figure 1-2 CNSS security model

Copyright © 2014 Cengage Learning®.

security; it also shows that policy is the space where these components overlap. (You will learn about policy in detail in Chapter 4.)

CNSS Security Model

The CNSS document *NSTISSI No. 4011 National Training Standard for Information Systems Security (InfoSec) Professionals*[1] presents a comprehensive model of InfoSec known as the McCumber Cube, which is named after its developer, John McCumber. Shown in Figure 1-2, which is an adaptation of the NSTISSI model, the McCumber Cube serves as the standard for understanding many aspects of InfoSec, shows the three dimensions that are central to the discussion of InfoSec: information characteristics, information location, and security control categories. If you extend the relationship among the three dimensions that are represented by the axes in the figure, you end up with a 3 × 3 × 3 cube with 27 cells. Each cell represents an area of intersection among these three dimensions, which must be addressed to secure information. When using this model to design or review any InfoSec program, you must make sure that each of the 27 cells is properly addressed by each of the three communities of interest. For example, the cell representing the intersection of the technology, integrity, and storage criteria could include controls or safeguards addressing the use of technology to protect the integrity of information while in storage. Such a control might consist of a host intrusion detection system (HIDS), for example, which would alert the security administrators when a critical file was modified or deleted.

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

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

Key Concepts of Information Security

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

Confidentiality

Confidentiality is the characteristic of information whereby only those with sufficient privileges and a demonstrated need may access it. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used, including:

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

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

Integrity

In general, **integrity** is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being entered, stored, or transmitted.

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

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

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

Availability **Availability** of information occurs when users have access to it in a usable format, without interference or obstruction. (For the purposes of this definition, a user may be either a person or another computer system.) Availability does not imply that the information is accessible to any user; rather, it means it is accessible to authorized users.

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

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

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

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

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

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

What Is Management?

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

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

Note that there are differences between leadership and management. A leader influences employees so that they are willing to accomplish objectives. He or she is expected to lead by example and demonstrate personal traits that instill a desire in others to follow. In other words, leadership provides purpose, direction, and motivation to those who follow.

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

Behavioral Types of Leaders

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

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

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

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

Management Characteristics

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

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

The traditional approach to management theory is often well covered in introductory business courses and will not be revisited here. Rather, we will focus on the POLC principles that managers employ when dealing with tasks. Figure 1-3 summarizes these principles and illustrates how they are conceptually related.

Planning

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

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

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

The planning process begins with the creation of strategic plans for the entire organization. The resulting plan is then divided into planning elements relevant to each major business unit of the organization. These business units in turn create business plans that meet the requirements of the overall organizational strategy. The plans are communicated to mid-level