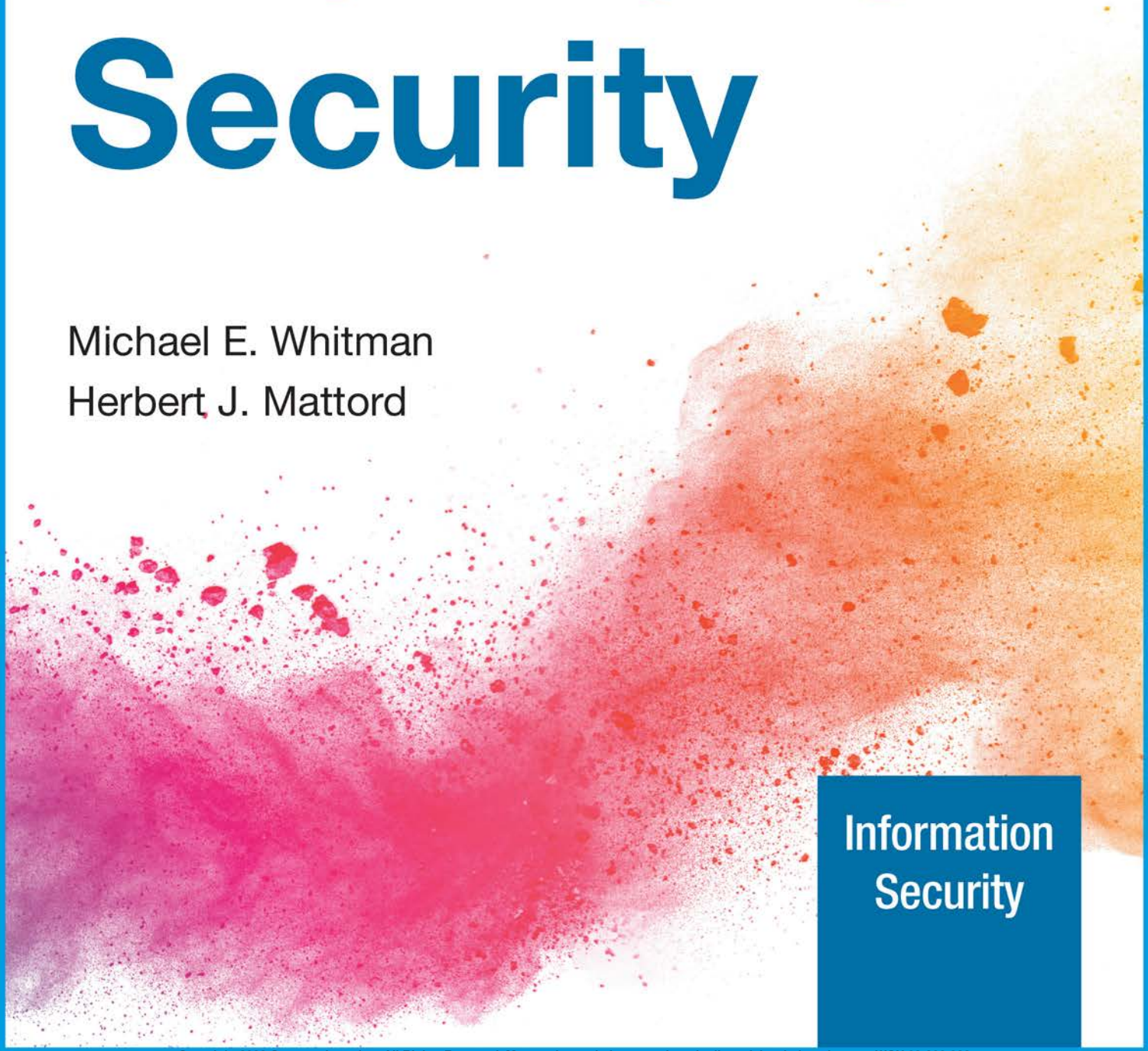
CENGAGE

Seventh Edition

Principles of Information Security

Michael E. Whitman
Herbert J. Mattord



Information Security

Seventh Edition

Principles of Information Security

Michael E. Whitman, *Ph.D., CISM, CISSP*
Herbert J. Mattord, *Ph.D., CISM, CISSP*

Information Security

CENGAGE

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

Principles of Information Security,
7th Edition
Michael E. Whitman and Herbert J. Mattord

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management: Thais Alencar

Product Director: Mark Santee

Associate Product Manager: Danielle Klahr

Product Assistant: Tom Benedetto

Executive Director, Learning: Natalie Skadra

Learning Designer: Mary Clyne

Vice President, Product Marketing: Jason Sakos

Portfolio Marketing Manager: Mackenzie Paine

Senior Director, Content Creation: Rebecca von Gillern

Content Manager: Christina Nyren

Director, Digital Production Services: Krista Kellman

Senior Digital Delivery Lead: Jim Vaughey

Developmental Editor: Dan Seiter

Production Service/Composition: SPi Global

Design Director: Jack Pendleton

Designer: Erin Griffin

Text Designer: Erin Griffin

Cover Designer: Erin Griffin

Cover image(s): Vandathai/Shutterstock.com

Library of Congress Control Number: 2021909680

ISBN: 978-0-357-50643-1

Cengage
200 Pier 4 Boulevard
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**.

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.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: 2021

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

—MEW

To my grandchildren, Julie and Ellie; it is a wonderful life.

—HJM

Brief Contents

Table of Contents

Module 6

Module 7

Preface

The world continues to become ever more interconnected. As global information networks continue to expand, the interconnection of devices of every description becomes vital, as does the smooth operation of communication, computing, and automation solutions. However, ever-evolving threats such as malware and phishing attacks and the success of criminal and hostile government attackers illustrate weaknesses in the current technical landscape and the need to provide heightened security for information systems.

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

The purpose of *Principles of Information Security*, *Seventh Edition*, is to continue to meet the need for a current, high-quality academic resource that surveys the full breadth of the information security and cybersecurity disciplines. Even today, there remains a lack of resources that provide students with a *balanced* introduction to the managerial and technical aspects of these fields. By specifically focusing our writing on the common body of knowledge, we hope to close this gap. Further, there is a clear need to include principles from criminal justice, political science, computer science, information systems, and other related disciplines to gain a clear understanding of information security and cybersecurity principles and formulate interdisciplinary solutions for system vulnerabilities. The essential tenet of this text is that information security and cybersecurity in the modern organization is a problem for management to solve, and not one that technology alone can address. In other words, an organization's information security has important economic consequences for which management will be held accountable.

Approach

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

Structure And Module Descriptions

Principles of Information Security, *Seventh Edition*, is structured to follow an approach that moves from the strategic aspects of information security to the operational—beginning with the external impetus for information security, moving through the organization's strategic approaches to governance, risk management, and regulatory compliance, and continuing with the technical and

operational implementation of security in the organization. Our use of this approach is intended to provide a supportive but not overly dominant foundation that will guide instructors and students through the information domains of information security. To serve this end, the content is organized into 12 modules.

Module 1—Introduction to Information Security

The opening module establishes the foundation for understanding the broader field of information security. This is accomplished by defining key terms, explaining essential concepts, and reviewing the origins of the field and its impact on the understanding of information security.

Module 2—The Need for Information Security

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

The module also examines the various threats facing organizations and presents methods for ranking and prioritizing these threats as organizations begin their security planning process. The module continues with a detailed examination of the types of attacks that could result from these threats, and how these attacks could affect the organization's information systems. Module 2 also provides further discussion of the key principles of information security, some of which were introduced in Module 1: confidentiality, integrity, availability, authentication, identification, authorization, accountability, and privacy.

Module 3—Information Security Management

This module presents the different management functions within the field of information security and defines information security governance. It continues with management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines. The module also explains data classification schemes, both military and private, as well as the security education, training, and awareness (SETA) program. The module concludes with discussions on information security blueprints.

Module 4—Risk Management

Before the design of a new information security solution can begin, information security analysts must first understand the current state of the organization and its relationship to information security. Does the organization have any formal information security mechanisms in place? How effective are they? What policies and procedures have been published and distributed to security managers and end users? This module explains how to conduct a fundamental information security assessment by describing procedures for identifying and prioritizing threats and assets as well as procedures for identifying what controls are in place to protect these assets from threats. The module also discusses the various types of control mechanisms and identifies the steps involved in performing the initial risk assessment. The module continues by defining risk management as the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. Module 4 concludes with a discussion of risk analysis and various types of feasibility analyses.

Module 5—Incident Response and Contingency Planning

This module examines the planning process that supports business continuity, disaster recovery, and incident response; it also describes the organization's role during incidents and specifies when the organization should involve outside law enforcement agencies. The module includes coverage of the subject of digital forensics.

Module 6—Legal, Ethical, and Professional Issues in Information Security

A critical aspect of the field is a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities that provides important insights into the regulatory constraints that govern business. This module examines several key laws that shape the field of information security and examines the computer ethics to which those who implement security must adhere. This module also presents several common legal and ethical issues found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

Module 7—Security and Personnel

The next area in the implementation stage addresses personnel issues. Module 7 examines both sides of the personnel coin: security personnel and security of personnel. It examines staffing issues, professional security credentials, and the implementation of employment policies and practices. The module also discusses how information security policy affects and is affected by consultants, temporary workers, and outside business partners.

Module 8—Security Technology: Access Controls, Firewalls, and VPNs

Module 8 provides a detailed overview of the configuration and use of technologies designed to segregate the organization's systems from the insecure Internet. This module examines the various definitions and categorizations of firewall technologies and the architectures under which firewalls may be deployed. The module discusses the rules and guidelines associated with the proper configuration and use of firewalls. Module 8 also discusses remote dial-up services and the security precautions necessary to secure access points for organizations still deploying this older technology. The module continues by presenting content filtering capabilities and considerations, and concludes by examining technologies designed to provide remote access to authorized users through virtual private networks.

Module 9—Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools

Module 9 continues the discussion of security technologies by examining the concept of intrusion and the technologies necessary to prevent, detect, react, and recover from intrusions. Specific types of intrusion detection and prevention systems (IDPSs)—the host IDPS, network IDPS, and application IDPS—and their respective configurations and uses are presented and discussed. The module examines specialized detection technologies that are designed to entice attackers into decoy systems (and thus away from critical systems) or simply to identify the attacker's entry into these decoy areas. Such systems are known as honeypots, honeynets, and padded cell systems. The discussion also examines trace-back systems, which are designed to track down the true address of attackers who were lured into decoy systems. The module then examines key security tools that information security professionals can use to monitor the current state of their organization's systems and identify potential vulnerabilities or weaknesses in the organization's overall security posture. Module 9 concludes with a discussion of access control devices commonly deployed by modern operating systems and new technologies in the area of biometrics that can provide strong authentication to existing implementations.

Module 10—Cryptography

Module 10 continues the study of security technologies by describing the underlying foundations of modern cryptosystems as well as their architectures and implementations. The module begins by summarizing the history of cryptography and discussing the various types of ciphers that played key roles in that history. The module also examines some

of the mathematical techniques that comprise cryptosystems, including hash functions. The module then extends this discussion by comparing traditional symmetric encryption systems with more modern asymmetric encryption systems and examining the role of asymmetric systems as the foundation of public-key encryption systems. Also covered are the cryptography-based protocols used in secure communications, including HTTPS, S/MIME, and SET. The module then discusses steganography and its emerging role as an effective means of hiding information. The module concludes by revisiting attacks on information security that are specifically targeted at cryptosystems.

Module 11—Implementing Information Security

The preceding modules provide guidelines for how an organization might design its information security program. Module 11 examines the elements critical to *implementing* this design. Key areas in this module include the bull's-eye model for implementing information security and a discussion of whether an organization should outsource components of its information security program. The module also discusses change management, program improvement, and additional planning for business continuity efforts.

Module 12—Information Security Maintenance

Last and most important is the discussion of maintenance and change. Module 12 describes the ongoing technical and administrative evaluation of the information security program that an organization must perform to maintain the security of its information systems. This module explores the controlled administration of changes to modern information systems to prevent the introduction of new security vulnerabilities. Special considerations needed for vulnerability analysis are explored, from Internet penetration testing to wireless network risk assessment. The module concludes with extensive coverage of physical security considerations.

