Fourth Edition

PRINCIPLES OF INFORMATION SECURITY

Michael E. Whitman, Herbert J. Mattord

PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Principles of Information Security

Fourth Edition

Principles of Information Security

Fourth Edition

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

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

COURSE TECHNOLOGY
CENGAGE Learning™

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

COURSE TECHNOLOGY
CENGAGE Learning™

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

Vice President Editorial, Career Education & Training Solutions: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Steve Helba

Managing Editor: Marah Bellegarde

Product Manager: Natalie Pashoukos

Development Editor: Lynne Raughley

Editorial Assistant: Jennifer Wheaton

Vice President Marketing, Career Education & Training Solutions: Jennifer Ann Baker

Marketing Director: Deborah S. Yarnell

Senior Marketing Manager: Erin Coffin

Associate Marketing Manager: Shanna Gibbs

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

Manufacturing Coordinator: Amy Rogers

Technical Edit/Quality Assurance: Green Pen Quality Assurance

For more information, contact or find us on the World Wide Web at: www.course.com

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

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

Library of Congress Control Number: 2010940654

ISBN-13: 978-1-111-13821-9

ISBN-10: 1-111-13821-4

Course Technology
20 Channel Center
Boston, MA 02210
USA

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

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

For your lifelong learning solutions, visit **course.cengage.com**

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

Printed in the United States of America
1 2 3 4 5 6 7 8 9 14 13 12 11 10

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

To my wife Carola; without your support, none of this would be possible.
—HJM

Brief Table of Contents

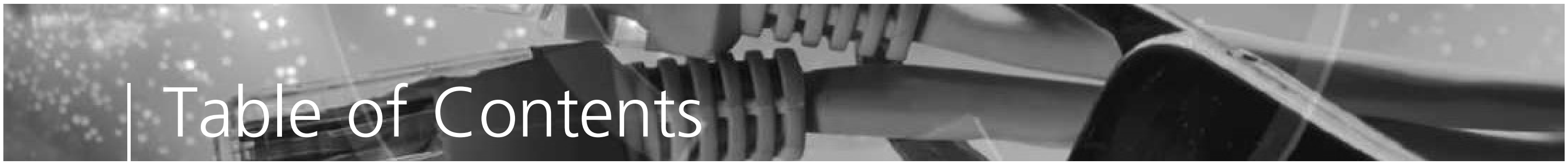


Table of Contents

CHAPTER 10

CHAPTER 11

Preface

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

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

The purpose of *Principles of Information Security, Fourth Edition*, is to fill the need for a quality academic textbook that surveys the discipline of information security. While there are dozens of quality publications on information security and assurance that are oriented to the practitioner, there is a dearth of textbooks that provide the student with a balanced introduction to both security management and the technical components of security. By creating a book specifically from the perspective of the discipline of information systems, we hope to close this gap. Further, there is a clear need for criminal justice, political science, accounting information systems, and other disciplines to gain a clear understanding of the principles of information security, in order to formulate interdisciplinary solutions for systems vulnerabilities. The essential tenet of this textbook is that information security in the modern organization is a problem for management to solve, and not one that technology alone can address. In other words, the information security of an organization has important economic consequences, for which management will be held accountable.

Approach

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

Structure and Chapter Descriptions

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

Section I—Introduction

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

Section II—Security Investigation Phase

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

The chapter also examines the various threats facing organizations and presents methods for ranking these threats (in order to assign them relative priority) that organizations can use when they begin their security planning process. The chapter continues with a detailed examination of the types of attacks that could result from these threats, and how these attacks could impact the organization's information systems. The chapter also provides a further discussion of the key principles of information security, some of which were introduced in Chapter 1: confidentiality, integrity, availability, authentication and identification, authorization, accountability, and privacy.

Finally, the chapter explains the concept and tenets of software assurance, and provides insight into the newly developing common body of knowledge in software assurance, along with several "deadly security sins" of software development.

Chapter 3—Legal, Ethical, and Professional Issues in Information Security In addition to being a fundamental part of the SecSDLC investigation process, a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities provides important insights into the regulatory constraints that govern business. This chapter examines several key laws that shape the field of information security, and presents a detailed examination of the computer ethics that those who implement security must adhere to. Although ignorance of the law is no excuse, it's considered better than negligence (that is, knowing the law but doing nothing to comply with it). This chapter also presents several legal and ethical issues that are commonly found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

Section III—Security Analysis

Chapter 4—Risk Management Before the design of a new information security solution can begin, the 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 the security managers and end users? This chapter describes how to conduct a fundamental information security assessment by describing the procedures for identifying and prioritizing threats and assets, and the procedures for identifying what controls are in place to protect these assets from threats. The chapter also provides a discussion of the various types of control mechanisms and identifies the steps involved in performing the initial risk assessment. The chapter continues by defining risk management as the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. The chapter concludes with a discussion of risk analysis and the various types of feasibility analyses.

Section IV—Logical Design

Chapter 5—Planning for Security Chapter 5 presents a number of widely accepted security models and frameworks. It examines best business practices and standards of due care and due diligence, and offers an overview of the development of security policy. This chapter details the major components, scope, and target audience for each of the levels of security policy. This chapter also explains data classification schemes, both military and private, as well as the security education training and awareness (SETA) program. The chapter examines the planning process that supports business continuity, disaster recovery, and incident response; it also describes the organization's role during incidents and specifies when the organization should involve outside law enforcement agencies.