Features

The following features exemplify our approach to teaching information security:

- *Information Security Professionals' Common Bodies of Knowledge*—Because the authors hold both the Certified Information Security Manager (CISM) and Certified Information Systems Security Professional (CISSP) credentials, those knowledge domains have had an influence in the design of this resource. Although care was taken to avoid producing a certification study guide, the authors' backgrounds ensure that their treatment of information security integrates the CISM and CISSP Common Bodies of Knowledge (CBKs).
- *Opening and Closing Scenarios*—Each module opens and closes with a short story that features the same fictional company as it encounters information security issues commonly found in real-life organizations. At the end of each module, a set of discussion questions provides students and instructors with opportunities to discuss the issues suggested by the story as well as offering an opportunity to explore the ethical dimensions of those issues.
- *Clearly Defined Key Terms*—Each key term is defined in a marginal note close to the term's first use. While the terms are referenced in the body of the text, the isolation of the definitions from the discussion allows a smoother presentation of the key terms and supports their standardization throughout all Whitman and Mattord works.
- *In-Depth Features*—Interspersed throughout the modules, these features highlight interesting topics and detailed technical issues, giving students the option of delving into information security topics more deeply.
- *Hands-On Learning*—At the end of each module, students will find a module summary and review questions as well as exercises. In the exercises, students are asked to research, analyze, and write responses to reinforce learning objectives, deepen their understanding of the reading, and examine the information security arena outside the classroom.

New To This Edition

- All graphics and tables are now in color.
- The newest relevant laws and industry trends are covered.
- The content on contingency planning and incident response has been significantly enhanced and moved into a module of its own to give additional emphasis to this critical topic.
- The risk management module has been updated to reflect recent industry changes in risk management methodology.
- The module that encompasses cryptography has been enhanced to include expanded coverage of blockchain and payment system security.
- Increased visibility for terminology used in the industry is provided by the prominent display of key terms throughout this resource and across the Whitman and Mattord series.
- Updated and additional "For More Information" boxes provide Web locations where students can find more information about the subjects being covered in the reading.

MindTap For *Principles of Information Security, Seventh Edition*

The complete text and supporting activities for *Principles of Information Security* are available on Cengage's MindTap platform. It gives you complete control of your course so you can provide engaging content, challenge every learner, and build student confidence. Customize interactive syllabi to emphasize high-priority topics, then add your own material or notes to the eBook as desired. This outcome-driven application gives you the tools needed to empower students and boost both understanding and performance.

Access Everything You Need in One Place

Cut down on prep with the preloaded and organized MindTap course materials. Teach more efficiently with interactive multimedia, assignments, and quizzes. Give your students the power to read, listen, and study on their phones so they can learn on their terms.

Empower Students to Reach Their Potential

Twelve distinct metrics give you actionable insights into student engagement. Identify topics that are troubling your class and instantly communicate with students who are struggling. Students can track their scores to stay motivated toward their goals. Together, you can be unstoppable.

Control Your Course—and Your Content

Get the flexibility to reorder textbook chapters, add your own notes, and embed a variety of content, including Open Educational Resources (OER). Personalize course content to your students' needs. They can even read your notes, add their own, and highlight key text to aid their learning.

Get a Dedicated Team, Whenever You Need Them

MindTap isn't just a tool; it's backed by a personalized team eager to support you. We can help set up your course and tailor it to your specific objectives, so you'll be ready to make an impact from day one. Know we'll be standing by to help you and your students until the final day of the term.

MindTap activities for Whitman and Mattord's *Principles of Information Security* are 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 you 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 "Security for Life" assignments encourage students to stay current and start practicing lifelong learning. Pre- and post-course assessments allow you to measure how much students have learned using analytics and reporting that make it easy to see where the class stands in terms of progress, engagement, and completion rates. Learn more at *www.cengage.com/mindtap/*.

Instructor Resources

Free to all instructors who adopt *Principles of Information Security* for their courses is a complete package of instructor resources accessible via single sign-on (SSO). Instructors can request an SSO account at *Cengage.com*.

Resources include the following:

- *Instructor's Manual*—This manual includes course objectives, key terms, teaching outlines and tips, quick quizzes, and additional information to help you plan and facilitate your instruction.
- *Solutions Manual*—This resource contains answers and explanations for all end-of-module review questions and exercises.
- *Cengage Testing Powered by Cognero*—A flexible, online system 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 module. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for module review, or to be printed for classroom distribution. Some tables and figures are included in the PowerPoint slides; however, all are available in the online instructor resources. Instructors are also at liberty to add their own slides.
- *Lab Exercises Available in the MindTap Edition and in the Instructor's Resource Kit (IRK)*—These exercises, written by the authors, can be used to provide technical experience in conjunction with the text. Contact your Cengage learning consultant for more information.
- *Readings and Cases*—Cengage also produced two texts by the authors—*Readings and Cases in the Management of Information Security* (ISBN-13: 9780619216276) and *Readings & Cases in Information Security: Law & Ethics* (ISBN-13: 9781435441576)—which make excellent companion texts. Contact your Cengage learning consultant for more information.
- *Curriculum Model for Programs of Study in Information Security/Cybersecurity*—In addition to the texts authored by this team, a curriculum model for programs of study in information security and cybersecurity is available from the Kennesaw State University (KSU) Institute for Cybersecurity Workforce Development (*https://cyberinstitute.kennesaw.edu/docs/ModelCurriculum-2021.pdf*). This document provides details on the authors' experiences in designing and implementing security coursework and curricula, as well as guidance and lessons learned.

Author Team

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

Michael E. Whitman, Ph.D., CISM, CISSP, is a Professor of Information Security and Assurance and the Executive Director of the KSU Institute for Cybersecurity Workforce Development (*cyberinstitute.kennesaw.edu*). Dr. Whitman is an active researcher in information security, fair and responsible use policies, ethical computing, and curriculum development methodologies. He currently teaches graduate and undergraduate courses in information security and cybersecurity management. He has published articles in the top journals in his field, including *Information Systems Research*, *Communications of the ACM*, *Information and Management*, *Journal of International Business Studies*, and *Journal of Computer Information Systems*. Dr. Whitman is also the Co-Editor-in-Chief of the *Journal of Cybersecurity Education, Research and Practice*. Dr. Whitman is also the co-author of *Management of Information Security* and *Principles of Incident Response and Disaster Recovery*, among other works, all published by Cengage. Prior to his career in academia, Dr. Whitman was an officer in the United States Army, which included duties as Automated Data Processing Systems Security Officer (ADPSSO).

Herbert J. Mattord, Ph.D., CISM, CISSP, completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner before joining the faculty of Kennesaw State University in 2002. Dr. Mattord is the Director of Education and Outreach for the KSU Institute for Cybersecurity Workforce Development (*cyberinstitute.kennesaw.edu)*. Dr. Mattord is also the Co-Editor-in-Chief of the *Journal of Cybersecurity Education, Research and Practice*. During his career as an IT practitioner, he has been an adjunct professor at Kennesaw State University, Southern Polytechnic State University in Marietta, Georgia, Austin Community College in Austin, Texas, and Texas State University: San Marcos. He currently teaches graduate and undergraduate courses in information security and cybersecurity. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this resource was acquired. Dr. Mattord is also the co-author of *Management of Information Security*, *Principles of Incident Response and Disaster Recovery*, and other works, all published by Cengage.

Acknowledgments

The authors would like to thank their families for their support and understanding for the many hours dedicated to this project—hours taken away, in many cases, from family activities.

Contributors

Several people and organizations also provided materials for this resource, and we thank them for their contributions:

- The National Institute of Standards and Technology (NIST) is the source of many references, tables, figures, and other content used in many places in the text.

Reviewers

We are indebted to the following reviewers for their perceptive feedback during the module-by-module reviews of the text:

- Paul Witman, California Lutheran University
- Mia Plachkinova, Kennesaw State University

Special Thanks

The authors thank the editorial and production teams at Cengage. Their diligent and professional efforts greatly enhanced the final product:

- Dan Seiter, Developmental Editor
- Danielle Klahr, Associate Product Manager
- Christina Nyren, Content Manager

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

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

Our Commitment

The authors are committed to serving the needs of adopters and users of this resource. We would be pleased and honored to receive feedback on the text and supporting materials. You can contact us at *infosec@kennesaw.edu*.

Foreword

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

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

I have spent 40 years of my life in a field that I found to be exciting and rewarding, working with computers and pitting my wits against malicious people, and you will too. Security controls and practices include logging on and off, using passwords, encrypting and backing up vital information, locking doors and drawers, motivating stakeholders to support security, and installing antivirus software.

These means of protection have no benefit except rarely, when adversities occur. Good security is in effect when nothing bad happens, and when nothing bad happens, who needs security? Nowadays, one reason we need security is because the law, regulations, and auditors say so—especially if we deal with the personal information of others, electronic money, intellectual property, and keeping ahead of the competition.

There is great satisfaction in knowing that your employer's information and systems are reasonably secure and that you are paid a good salary, are the center of attention in emergencies, and are applying your wits against the bad guys. This makes up for the downside of your security work. It is no job for perfectionists because you will almost never be fully successful, and there will always be vulnerabilities that you aren't aware of or that the bad guys discover first. Our enemies have a great advantage over us. They have to find only one vulnerability and one target to attack in a known place, electronically or physically at a time of their choosing, while we must defend from potentially millions of attacks against assets and vulnerabilities that are no longer in one computer room but are spread all over the world. It's like playing a game in which you don't know your opponents and where they are, what they are doing, or why they

are doing it, and they are secretly changing the rules as they play. You must be highly ethical, defensive, secretive, and cautious. Bragging about the great security you are employing might tip off the enemy. Enjoy the few successes that you experience, for you will not even know about some of them.

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

Likewise, you should use every opportunity to seek out attackers and understand what motivates their actions and how they operate. This experience gives you great cachet as a real and unique expert, even with minimal exposure to only a few enemies.

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

You must be thorough and meticulous and document everything pertinent, in case your competence is questioned and to meet the requirements of the Sarbanes–Oxley Law. Keep your documents safely locked away. Documentation is important so that when adversity hits and you lose the game, you will have proof of being diligent in spite of the loss. Otherwise, your career could be damaged, or at least your effectiveness will be diminished.

For example, if the loss occurred because management failed to give you an adequate budget and support for security you knew you required, you need to have documented that failure before the incident occurred. Don't brag about how great your security is, because it can always be beaten. Keep and expand checklists for everything: threats, vulnerabilities, assets, key potential victims, suspects of wrongdoing, security supporters and nonsupporters, attacks, enemies, criminal justice resources, auditors, regulators, and legal counsel. To assist your stakeholders, who are the front-line defenders of their information and systems, identify what they must protect and know the real extent of their security.

Make sure that upper management and other people to whom you report understand the nature of your job and its limitations.

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

One of the most exciting parts of the job is the insight you gain about the inner workings and secrets of your organization, its business, and its culture. As an information security consultant, I was privileged to learn about the culture and secrets of more than 250 of the largest corporations throughout the world. I had the opportunity to interview and advise the most powerful business executives, if only for a few minutes of their valuable time. You should always be ready with a "silver bullet," a high-impact solution to recommend in your short time with top management for the greatest benefit of enterprise security.

Carefully learn the limits of management's security appetites. Know the nature of the business, whether it is a government department or a hotly competitive business. I once found myself in a meeting with a board of directors intensely discussing the protection of their greatest trade secret, the manufacturing process of their new disposable diapers.

Finally, we come to the last important bit of advice. Be trustworthy and develop mutual trust among your peers. Your most important objectives are not just risk reduction and increased security. They also include diligence to avoid negligence and endangerment, compliance with all of the laws and standards, and enablement when security becomes a competitive or budget issue. To achieve these objectives, you must develop a trusting exchange of the most sensitive security intelligence among your peers so you'll know where your organization stands relative to other enterprises. But be discreet and careful about it. You need to know the generally accepted and current security solutions. If the information you exchange is exposed, it could ruin your career and others, and could create a disaster for your organization. Your personal and ethical performance must be spotless, and you must protect your reputation at all costs.

Pay particular attention to the ethics section of this resource. I recommend that you join the Information Systems Security Association, become active in it, and become professionally certified as soon as you are qualified. My favorite certification is the Certified Information Systems Security Professional (CISSP) from the International Information System Security Certification Consortium.

Donn B. Parker, CISSP Retired
Sunnyvale, California

MODULE 1

Introduction to Information Security

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

1. Define information security
2. Discuss the history of computer security and explain how it evolved into information security
3. Define key terms and critical concepts of information security
4. Describe the information security roles of professionals within an organization

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

—The Book of Five Rings

Opening Scenario

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

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

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

"Sure did, Amy. But now I have another issue I need your help with."

"Sure, Bob. Tell me about it."

"Well, my PC is acting weird," Bob said. "When I open my e-mail app, my mailbox doesn't respond to the mouse or the keyboard."

"Did you try a reboot yet?"

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

"OK, Bob. We've tried the usual stuff we can do over the phone. Let me open a case, and I'll have a tech contact you for remote diagnosis as soon as possible."

Amy looked up at the help desk ticket status monitor on the wall at the end of the room. She saw that only two technicians were currently dispatched to user support, and because it was the day shift, four technicians were available. "Shouldn't be long at all, Bob."

She hung up and typed her notes into the company's trouble ticket tracking system. She assigned the newly generated case to the user dispatch queue, which would page the user support technician with the details in a few minutes.

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

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

After that click, her PC showed the Windows "please wait" cursor for a second and then the mouse pointer reappeared. Nothing happened. She clicked the next e-mail message in the queue. Nothing happened. Her phone rang again. She clicked the icon on her computer desktop to activate the call management software and activated her headset. "Hello, Help Desk, how can I help you?" She couldn't greet the caller by name because her computer had not responded.

"Hello, this is Erin Williams in Receiving."

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

"Hi, Erin," Amy said. "What's up?"

"Nothing," Erin answered. "That's the problem." The rest of the call was a replay of Bob's, except that Amy had to jot notes down on a legal pad. She couldn't notify the user support team either. She looked at the ticket status monitor again. It had gone dark. No numbers at all.

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

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

Introduction To Information Security

Every organization, whether public or private and regardless of size, has information it wants to protect. It could be customer information, product or service information, and/or employee information. Regardless of the source, it is the organization's job to protect the information to the best of its ability. Organizations have a responsibility to all its stakeholders to protect that information. Unfortunately, there aren't enough security professionals to go around. As a result, everyone in the organization must have a working knowledge of how to protect the information assigned to them and how to assist in preventing the unauthorized disclosure, damage, or destruction of that information. After all, if you're not part of the solution, you're part of the problem.

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

The history of information security begins with the concept of **computer security**. The need for computer security arose during World War II when the first mainframe computers were developed and used to aid computations for communication code-breaking messages from enemy cryptographic devices like the Enigma, shown in Figure 1-1. Multiple levels of security were implemented to protect these devices and the missions they served. This required new processes as well as tried-and-true methods needed to maintain data confidentiality. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and technologically sophisticated computer security safeguards.

computer security

In the early days of computers, this term specified the protection of the physical location and assets associated with computer technology from outside threats, but it later came to represent all actions taken to protect computer systems from losses.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on a MOTD (message of the day) file while another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed to every output file.[1]

The 1960s

During the Cold War, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks. These mainframes required a less cumbersome process of communication than mailing magnetic tapes between computer centers. In response to this need, the U.S. Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. In 1968, Dr. Larry Roberts developed the ARPANET project, which evolved into what we now know as the Internet. Figure 1-2 is an excerpt from his program plan.

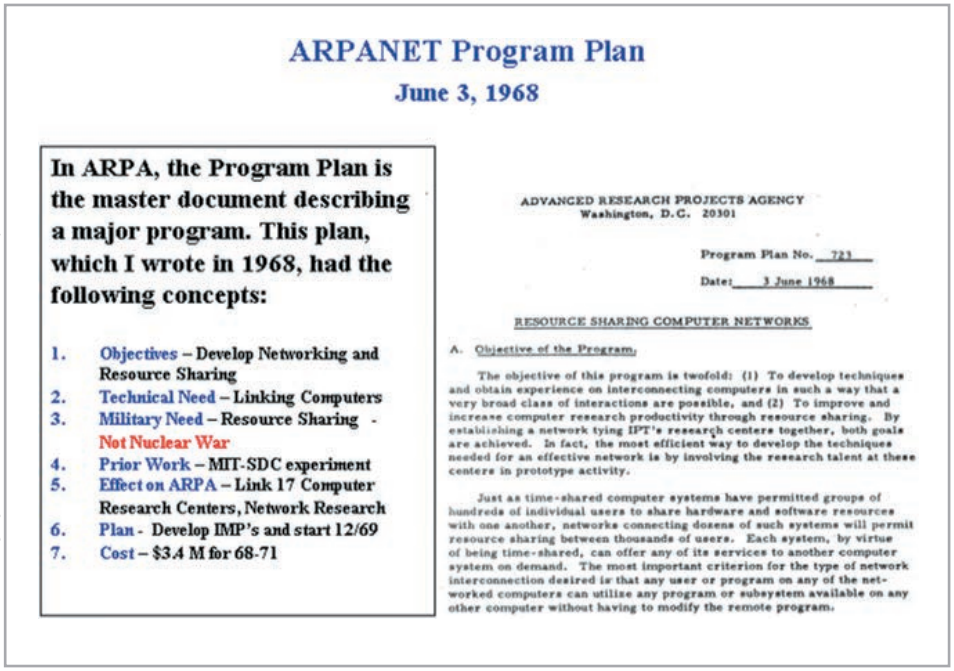
For more information on Dr. Roberts, including links to his recorded presentations, visit the Internet Hall of Fame at *www.internethalloffame.org/inductees/lawrence-roberts*.

© kamilpetran/Shutterstock.com

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

Source: © kamilpetran/Shutterstock.com.[2]

Figure 1-1 The Enigma



Source: Courtesy of Dr. Lawrence Roberts. Used with permission.[3]

Figure 1-2 Development of the ARPANET

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

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

The 1970s and '80s

During the next decade, ARPANET became more popular and saw wider use, increasing the potential for its misuse. In 1973, Internet pioneer Robert M. Metcalfe (pictured in Figure 1-3) identified fundamental problems with ARPANET security. As one of the creators of Ethernet, a dominant local area networking protocol, he knew that individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded, including vulnerability of password structure and formats, lack of safety procedures for dial-up connections, and nonexistent user identification and authorizations. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was commonly referred to as network insecurity.[4] For a timeline that includes seminal studies of computer security, see Table 1-1.

Security that went beyond protecting physical computing devices and their locations effectively began with a single paper published by the RAND Corporation in February 1970 for the Department of Defense. RAND Report R-609 attempted to define the multiple controls and mechanisms necessary for the protection of a computerized data processing system. The document was classified for almost 10 years, and is now considered to be the paper that started the study of computer security.

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

Table 1-1 Key Dates in Information Security

Date	Document
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems*.
1970	Willis H. Ware authors the report "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security—RAND Report R-609," which was not declassified until 1979. It became known as the seminal work identifying the need for computer security.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in *Preliminary Notes on the Design of Secure Military Computer Systems.*
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the *Federal Register*.
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[5]
1979	Morris and Thompson author "Password Security: A Case History," published in the *Communications of the Association for Computing Machinery* (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system. Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1984	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report, the authors examined four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[6] Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore, no technique can be secure against the system administrator or other privileged users . . . the naive user has no chance."[7]
1992	Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

In June 1967, ARPA formed a task force to study the process of securing classified information systems. The task force was assembled in October 1967 and met regularly to formulate recommendations, which ultimately became the contents of RAND Report R-609. The document was declassified in 1979 and released as *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security—RAND Report R-609-1*.[8] The content of the two documents is identical with the exception of two transmittal memorandums.

For more information on the RAND Report, visit www.rand.org/pubs/reports/R609-1.html.

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

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

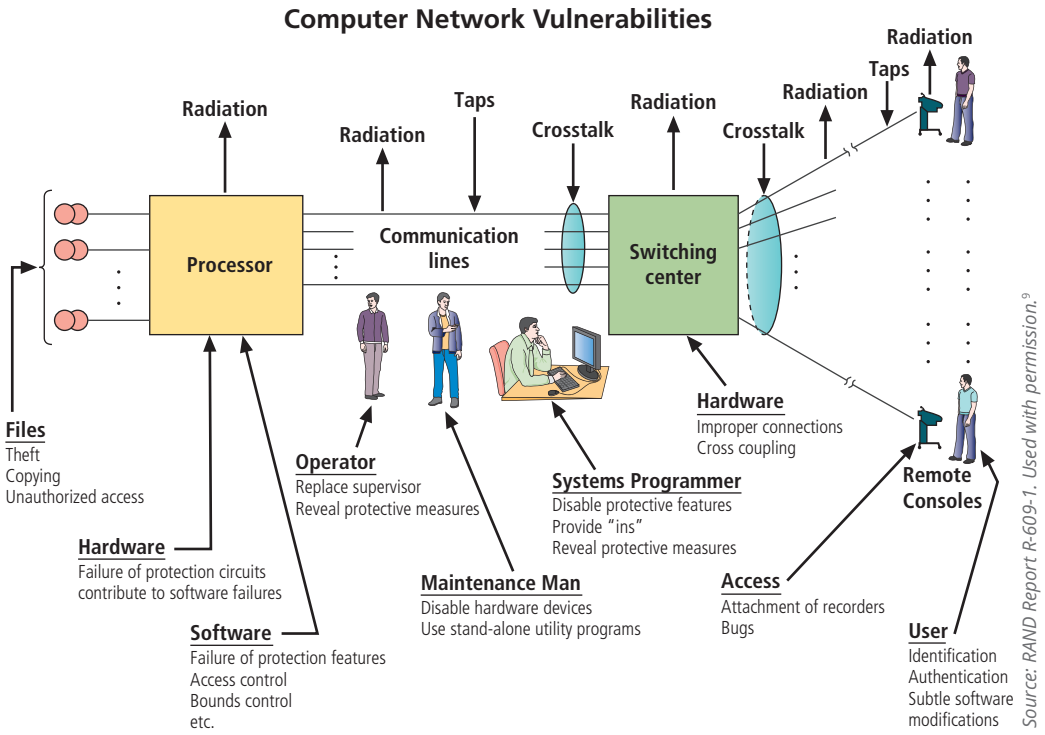


Figure 1-4 Illustration of computer network vulnerabilities from RAND Report R-609

MULTICS

Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS). Although it is now obsolete, MULTICS is noteworthy because it was the first operating system to integrate security into its core functions. It was a mainframe, time-sharing operating system developed in the mid-1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).

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

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

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

In the early 1980s, TCP (the Transmission Control Protocol) and IP (the Internet Protocol) were developed and became the primary protocols for the ARPANET, eventually becoming the protocols used on the Internet to this day. During the same time frame, the hierarchical Domain Name System, or DNS, was developed. The first dial-up Internet service provider (ISP)—The World, operated by Standard Tool & Die—came online, allowing home users to access the Internet. Prior to that, vendors like CompuServe, GEnie, Prodigy, and Delphi had provided dial-up access for online computer services, while independent bulletin board systems (BBSs) became popular for sharing information among their subscribers.

For more information on the history of the Internet, visit *www.livescience.com/20727-internet-history.html*.

In the mid-1980s, the U.S. government passed several key pieces of legislation that formalized the recognition of computer security as a critical issue for federal information systems. The Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987 defined computer security and specified responsibilities and associated penalties. These laws and others are covered in Module 6.

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

The 1990s

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

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

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

In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations. Antivirus products became extremely popular, and information security began to emerge as an independent discipline.

2000 to Present

Today, the Internet brings millions of unsecured computer networks and billions of computer systems into continuous communication with each other. The security of each computer's stored information is contingent on the security level of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. Other growing concerns are the threat of countries engaging in information warfare and the possibility that business and personal information systems could become casualties if they are undefended. Since 2000, Sarbanes–Oxley and other laws related to privacy and corporate responsibility have affected computer security.

The attack on the World Trade Centers on September 11, 2001, resulted in major legislation changes related to computer security, specifically to facilitate law enforcement's ability to collect information about terrorism. The USA PATRIOT Act of 2001 and its follow-up laws are discussed in Module 6.

The 21st century also saw the massive rise in mobile computing, with smartphones and tablets possessing more computing power than early-era mainframe systems. Embedded devices have seen the creation of computing built into everyday objects in the Internet of Things (IoT). Each of these networked computing platforms brings its own set of security issues and concerns as they are connected into networks with legacy platforms and cloud-based service delivery systems. Technology that is supposed to be seamless turns out to have many connection points, each with its

own set of security and reliability vulnerabilities. The emergence of tools to deal with now-routine threats at large scale has led to the development of complete solutions for unified threat management, data loss prevention, and security information and event management. The solutions will be explored in more detail in later modules.

Wireless networking, and the risks associated with it, has become ubiquitous and pervasive, with widely available connectivity providing ready access to the Internet as well as local networks that are usually ill-prepared for access by the public. This opens the local net as well as the Internet to a constant threat of anonymous attacks from very large numbers of people and devices.

The threat environment has grown from the semiprofessional hacker defacing Web sites for amusement to professional cybercriminals maximizing revenue from theft and extortion, as well as government-sponsored cyberwarfare groups striking military, government, and commercial targets by intent and by opportunity. The attack sources of today are well-prepared and are attacking all connected public and private systems and users.

What Is Security?

Security is protection. Protection from adversaries—those who would do harm, intentionally or otherwise—is the ultimate objective of security. National security, for example, is a multilayered system that protects the sovereignty of a state, its people, its resources, and its territory. Achieving the appropriate level of security for an organization also requires a multifaceted system. A successful organization should have multiple layers of security in place to protect its people, operations, physical infrastructure, functions, communications, and information.

The Committee on National Security Systems (CNSS) defines **information security** as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information.[10] Figure 1-5 shows that information security includes the broad areas of information security management, data security, and **network security**. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triad. The **C.I.A. triad** (see Figure 1-6) has been the standard for computer security in both industry and government since the development of the mainframe. This standard is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics is as important today as it has always been, but the C.I.A. triad model is generally viewed as no longer adequate in addressing the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This vast array of

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

information security
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.

network security
A subset of communications security; the protection of voice and data networking components, connections, and content.

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

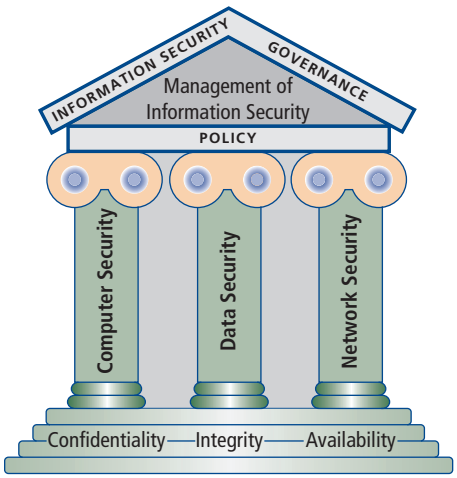


Figure 1-5 Components of information security

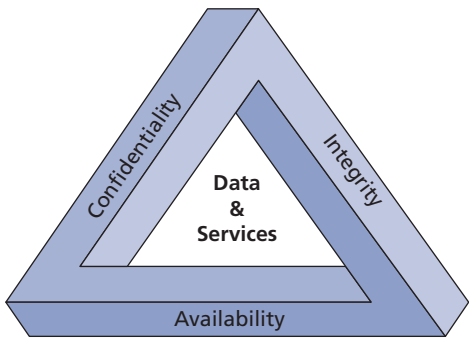


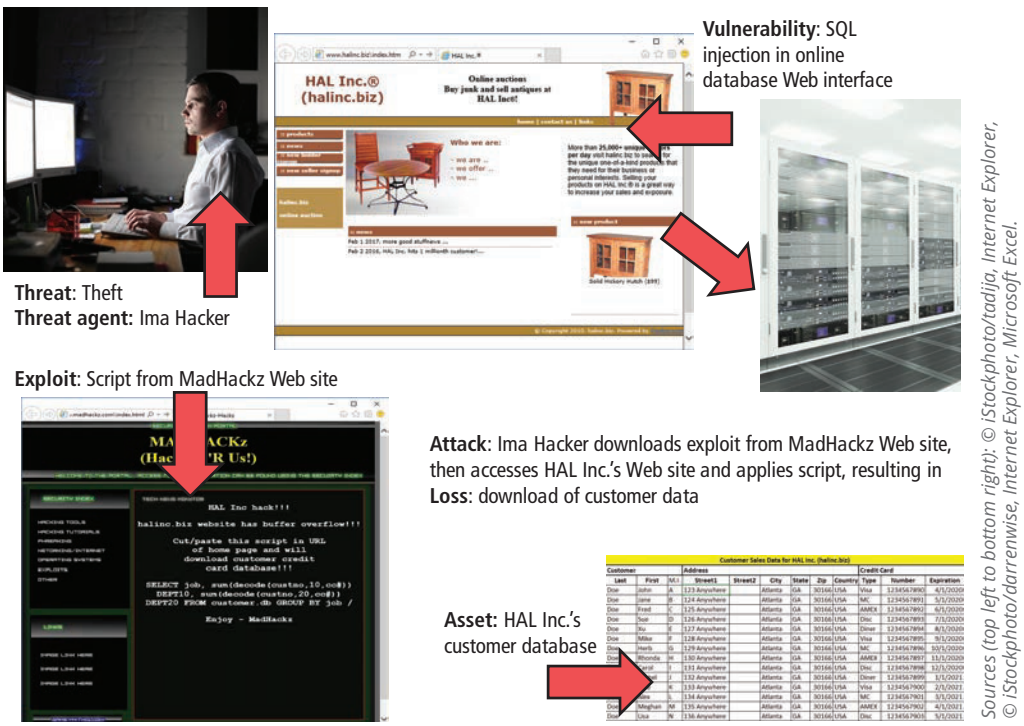
Figure 1-6 The C.I.A. triad

constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment. The expanded model consists of a list of critical characteristics of information, which are described in the next section. C.I.A. triad terminology is used in this module because of the breadth of material that is based on it.

Key Information Security Concepts

This book uses many terms and concepts that are essential to any discussion of information security. Some of these terms are illustrated in Figure 1-7; all are covered in greater detail in subsequent modules.

- **Access**—A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers must gain illegal access to a system. Access controls regulate this ability.
- **Asset**—The 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.
- **Attack**—An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone who casually reads sensitive information not intended for his or her use is committing a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a building fire is an unintentional attack. A direct attack is perpetrated by a hacker using a PC to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems—for example, as part of a botnet (slang for *robot network*). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.



Sources (top left to bottom right): © iStockphoto/tadija, Internet Explorer, © iStockphoto/darrenwise, Internet Explorer, Microsoft Excel.

Figure 1-7 Key concepts in information security

- **Control, safeguard, or countermeasure**—Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The various levels and types of controls are discussed more fully in the following modules.
- **Exploit**—A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or created by the attacker. Exploits make use of existing software tools or custom-made software components.
- **Exposure**—A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker.
- **Loss**—A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. When an organization's information is stolen, it has suffered a loss.
- **Protection profile** or **security posture**—The entire set of controls and safeguards—including policy, education, training and awareness, and technology—that the organization implements to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although a security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.
- **Risk**—The probability of an unwanted occurrence, such as an adverse event or loss. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk they are willing to accept.
- **Subjects** and **objects of attack**—A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity. See Figure 1-8. A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other systems (subject).
- **Threat**—Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*. The two terms are technically distinct, but to simplify discussion, the text will continue to use the term *threat* to describe threat sources.
- **Threat agent**—The specific instance or a component of a threat. For example, the threat source of "trespass or espionage" is a category of potential danger to information assets, while "external professional hacker" (like Kevin Mitnick, who was convicted of hacking into phone systems) is a specific threat agent. A lightning strike, hailstorm, or tornado is a threat agent that is part of the threat source known as "acts of God/acts of nature."

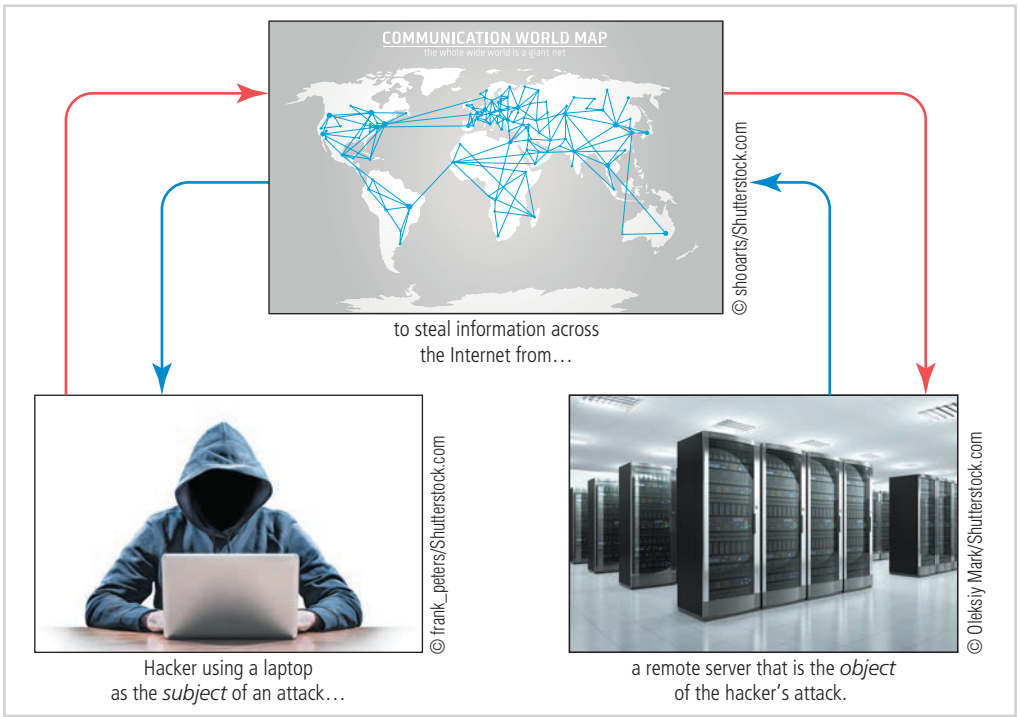


Figure 1-8 Computer as the subject and object of an attack

- **Threat event**—An occurrence of an event caused by a threat agent. An example of a threat event might be damage caused by a storm. This term is commonly used interchangeably with the term *attack*.
- **Threat source**—A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents. Threat sources are always present and can be purposeful or undirected. For example, threat agent "hackers," as part of the threat source "acts of trespass or espionage," purposely threaten unprotected information systems, while threat agent "severe storms," as part of the threat source "acts of God/acts of nature," incidentally threaten buildings and their contents.
- **Vulnerability**—A potential weakness in an asset or its defensive control system(s). Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

Critical Characteristics of Information

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases or, more commonly, decreases. Some characteristics affect information's value to users more than others, depending on circumstances. For example, timeliness of information can be a critical factor because information loses much or all of its value when delivered too late. Though information security professionals and end users share an understanding of the characteristics of information, tensions can arise when the need to secure information from threats conflicts with the end users' need for unhindered access to it. For instance, end users may perceive two-factor authentication in their login—which requires an acknowledgment notification on their smartphone—to be an unnecessary annoyance. Information security professionals, however, may consider two-factor authentication necessary to ensure that only authorized users access the organization's systems and data. Each critical characteristic of information—that is, the expanded C.I.A. triad—is defined in the following sections.

Confidentiality

Confidentiality ensures that *only* users with the rights, privileges, and need to access information are able to do so. When unauthorized individuals or systems view information, its confidentiality is breached. To protect the confidentiality of information, you can use several measures, including the following:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users

Confidentiality, like most characteristics of information, is interdependent with other characteristics and is closely related to the characteristic known as privacy. The relationship between these two characteristics is covered in more detail in Module 6. The value of confidentiality is especially high for personal information about employees, customers, or patients. People who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, a healthcare facility, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but disclosure of confidential information also happens by mistake—for example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* it.

confidentiality

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

Other examples of confidentiality breaches include an employee throwing away a document that contains critical information without shredding it, or a hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about its clients, such as names, addresses, and credit card numbers.

As a consumer, you give up pieces of personal information in exchange for convenience or value almost daily. By using a "members" card at a grocery store, you disclose some of your spending habits. When you fill out an online survey, you exchange pieces of your personal history for access to online privileges. When you sign up for a free magazine, Web resource, or free software application, you provide **personally identifiable information (PII)**. The bits and pieces of personal information you

personally identifiable information (PII)

Information about a person's history, background, and attributes that can be used to commit identity theft; typically includes a person's name, address, Social Security number, family information, employment history, and financial information.

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

disclose may be copied, sold, replicated, distributed, and eventually coalesced into profiles and even complete dossiers of you and your life.

Integrity

Information has **integrity** when it is in its expected state and can be trusted. 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 stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity, as shown by the file size. Another key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the bit values in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique.

If a computer system performs the same hashing algorithm on a file and obtains a different number than the file's recorded hash value, the file has been compromised and the integrity of the information is lost. Information integrity is the cornerstone of information systems because information is of no value or use if users cannot verify its integrity. File hashing and hash values are examined in detail in Module 10.

File corruption is not necessarily the result of external forces, such as hackers. Noise in the transmission media, for instance, can also cause data to lose its integrity. Transmitting data on a circuit with a low voltage level can alter and corrupt the data. Redundancy bits and check bits can compensate for internal and external threats to the integrity of information. During each transmission, algorithms, hash values, and error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted.

Unfortunately, even the routine use of computers can result in unintended changes to files as the equipment degrades, software malfunctions, or other "natural causes" occur.

Unintentional Disclosures

The number of unintentional information releases due to malicious attacks is substantial. Millions of people lose information to hackers and malware-focused attacks annually. However, organizations occasionally lose, misplace, or inadvertently release information in an event not caused by hackers or other electronic attacks.

In 2020, Virgin Media, a communications company, left more than 900,000 users' information unsecured for almost a year after one of its databases was misconfigured by employees. Also in 2020, more than 5.2 million customers of Marriott International were exposed in a data breach resulting from the misuse of two employees' credentials. This disclosure occurred not two years after Marriott's reservation database was breached, exposing more than 383 million guests and resulting in the loss of more than five million passport numbers.[11]

The Georgia Secretary of State gave out more than six million voters' private information, including Social Security numbers, in a breach that occurred in late 2015. The breach was found to have been caused by an employee who failed to follow established policies and procedures, and resulted in the employee being fired. While the agency claimed it recovered all copies of the data that were sent to 12 separate organizations, it was still considered a data breach.

In January 2008, GE Money, a division of General Electric, revealed that a data backup tape with credit card data from approximately 650,000 customers and more than 150,000 Social Security numbers went missing from a records management company's storage facility. Approximately 230 retailers were affected when Iron Mountain, Inc., announced it couldn't find a magnetic tape.[12]

In February 2005, the data aggregation and brokerage firm ChoicePoint revealed that it had been duped into releasing personal information about 145,000 people to identity thieves in 2004. The perpetrators used stolen identities to create ostensibly legitimate business entities, which then subscribed to ChoicePoint to acquire the data fraudulently. The company reported that the criminals opened many accounts and recorded personal information, including names, addresses, and identification numbers. They did so without using any network or computer-based attacks; it was simple fraud. The fraud was feared to have allowed the perpetrators to arrange hundreds of identity thefts.

The giant pharmaceutical organization Eli Lilly and Co. released the e-mail addresses of 600 patients to one another in 2001. The American Civil Liberties Union (ACLU) denounced this breach of privacy, and information technology industry

analysts noted that it was likely to influence the public debate on privacy legislation. The company claimed the mishap was caused by a programming error that occurred when patients who used a specific drug produced by Lilly signed up for an e-mail service to access company support materials.

These are but a few of the multitudes of data breaches that occur regularly in the world, day in and day out. Wikipedia maintains a list of the more well-known breaches at *https://en.wikipedia.org/wiki/List_of_data_breaches*.

For more details on information losses caused by attacks, visit Wikipedia.org and search on the terms "data breach" and "timeline of computer security hacker history."

Availability

Availability enables authorized users—people or computer systems—to access information without interference or obstruction and to receive it in the required format. Consider, for example, research libraries that require identification before entrance. Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron's identification before the patron has free access to the book stacks. Once authorized patrons have access to the stacks, they expect to find the information they need in a usable format and familiar language. In this case, the information is bound in a book that is written in English.

Accuracy

Information has **accuracy** when it is free from mistakes or errors and has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider a checking account, for example. You assume that the information in your account is an accurate representation of your finances. Incorrect information in the account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much money from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make other mistakes, such as bouncing a check that overdraws your account.

Authenticity

Information is **authentic** when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know its origin. This is not always the case. E-mail spoofing, the act of sending an e-mail message with a modified field, is a problem for many people today because the modified field often is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that the messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have.

Utility

The **utility** of information is its usefulness. In other words, information has value when it can serve a purpose. If information is available but is not in a meaningful format to the end user, it is not useful. For example, U.S. Census data can quickly become overwhelming and difficult for a private citizen to interpret; however, for a politician, the same data reveals information about residents in a district—such as their race, gender, and age. This information can help form a politician's campaign strategy or shape their policies and opinions on key issues.

Possession

The **possession** of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach

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

accuracy
An attribute of information that describes how data is free of errors and has the value that the user expects.

authenticity
An attribute of information that describes how data is genuine or original rather than reproduced or fabricated.

utility
An attribute of information that describes how data has value or usefulness for an end purpose.

possession
An attribute of information that describes how the data's ownership or control is legitimate or authorized.

McCumber Cube

A graphical representation of the architectural approach used in computer and information security; commonly shown as a cube composed of 3×3×3 cells, similar to a Rubik's Cube.

of possession, a breach of possession does not always lead to a breach of confidentiality. For example, assume a company stores its critical customer data using an encrypted file system. An employee who has quit decides to take a copy of the tape backups and sell the customer records to the competition. The removal of the tapes from their secure environment is a breach of possession. Because the data is encrypted, neither the former employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach of confidentiality. Today, people who are caught selling company secrets face increasingly stiff fines and a strong likelihood of jail time. Also, companies are growing more reluctant to hire people who have demonstrated dishonesty in their past. Another example might be that of a ransomware attack in which a hacker encrypts important information and offers to provide the decryption key for a fee. The attack would result in a breach of possession because the owner would no longer have possession of the information.

CNSS Security Model

The definition of information security in this text is based in part on the National Training Standard for Information Systems Security Professionals, NSTISSI No. 4011 (1994). The hosting organization is CNSS, which is responsible for coordinating the evaluation and publication of standards related to the protection of National Security Systems (NSS). CNSS was originally called the National Security Telecommunications and Information Systems Security Committee (NSTISSC) when established in 1990 by National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*. The outdated CNSS standards are expected to be replaced by a newer document from the National Institute of Standards and Technology (NIST) called Special Publication (SP) 800-16 Rev. 1 (2014), "A Role-Based Model for Federal Information Technology/Cyber Security Training," in the near future.

For more information on CNSS and its standards, see *www.cnss.gov/CNSS/issuances/Instructions.cfm*.

The model, which was created by John McCumber in 1991, provides a graphical representation of the architectural approach widely used in computer and information security; it is now known as the **McCumber Cube**.[13] As shown in Figure 1-9, the McCumber Cube shows three dimensions. When extrapolated, the three dimensions of each axis become a 3×3×3 cube with 27 cells representing areas that must be addressed to secure today's information systems. To ensure comprehensive system security, each of the 27 areas must be properly addressed. For example, the intersection of technology, integrity, and storage requires a set of controls or safeguards that address the need to use *technology* to protect the *integrity* of information while in *storage*. One such control might be a system for detecting host intrusion that protects the integrity of information by alerting security administrators to the potential

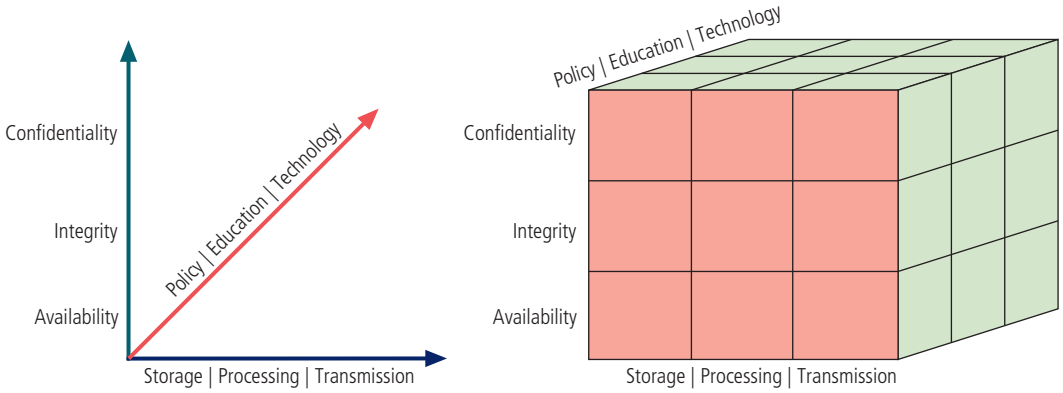


Figure 1-9 The McCumber Cube[14]

modification of a critical file. A common omission from such a model is the need for guidelines and policies that provide direction for the practices and implementations of technologies. The need for policy is discussed in subsequent modules of this book.

Components Of An Information System

As shown in Figure 1-10, an **information system (IS)** is much more than computer hardware and software; it includes multiple components, all of which work together to support personal and professional operations. Each of the IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the IS also has its own security requirements.

Software

The software component of an IS includes applications (programs), operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The IT industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.

Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, costs, and manpower. Information security is all too often implemented as an afterthought rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

information system (IS)

The entire set of software, hardware, data, people, procedures, and networks that enable the use of information resources in the organization.

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. **Physical security** policies deal with hardware as a physical

physical security

The protection of material items, objects, or areas from unauthorized access and misuse.

Figure 1-10 Components of an information system

asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted hardware access is possible.

Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices. The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind until the target placed the computer on the baggage scanner. As the computer was whisked through, the second perpetrator slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.

While the security response to September 11 did tighten the security process at airports, hardware can still be stolen in offices, coffee houses, restaurants, and other public places. Although laptops and notebook computers might be worth a few thousand dollars, the information stored on them can be worth a great deal more to disreputable organizations and individuals. Consider that unless plans and procedures are in place to quickly revoke privileges on stolen devices like laptops, tablets, and smartphones, the privileged access that these devices have to cloud-based data stores could be used to steal information that is many times more valuable than the device itself.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When used properly, they should improve the security of the data and the applications that rely on the data. Unfortunately, many system development projects do not make full use of a database management system's security capabilities, and in some cases, the database is implemented in ways that make it less secure than traditional file systems. Because data and information exist in physical form in many organizations as paper reports, handwritten notes, and computer printouts, the protection of physical information is as important as the protection of electronic, computer-based information. As an aside, the terms *data* and *information* are used interchangeably today. Information was originally defined as *data with meaning,* such as a report or statistical analysis. For our purposes, we will use the term *information* to represent both unprocessed data and actual information.

People

Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C., a great army threatened the security and stability of the Chinese empire. So ferocious were the Hun invaders that the Chinese emperor commanded the construction of a great wall that would defend against them. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for more than a thousand years. Initially, the Khan's army tried to climb over, dig under, and break through the wall. In the end, the Khan simply bribed the gatekeeper—and the rest is history.

Whether this event actually occurred or not, the timeless moral to the story is that people can be the weakest link in an organization's information security program. Unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate people to obtain access information about a system. This topic is discussed in more detail in Module 2.

Procedures

Procedures are another frequently overlooked component of an IS. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, it poses a threat to the integrity of the information. For example, a consultant to a bank learned how to wire funds by using the computer center's

procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), the bank consultant ordered millions of dollars to be transferred by wire to his own account. Lax security procedures caused the loss of more than $10 million before the situation was corrected. Most organizations distribute procedures to employees so they can access the information system, but many of these companies often fail to provide proper education for using the procedures safely. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of an organization on a need-to-know basis.

Networks

Networking is the IS component that moves data and information between the components of the information system and has created much of the need for increased computer and information security. Prior to networking, physical security was the dominant focus when protecting information. When information systems are connected to each other to form LANs, and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. Networking technology is accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to the system's hardware components is still important. However, when computer systems are networked, this approach is no longer enough. Steps to provide network security such as installing and configuring firewalls are essential, as is implementing intrusion detection systems to make system owners aware of ongoing compromises.

The definition of what an information system is and the roles that it plays has been getting some attention in industry and academia. As information systems have become the core elements of most organizations' ongoing operations, do they still need to be considered anything other than the way companies do all of their business?

For another view of what makes an information system, and to better understand how we might approach improving its security, you can read this article at Technopedia: *www.techopedia.com/definition/24142/information-system-is*.

Security And The Organization

Security has to begin somewhere in the organization, and it takes a wide range of professionals to support a diverse information security program. The following sections discuss the development of security as a program and then describe typical information security responsibilities of various professional roles in an organization.

Balancing Information Security and Access

Even with the best planning and implementation, it is impossible to obtain perfect information security. Information security cannot be absolute: It is a process, not a goal. You can make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information. On the other hand, a completely secure information system would not allow anyone access. To achieve balance—that is, to operate an information system that satisfies users and security professionals—the security level must allow reasonable access yet protect against threats. Figure 1-11 shows some of the competing voices that must be considered when balancing information security and access.

Because of today's security concerns and issues, an information system or data processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by obsessive focus on protecting and administering the information systems. Information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure that data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after addressing concerns about loss, damage, interception, or destruction.

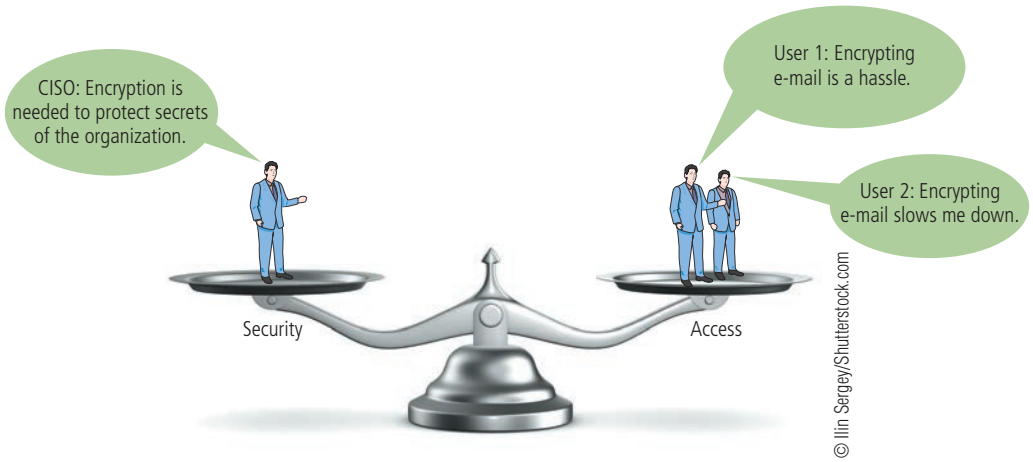


Figure 1-11 Balancing information security and access

Approaches to Information Security Implementation

The implementation of information security in an organization must begin somewhere and cannot happen overnight. Securing information assets is an incremental process that requires coordination, time, and patience. Information security can begin as an attempt by systems administrators to improve the security of their systems by working together. This is often referred to as a **bottom-up approach**. The key advantage of the bottom-up approach is the technical expertise of individual administrators. By working with information systems on a day-to-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, the bottom-up approach seldom works because it lacks critical features such as participant support and organizational staying power.

The **top-down approach** has a higher probability of success. With this approach, the project is formally designed and supported by upper-level managers who issue policies, procedures, and processes, dictate the goals and expected outcomes, and determine accountability for each required action. This approach has strong upper management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy known as a systems development life cycle.

For any organization-wide effort to succeed, management must buy into and fully support it. The role of the champion—typically an executive such as a chief information officer (CIO) or the vice president of information technology (VP-IT)—in this effort cannot be overstated. The champion moves the project forward, ensures that it is properly managed, and pushes for acceptance throughout the organization. Without this high-level support, many mid-level administrators fail to make time for the project or dismiss it as a low priority. The involvement and support of end users is also critical to the success of this type of project. Users are most directly affected by the process and outcome of the project and must be included in the information security process. Key end users should be assigned to a joint application development (JAD) team. To succeed, the JAD must have staying power. It must be able to survive employee turnover and should not be vulnerable to changes in the personnel team that is developing the information security system. This means the processes and procedures must be documented and integrated into the organizational culture. They must be adopted and promoted by the organization's management.

bottom-up approach

A method of establishing security policies and/or practices that begins as a grassroots effort in which systems administrators attempt to improve the security of their systems.

top-down approach

A methodology of establishing security policies and/or practices that is initiated by upper management.

The organizational hierarchy and its relationship to the bottom-up and top-down approaches are illustrated in Figure 1-12.

Security Professionals

Because information security is best initiated from the top down, senior management is the key component and the vital force for a successful implementation of an information security program. However, administrative support is also essential to developing and executing specific security policies and procedures, and of course, technical expertise is essential to implementing the details of the information security program.

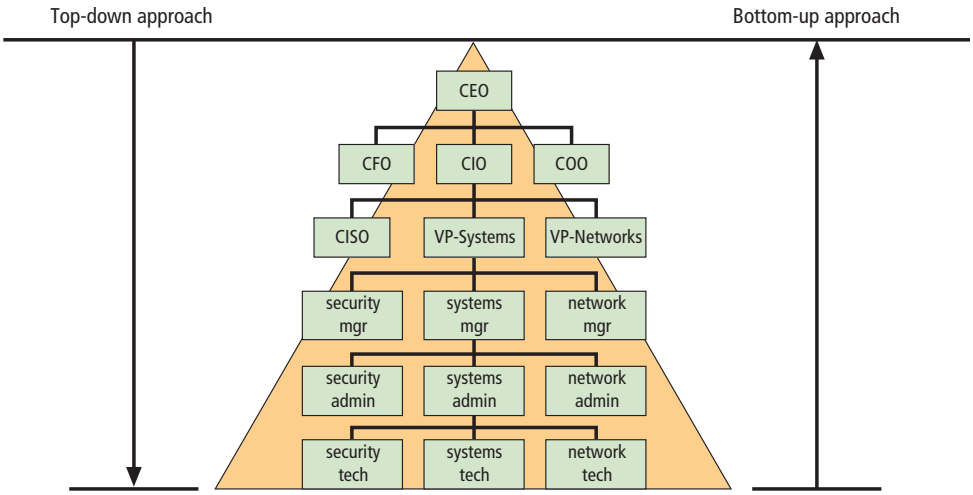


Figure 1-12 Approaches to information security implementation

Senior Management

The senior technology officer is typically the **chief information officer (CIO)**, although other titles such as vice president of information, VP of information technology, and VP of systems may be used. The CIO is primarily responsible for advising the chief executive officer, president, or company owner on strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the entire organization into strategic information plans for the information systems or information technology division of the organization. Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

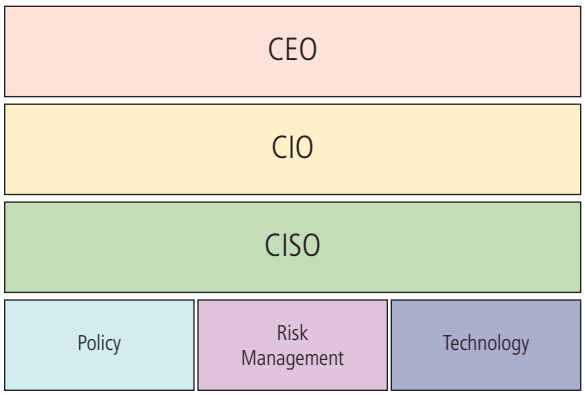


Figure 1-13 The CISO's place and roles

The **chief information security officer (CISO)** has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or by a similar title. The CISO usually reports directly to the CIO, although in larger organizations, one or more layers of management might exist between the two. However, the recommendations of the CISO to the CIO must be given equal if not greater priority than other technology and information-related proposals. The most common placement of CISOs in organizational hierarchies, along with their assigned roles and responsibilities, is illustrated in Figure 1-13. Note that the placement and accountabilities of the CISO have been the subject of debate across the industry for decades.[15]

chief information officer (CIO)

An executive-level position that oversees the organization's computing technology and strives to create efficiency in the processing and access of the organization's information.

chief information security officer (CISO)

The title typically assigned to the top information security manager in an organization.

An emerging trend is the "Virtual CISO." Many consulting organizations are offering this as a service to clients as a means to gain the advantages of having a CISO's perspective on solving security problems without the complexities and expense of hiring a dedicated executive.

You can look into what a vCISO is and does with a short reading session on the Web. Start with an article by Doug Drinkwater from *CSO Magazine* at *www.csoonline.com/article/3259926/what-is-a-virtual-ciso-when-and-how-to-hire-one.html*.

Information Security Project Team

The information security project team should consist of people who are experienced in one or multiple facets of the required technical and nontechnical areas. Many of the same skills needed to manage and implement security are also needed to design it. Members of the team fill the following roles:

- *Champion*—A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization
- *Team leader*—A project manager who may also be a departmental line manager or staff unit manager, and who understands project management, personnel management, and information security technical requirements
- *Security policy developers*—People who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies
- *Risk assessment specialists*—People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used
- *Security professionals*—Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint
- *Systems administrators*—People with the primary responsibility for administering systems that house the information used by the organization
- *End users*—Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

The four types of data ownership and their respective responsibilities are outlined here:

data owners
Individuals who control, and are therefore ultimately responsible for, the security and use of a particular set of information.

data custodians
Individuals who are responsible for the storage, maintenance, and protection of information.

data stewards
See *data custodians*.

data trustees
Individuals who are assigned the task of managing a particular set of information and coordinating its protection, storage, and use.

data users
Internal and external stakeholders (customers, suppliers, and employees) who interact with information in support of their organization's planning and operations.

- *Data owners*—**Data owners** usually determine the level of data classification as well as the changes to that classification required by organizational change. The data owners work with subordinate managers to oversee the day-to-day administration of the data.
- *Data custodians*—Working directly with data owners, **data custodians** (also known as **data stewards**) are responsible for the information and the systems that process, transmit, and store it. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.
- *Data trustees*—**Data trustees** are individuals appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use. Because data owners are typically top-level executives and managers too busy to oversee the management of their data, they will typically appoint a senior subordinate as a data trustee to handle those responsibilities.
- *Data users*—Everyone in the organization is responsible for the security of data, so **data users** are included here as all individuals or end users with access to information and thus an information security role.

Communities of Interest

community of interest
A group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives.

Each organization develops and maintains its own unique culture and values. Within each organizational culture, one or more **communities of interest** usually develop and evolve. While an organization can have many different communities of interest,

this book identifies the three that are most common and that have roles and responsibilities in information security. In theory, each role must complement the other, but this is often not the case in practice.

Information Security Management and Professionals

The roles of information security professionals are aligned with the goals and mission of the information security community of interest. These job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks.

Information Technology Management and Professionals

The community of interest made up of IT managers and skilled professionals in systems design, programming, networks, and other related disciplines has many of the same objectives as the information security community. However, its members focus more on costs of system creation and operation, ease of use for system users, and timeliness of system creation, as well as transaction response time. The goals of the IT community and the information security community are not always in complete alignment, and depending on the organizational structure, this may cause conflict.

Organizational Management and Professionals

The organization's general management team and the rest of the personnel in the organization make up the other major community of interest. This large group is almost always made up of subsets of other interests as well, including executive management, production management, human resources, accounting, and legal staff, to name just a few. The IT community often categorizes these groups as users of information technology systems, while the information security community categorizes them as security subjects. In fact, this community serves as the greatest reminder that all IT systems and information security objectives exist to further the objectives of the broad organizational community. The most efficient IT systems operated in the most secure fashion ever devised have no value if they are not useful to the organization as a whole.

Information Security: Is It An Art Or A Science?

Given the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. System technologists, especially those with a gift for managing and operating computers and computer-based systems, have long been suspected of using more than a little magic to keep the systems running as expected. In information security, such technologists are sometimes called *security artisans*.[16] Everyone who has studied computer systems can appreciate the anxiety most people feel when faced with complex technology. Consider the inner workings of the computer: With the mind-boggling functions performed by the 1.4 billion transistors found in a CPU, the interaction of the various digital devices over the local networks and the Internet, and the memory storage units on the circuit boards, it's a miracle that computers work at all.

Security as Art

The administrators and technicians who implement security can be compared to a painter applying oils to canvas. A touch of color here, a brush stroke there, just enough to represent the image the artist wants to convey without overwhelming the viewer—or in security terms, without overly restricting user access. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While many manuals exist to support individual systems, no manual can help implement security throughout an entire interconnected system. This is especially true given the complex levels of interaction among users, policy, and technology controls.

Security as Science

Technology developed by computer scientists and engineers—which is designed for rigorous performance levels—makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the

interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate all of these faults.

The faults that remain are usually the result of technology malfunctioning for any of a thousand reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

Security as a Social Science

A third view to consider is information security as a social science, which integrates components of art and science and adds another dimension to the discussion. Social science examines the behavior of people as they interact with systems, whether they are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people who interact with the system, intentionally or otherwise.

There is a long-standing joke in IT that is sometimes told when a user has the experience of using a system that is not performing as expected: "It's not a bug, it's a feature!" This situation occurs when a system performs as it was designed but not as users anticipated, or when users simply don't have the skills or knowledge to make full use of the system. The same is true when an attacker learns of unintended ways to use systems, not by taking advantage of defects in a system, but by taking advantage of *unintended* functions or operations. Although the science of the system may be exact, its use or misuse—the human side of systems—is not.

End users who need the very information that security personnel are trying to protect may be the weakest link in the security chain. By understanding some behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, coupled with appropriate policy and training issues, can substantially improve the performance of end users and result in a more secure information system.

Closing Scenario

The next day at SLS found everyone on the technical support team busy and focused on the unified threat management system as they restored computer systems to their former state and validated the virus and worm control systems. Amy found herself learning how to reinstall desktop computer operating systems and applications as SLS made a heroic effort to recover from the attack of the previous day.

Discussion Questions

1. Do you think this event was caused by an insider or an outsider? Explain your answer.
2. Other than installing malware control software, what can SLS do to prepare for the next incident?
3. Do you think this attack was the result of malware? Explain your answer.

Ethical Decision Making

Often an attacker crafts e-mail attacks containing malware designed to take advantage of the curiosity or even greed of the recipients. Imagine that the message body Amy saw in the e-mail from Davey had been "See our managers' salaries and SSNs" instead of "Funniest joke you'll see today."

1. Would it be ethical for Amy to open such a file?
2. If such an e-mail came in, what would be the best action to take?

Selected Readings

- *Beyond Fear* by Bruce Schneier, 2006, Springer-Verlag, New York. This book is an excellent look at the broader areas of security. Of special note is Chapter 4, "Systems and How They Fail," which describes how systems are often implemented and how they might be vulnerable to threats and attacks.
- *Fighting Computer Crime* by Donn B. Parker, 1983, Macmillan Library Reference.
- *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943* by David Kahn, 1991, Houghton Mifflin.
- Glossary of Terms Used in Security and Intrusion Detection by SANS Institute. This glossary can be accessed online at *www.sans.org/resources/glossary.php*.
- RFC 2828–Internet Security Glossary from the Internet RFC/STD/FYI/BCP Archives. This glossary can be accessed online at *www.faqs.org/rfcs/rfc2828.html*.
- SP 800-12, "An Introduction to Computer Security: The NIST Handbook." This document can be accessed online at *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*.

Module Summary

- Information security evolved from the early field of computer security.
- Security is protection from danger. A successful organization should have multiple layers of security in place to protect its people, operations, physical infrastructure, functions, communications, and information.
- Information security is the protection of information assets that use, store, or transmit information through the application of policy, education, and technology.
- The critical characteristics of information, including confidentiality, integrity, and availability (the C.I.A. triad), must be protected at all times. This protection is implemented by multiple measures that include policies, education, training and awareness, and technology.
- Information systems are made up of the major components of hardware, software, data, people, procedures, and networks.
- Upper management drives the top-down approach to security implementation, in contrast with the bottom-up approach or grassroots effort, in which individuals choose security implementation strategies.
- The control and use of data in the organization is accomplished by the following parties:
  - Data owners, who are responsible for the security and use of a particular set of information
  - Data custodians, who are responsible for the storage, maintenance, and protection of the information
  - Data trustees, who are appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use
  - Data users, who work with the information to perform their daily jobs and support the mission of the organization
- Each organization has a culture in which communities of interest are united by similar values and share common objectives. The three communities in information security are general management, IT management, and information security management.
- Information security has been described as both an art and a science, and it comprises many aspects of social science as well.

Review Questions

1. What is the difference between a threat agent and a threat source?
2. What is the difference between vulnerability and exposure?
3. What is a loss in the context of information security?
4. What type of security was dominant in the early years of computing?
5. What are the three components of the C.I.A. triad? What are they used for?
6. If the C.I.A. triad is incomplete, why is it so commonly used in security?

7. Describe the critical characteristics of information. How are they used in the study of computer security?
8. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?
9. What is the McCumber Cube, and what purpose does it serve?
10. Which paper is the foundation of all subsequent studies of computer security?
11. Why is the top-down approach to information security superior to the bottom-up approach?
12. Describe the need for balance between information security and access to information in information systems.
13. How can the practice of information security be described as both an art and a science? How does the view of security as a social science influence its practice?
14. Who is ultimately responsible for the security of information in the organization?
15. What is the relationship between the MULTICS project and the early development of computer security?
16. How has computer security evolved into modern information security?
17. What was important about RAND Report R-609?
18. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these decisions are carried out?
19. Who should lead a security team? Should the approach to security be more managerial or technical?
20. Besides the champion and team leader, who should serve on an information security project team?

Exercises

1. Look up "the paper that started the study of computer security." Prepare a summary of the key points. What in this paper specifically addresses security in previously unexamined areas?
2. Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components of each cell.
3. Using the Web, identify the chief executive officer (CEO), chief information officer (CIO), chief information security officer (CISO), and systems administrator for your school. Which of these people represents the data owner? Which represents the data custodian?
4. Using the Web, find a large company or government agency that is familiar to you or located in your area. Try to find the name of the CEO, the CIO, and the CISO. Which was easiest to find? Which was hardest?
5. Using the Web, find out more about Kevin Mitnick. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.

References

1. Salus, Peter. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. November 19, 1998. Accessed June 15, 2020, from *www.sane.nl/events/sane98/aftermath/salus.html*.
2. Bletchley Park Trust and kamilpetran/Shutterstock.com.
3. Roberts, Larry. "Program Plan for the ARPANET." Provided by Dr. Roberts on February 8, 2004.
4. Salus, Peter. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. November 19, 1998. Accessed June 15, 2020, from *www.sane.nl/events/sane98/aftermath/salus.html*.
5. Bisbey, Richard II, and Hollingworth, Dennis. "Protection Analysis: Final Report." May 1978. ISI/SR-78-13, USC/Information Sciences Institute. Marina Del Rey, CA 90291.
6. Grampp, F. T., and Morris, R. H. "UNIX Operating System Security." *AT&T Bell Laboratories Technical Journal* 63, no. 8 (1984): 1649–1672.
7. Reeds, J. A., and Weinberger, P.J. "The UNIX System: File Security and the UNIX System Crypt Command." *AT&T Bell Laboratories Technical Journal* 63, no. 8 (1984): 1673–1683.

8. Ware, Willis. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." RAND Online. October 10, 1979. Accessed June 15, 2020, from *www.rand.org/pubs/reports/R609-1.html*.
9. Ibid.
10. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) Professionals. File 4011. June 20, 1994. Accessed July 14, 2020, from *www.cnss.gov/CNSS/issuances/Instructions.cfm*.
11. Mihalcik, C. "Marriott Discloses New Data Breach Impacting 5.2 Million Guests." C|Net. Accessed July 9, 2020, from *www.cnet.com/news/marriott-discloses-new-data-breach-impacting-5-point-2-million-guests/*.
12. Claburn, Thomas. "GE Money Backup Tape with 650,000 Records Missing at Iron Mountain." Accessed June 22, 2020, from *www.informationweek.com/ge-money-backup-tape-with-650000-records-missing-at-iron-mountain/d/d-id/1063500*?.
13. McCumber, John. "Information Systems Security: A Comprehensive Model." Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD, October 1991.
14. Ibid.
15. Hayes, Mary. "Where the Chief Security Officer Belongs." *InformationWeek*, no. 877 (25 February 2002): 38.
16. Parker, D. B. *Fighting Computer Crime*. 1998. New York: Wiley Publishing, 189.

MODULE 2

The Need for Information Security

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

1. Discuss the need for information security
2. Explain why a successful information security program is the shared responsibility of the entire organization
3. List and describe the threats posed to information security and common attacks associated with those threats
4. List the common information security issues that result from poor software development efforts

Our bad neighbor makes us early stirrers, which is both healthful and good husbandry.

—William Shakespeare, King Henry, in Henry V, Act 4, Scene 1

Opening Scenario

Fred Chin, CEO of Sequential Label and Supply (SLS), leaned back in his leather chair and propped his feet up on the long mahogany table in the conference room where the SLS Board of Directors had just adjourned from their quarterly meeting.

"What do you think about our computer security problem?" he asked Gladys Williams, the company's chief information officer (CIO). He was referring to the outbreak of a malicious worm on the company's computer network the previous month.

Gladys replied, "I think we have a real problem, and we need to put together a real solution. We can't sidestep this with a quick patch like last time." Six months ago, most of the systems on the company network had been infected with a virus program that came from an employee's personal USB drive. To prevent this from happening again, all users in the company were now prohibited from using personal devices on corporate systems and networks.

Fred wasn't convinced. "Can't we just allocate additional funds to the next training budget?"

Gladys shook her head. "You've known for some time now that this business runs on technology. That's why you hired me as CIO. I've seen this same problem at other companies, and I've been looking into our information security issues. My staff and I have some ideas to discuss with you. I've asked Charlie Moody to come in today to talk about it. He's waiting to speak with us."

When Charlie joined the meeting, Fred said, "Hello, Charlie. As you know, the Board of Directors met today. They received a report on the costs and lost production from the malware outbreak last month, and they directed us to improve the security of our technology. Gladys says you can help me understand what we need to do about it."

"To start with," Charlie said, "Instead of simply ramping up our antivirus solution or throwing resources at an endpoint protection product, we need to start by developing a formal information security program. We need a thorough review of our policies and practices, and we need to establish an ongoing risk management program. Then we can explore the technical options we have. There are some other things that are part of the process as well, but this is where I think we should start."

"Sounds like it is going to be complicated ... and expensive," said Fred.

Charlie looked at Gladys and then answered, "Well, there will probably be some extra expenses for specialized hardware and software, and we may have to slow down some of our product development projects a bit, but this approach will call more for a change in our attitude about security than just a spending spree. I don't have accurate estimates yet, but you can be sure we'll put cost-benefit worksheets in front of you before we commit any funds."

Fred thought about this for a few seconds. "Okay. What's our next step?"

Gladys answered, "First, we need to initiate a project plan to develop our new information security program. We'll use our usual systems development and project management approach. There are a few differences, but we can easily adapt our current models. We'll need to reassign a few administrators to help Charlie with the new program. We'd also like a formal statement to the entire company identifying Charlie as our new chief information security officer and asking all of the department heads to cooperate with his new information security initiatives."

"Information security? What about computer security?" asked Fred.

Charlie responded, "Information security includes computer security, plus all the other things we use to do business: securing our information, networks, operations, communications, personnel, and intellectual property. Even our paper records need to be factored in."

"I see," Fred said. "Okay, Mr. Chief Information Security Officer." Fred held out his hand for a congratulatory handshake. "Bring me the draft project plan and budget in two weeks. The audit committee of the Board meets in four weeks, and we'll need to report our progress then."

Introduction To The Need For Information Security

Unlike any other business or information technology program, the primary mission of an information security program is to ensure that **information assets**—information and the systems that house them—are protected and thus remain safe and useful. Organizations expend a lot of money and thousands of hours to maintain their information assets. If threats to these assets didn't exist, those resources could be used exclusively to improve the systems that contain, use, and transmit the information. However, the threat of attacks on information assets is a constant concern, and the need for information security grows along with the sophistication of the attacks. While some organizations lump both information and systems under their definition of an information asset, others prefer to separate the true information-based assets (data, databases, data sets, and the applications that use data) from their **media**—the technologies that access, house, and carry the information. For our purposes, we will include both data and systems assets in our use of the term. Similarly, we'll use the term *information* to describe both **data** and **information**, as for most organizations the terms can be used interchangeably.

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

media
As a subset of information assets, the systems, technologies, and networks that store, process, and transmit information.

data
Items of fact collected by an organization; includes raw numbers, facts, and words.

information
Data that has been organized, structured, and presented to provide additional insight into its context, worth, and usefulness.

Organizations must understand the environment in which information assets reside so their information security programs can address actual and potential problems. This module describes the environment and identifies the threats to it, the organization, and its information.

Information security performs four important functions for an organization:

- Protecting the organization's ability to function
- Protecting the data and information the organization collects and uses, whether physical or electronic
- Enabling the safe operation of applications running on the organization's IT systems
- Safeguarding the organization's technology assets

Business Needs First

There is a long-standing saying in information security: When security needs and business needs collide, business wins. Without the underlying business to generate revenue and use the information, the information may lose value, and there would be no need for it. If the business cannot function, information security becomes less important. The key is to balance the needs of the organization with the need to protect information assets, realizing that business needs come first. This is not to say that information security should be casually ignored whenever there is a conflict, but to stress that decisions associated with the degree to which information assets are protected should be made carefully, considering both the business need to use the information and the need to protect it.

Protecting Functionality

The three communities of interest defined in Module 1—general management, IT management, and information security management—are each responsible for facilitating the information security program that protects the organization's ability to function. Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, implementing information security has more to do with *management* than *technology*. Just as managing payroll involves management more than mathematical wage computations, managing information security has more to do with risk management, policy, and its enforcement than the technology of its implementation. As the noted information security author Charles Cresson Wood writes:

> *In fact, a lot of [information security] is good management for information technology. Many people think that a solution to a technology problem is more technology. Well, not necessarily. … So a lot of my work, out of necessity, has been trying to get my clients to pay more attention to information security as a management issue in addition to a technical issue, information security as a people issue in addition to the technical issue.*[1]

Each of an organization's communities of interest must address information security in terms of business impact and the cost of business interruption rather than isolating security as a technical problem.

Protecting Data That Organizations Collect and Use

Without data, an organization loses its record of transactions and its ability to deliver value to customers. Any business, educational institution, or government agency that operates within the modern context of connected and responsive services relies on information systems. Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services. Therefore, protecting data *in transmission, in processing*, and *at rest* (*storage*) is a critical aspect of information security. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization's data.

Organizations store much of the data they deem critical in **databases**, managed by specialized software known as a database management system (DBMS). **Database security** is accomplished by applying a broad range of control approaches common to many areas of information security. Securing databases encompasses most of the topics covered in this textbook, including managerial, technical, and physical controls. *Managerial controls* include policy, procedure, and governance. *Technical controls* used to secure databases rely on knowledge of access control, authentication, auditing, application security, backup and recovery, encryption, and integrity controls. *Physical controls* include the use of data centers with locking doors, fire suppression systems, video monitoring, and physical security guards.

The fundamental practices of information security have broad applicability in database security. One indicator of this strong degree of overlap is that the International Information System Security Certification Consortium (ISC)[2], the organization that evaluates candidates for many prestigious information security certification programs, allows experience as a database administrator to count toward the experience requirement for the Certified Information Systems Security Professional (CISSP).

database

A collection of related data stored in a structured form and usually managed by specialized systems.

database security

A subset of information security that focuses on the assessment and protection of information stored in data repositories.

Enabling the Safe Operation of Applications

Today's organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications. A modern organization needs to create an environment that safeguards these applications, particularly those that are important elements of the organization's infrastructure—operating system platforms, certain

operational applications, electronic mail (e-mail), and instant messaging (IM) applications, like text messaging (short message service, or SMS). Organizations acquire these elements from a service provider, or they implement their own. Once an organization's infrastructure is in place, management must continue to oversee it and not relegate its management to the IT department.

Safeguarding Technology Assets in Organizations

To perform effectively, organizations must employ secure infrastructure hardware appropriate to the size and scope of the enterprise. For instance, a small business may get by in its start-up phase using a small-scale firewall, such as a *small office/home office (SOHO)* device.

In general, as an organization grows to accommodate changing needs, more robust technology solutions should replace security technologies the organization has outgrown. An example of a robust solution is a commercial-grade, unified security architecture device, complete with intrusion detection and prevention systems, public key infrastructure (PKI), and virtual private network (VPN) capabilities. Modules 8 through 10 describe these technologies in more detail.

Information technology continues to add new capabilities and methods that allow organizations to solve business information management challenges. In recent years, we have seen the emergence of the Internet and the Web as new markets. Cloud-based services, which have created new ways to deliver IT services, have also brought new risks to organizational information, additional concerns about the ways these assets can be threatened, and concern for how they must be defended.

Information Security Threats And Attacks

Around 500 B.C., the Chinese general Sun Tzu Wu wrote *The Art of War*, a military treatise that emphasizes the importance of knowing yourself as well as the threats you face.[2] To protect your organization's information, you must (1) know yourself—that is, be familiar with the information to be protected and the systems that store, transport, and process it—and (2) know your enemy; in other words, the threats you face. To make sound decisions about information security, management must be informed about the various threats to an organization's people, applications, data, and information systems. As discussed in Module 1, a threat represents a potential risk to an information asset, whereas an *attack* represents an ongoing act against the asset that could result in a loss. Threat agents damage or steal an organization's information or physical assets by using **exploits** to take advantage of *vulnerabilities* where controls are not present or no longer effective. Unlike threats, which are always present, attacks exist only when a specific act may cause a loss. For example, the *threat* of damage from a thunderstorm is present throughout the summer in many places, but an *attack* and its associated risk of loss exist only for the duration of an actual thunderstorm. The following sections discuss each of the major types of threats and corresponding attacks facing modern information assets.

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

4.8 Billion Potential Hackers

There is wide agreement that the threat from external sources increases when an organization connects to the Internet. The number of Internet users continues to grow; about 62 percent of the world's almost 7.8 billion people—that is, more than 4.8 billion people—have some form of Internet access, a dramatic increase over the 49.2 percent reported as recently as 2015. Table 2-1 shows Internet usage by continent. Since the time this data was collected in mid-2020, the world population has continued to grow, with an expected increase in Internet usage. Therefore, a typical organization with an online connection to its systems and information faces an ever-increasing pool of potential hackers.

exploit

A technique used to compromise a system; may also describe the tool, program, or script used in the compromise.

Table 2-1 World Internet Usage[3]

World Regions	Population (2020 Est.)	Population % of World	Internet Users (6/30/2020)	Penetration Rate (% Pop.)	Growth 2000–2020	Internet World %
Africa	1,340,598,447	17.2%	566,138,772	42.2%	12,441%	11.7%
Asia	4,294,516,659	55.1%	2,525,033,874	58.8%	2,109%	52.2%
Europe	834,995,197	10.7%	727,848,547	87.2%	592%	15.1%
Latin America/ Caribbean	654,287,232	8.4%	467,817,332	71.5%	2,489%	9.7%
Middle East	260,991,690	3.3%	184,856,813	70.8%	5,527%	3.8%
North America	368,869,647	4.7%	332,908,868	90.3%	208%	6.9%
Oceania/Australia	42,690,838	0.5%	28,917,600	67.7%	279%	0.6%
WORLD TOTAL	7,796,949,710	100.0%	4,833,521,806	62.0%	1,239%	100.0%

Notes: Internet usage and world population estimates are as of July 20, 2020.

Other Studies of Threats

Several studies in recent years have examined the threats and attacks to information security. One of the most recent studies, conducted in 2015, found that 67.1 percent of responding organizations suffered malware infections.

More than 98 percent of responding organizations identified malware attacks as a threat, with 58.7 percent indicating they were a significant or severe threat. Malware was identified as the second-highest threat source behind electronic phishing/spoofing.[4]

Table 2-2 shows these and other threats from internal stakeholders. Table 2-3 shows threats from external stakeholders. Table 2-4 shows general threats to information assets.

Table 2-2 Rated Threats from Internal Sources in 2015 SEC/CISE Survey of Threats to Information Protection[5]

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Inability/unwillingness to follow established policy	6.6%	17.2%	33.6%	26.2%	16.4%	66%
Disclosure due to insufficient training	8.1%	23.6%	29.3%	25.2%	13.8%	63%
Unauthorized access or escalation of privileges	4.8%	24.0%	31.2%	31.2%	8.8%	63%
Unauthorized information collection/data sniffing	6.4%	26.4%	40.0%	17.6%	9.6%	60%
Theft of on-site organizational information assets	10.6%	32.5%	34.1%	12.2%	10.6%	56%
Theft of mobile/laptop/tablet and related/ connected information assets	15.4%	29.3%	28.5%	17.9%	8.9%	55%
Intentional damage or destruction of information assets	22.3%	43.0%	18.2%	13.2%	3.3%	46%
Theft or misuse of organizationally leased, purchased, or developed software	29.6%	33.6%	21.6%	10.4%	4.8%	45%
Web site defacement	43.4%	33.6%	16.4%	4.9%	1.6%	38%
Blackmail of information release or sales	43.5%	37.1%	10.5%	6.5%	2.4%	37%

Table 2-3 Rated Threats from External Sources in 2015 SEC/CISE Survey of Threats to Information Protection[6]

From Outsiders or External Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Unauthorized information collection/data sniffing	6.4%	14.4%	21.6%	32.8%	24.8%	71%
Unauthorized access or escalation of privileges	7.4%	14.0%	26.4%	31.4%	20.7%	69%
Web site defacement	8.9%	23.6%	22.8%	26.8%	17.9%	64%
Intentional damage or destruction of information assets	14.0%	32.2%	18.2%	24.8%	10.7%	57%
Theft of mobile/laptop/tablet and related/connected information assets	20.5%	25.4%	26.2%	15.6%	12.3%	55%
Theft of on-site organizational information assets	21.1%	24.4%	25.2%	17.9%	11.4%	55%
Blackmail of information release or sales	31.1%	30.3%	14.8%	14.8%	9.0%	48%
Disclosure due to insufficient training	34.5%	21.8%	22.7%	13.4%	7.6%	48%
Inability/unwillingness to follow established policy	33.6%	29.4%	18.5%	6.7%	11.8%	47%
Theft or misuse of organizationally leased, purchased, or developed software	31.7%	30.1%	22.8%	9.8%	5.7%	46%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection[7]

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Electronic phishing/spoofing attacks	0.8%	13.1%	16.4%	32.0%	37.7%	79%
Malware attacks	1.7%	12.4%	27.3%	36.4%	22.3%	73%
Unintentional employee/insider mistakes	2.4%	17.1%	26.8%	35.8%	17.9%	70%
Loss of trust due to information loss	4.1%	18.9%	27.0%	22.1%	27.9%	70%
Software failures or errors due to unknown vulnerabilities in externally acquired software	5.6%	18.5%	28.2%	33.9%	13.7%	66%
Social engineering of employees/insiders based on social media information	8.1%	14.6%	32.5%	34.1%	10.6%	65%
Social engineering of employees/insiders based on other published information	8.9%	19.5%	24.4%	32.5%	14.6%	65%
Software failures or errors due to poorly developed, internally created applications	7.2%	21.6%	24.0%	32.0%	15.2%	65%
SQL injections	7.6%	17.6%	31.9%	29.4%	13.4%	65%

(*continues*)

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection[7] (*Continued*)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Social engineering of employees/insiders based on organization's Web sites	11.4%	19.5%	23.6%	31.7%	13.8%	63%
Denial of service (and distributed DoS) attacks	8.2%	23.0%	27.9%	32.8%	8.2%	62%
Software failures or errors due to known vulnerabilities in externally acquired software	8.9%	23.6%	26.8%	35.8%	4.9%	61%
Outdated organizational software	8.1%	28.2%	26.6%	26.6%	10.5%	61%
Loss of trust due to representation as source of phishing/spoofing attack	9.8%	23.8%	30.3%	23.0%	13.1%	61%
Loss of trust due to Web defacement	12.4%	30.6%	31.4%	19.8%	5.8%	55%
Outdated organizational hardware	17.2%	34.4%	32.8%	12.3%	3.3%	50%
Outdated organization data format	18.7%	35.8%	26.8%	13.8%	4.9%	50%
Inability/unwillingness to establish effective policy by management	30.4%	26.4%	24.0%	13.6%	5.6%	48%
Hardware failures or errors due to aging equipment	19.5%	39.8%	24.4%	14.6%	1.6%	48%
Hardware failures or errors due to defective equipment	17.9%	48.0%	24.4%	8.1%	1.6%	46%
Deviations in quality of service from other provider	25.2%	38.7%	25.2%	7.6%	3.4%	45%
Deviations in quality of service from data communications provider/ISP	26.4%	39.7%	23.1%	7.4%	3.3%	44%
Deviations in quality of service from telecommunications provider/ISP (if different from data provider)	29.9%	38.5%	18.8%	9.4%	3.4%	44%
Loss due to other natural disaster	31.0%	37.9%	23.3%	6.9%	0.9%	42%
Loss due to fire	26.2%	49.2%	21.3%	3.3%	0.0%	40%
Deviations in quality of service from power provider	36.1%	43.4%	12.3%	5.7%	2.5%	39%
Loss due to flood	33.9%	43.8%	19.8%	1.7%	0.8%	38%
Loss due to earthquake	41.7%	35.8%	15.0%	6.7%	0.8%	38%

Common Attack Pattern Enumeration and Classification (CAPEC)

A tool that security professionals can use to understand attacks is the Common Attack Pattern Enumeration and Classification (CAPEC) Web site hosted by Mitre—a nonprofit research and development organization sponsored by the U.S. government. This online repository can be searched for characteristics of a particular attack or simply browsed by professionals who want additional knowledge of how attacks occur procedurally.

For more information on CAPEC, visit *http://capec.mitre.org*, where contents can be downloaded or viewed online.