Section V—Physical Design

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

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

Chapter 7—Security Technology: Intrusion Detection, Access Control, and Other Security Tools Chapter 7 continues the discussion of security technologies by examining the concept of the 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 also presented and discussed. The chapter continues with an examination of the specialized detection technologies that are designed to entice attackers into decoy systems (and thus away from critical systems) or simply to identify the attackers' entry into these decoy areas, which are known as honey pots, honey nets, and padded cell systems. Also examined are trace-back systems, which are designed to track down the true address of attackers who were lured into decoy systems. The chapter continues with a detailed examination of some of the key security tools information security professionals can use to examine the current state of their organization's systems, and to identify any potential vulnerabilities or weaknesses that may exist in the systems or the organization's overall security posture. The chapter concludes with a discussion of access control devices commonly deployed by modern operating systems, and new technologies in the area of biometrics that can provide strong authentication to existing implementations.

Chapter 8—Cryptography Chapter 8 continues the section on security technologies with a presentation of the underlying foundations of modern cryptosystems, as well as a discussion of the architectures and implementations of those cryptosystems. The chapter begins with an overview of the history of modern cryptography, and a discussion of the various types of ciphers that played key roles in that history. The chapter also examines some of the mathematical techniques that comprise cryptosystems, including hash functions. The chapter extends this discussion by comparing traditional symmetric encryption systems with more modern asymmetric encryption systems. The chapter also examines the role of asymmetric systems as the foundation of public-key encryption systems. Also covered in this chapter are the cryptography-based protocols used in secure communications; these include protocols such as SHTTP, SMIME, SET, SSH, and several others. The chapter then provides a discussion of steganography, and its emerging role as an effective means of hiding information. The chapter concludes by revisiting those attacks on information security that are specifically targeted at cryptosystems.

Chapter 9—Physical Security A vital part of any information security process, physical security is concerned with the management of the physical facilities, the implementation of physical access control, and the oversight of environmental controls. From designing a secure data center to assessing the relative value of guards and watchdogs to resolving the technical issues involved in fire suppression and power conditioning, physical security involves a wide range of special considerations. Chapter 9 examines these considerations by factoring in the various physical security threats that modern organizations face.

Section VI—Implementation

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

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

Section VII—Maintenance and Change

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

Features

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

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

Chapter Scenarios—Each chapter opens with a short story that features the same fictional company as it encounters information security issues commonly found in real-life organizations. At the end of each chapter, there is a brief follow-up to the opening story and a set of discussion questions that provide students and instructors opportunities to discuss the issues that underlie the story's content.

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

Hands-On Learning—At the end of each chapter, students find a Chapter Summary and Review Questions as well as Exercises, which give them the opportunity to examine the information security arena outside the classroom. In the Exercises, students are asked to research, analyze, and write responses to questions that are intended to reinforce learning objectives and deepen their understanding of the text.

New to this Edition

- Enhanced section on Security Models and Standards, including access control models, Bell-LaPadula, Biba, and others, as well as enhanced coverage of NIST and ISO standards
- Information on security governance adds depth and breadth to the topic
- Provides coverage on the newest laws and a host of identity theft bills
- Addresses the methods and results of systems certification and accreditation in accordance with federal guidelines

Additional Student Resources

To access additional course materials including CourseMate, please visit www.cengagebrain.com. At the CengageBrain.com home page, search for the ISBN of your title (from the back cover of your book) using the search box at the top of the page. This will take you to the product page where these resources can be found.

CourseMate

The CourseMate that accompanies *Principles of Information Security, Fourth Edition* helps you make the grade.

CourseMate includes:

- An interactive eBook, with highlighting, note taking and search capabilities
- Interactive learning tools including:
  - Quizzes
  - Flashcards

- PowerPoint slides
- Glossary
- and more!

CourseMate

- Printed Access Code (ISBN 1-1111-3824-9)
- Instant Access Code (ISBN 1-1111-3825-7)

Instructor Resources

Instructor Resources CD

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

Electronic Instructor's Manual—The Instructor's Manual includes suggestions and strategies for using this text, and even suggestions for lecture topics. The Instructor's Manual also includes answers to the Review Questions and suggested solutions to the Exercises at the end of each chapter.

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

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

PowerPoint Presentations—This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid to be used for classroom presentation, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors can add their own slides for additional topics they introduce to the class.

Lab Manual—Course Technology has developed a lab manual to accompany this and other books: *The Hands-On Information Security Lab Manual* (ISBN 0-619-21631-X). The lab manual provides hands-on security exercises on footprinting, enumeration, and firewall configuration, as well as a number of detailed exercises and cases that can serve to supplement the book as laboratory components or as in-class projects. Contact your Course Technology sales representative for more information.

ExamView—ExamView®, the ultimate tool for objective-based testing needs. ExamView® is a powerful objective-based test generator that enables instructors to create paper, LAN- or Web-based tests from testbanks designed specifically for their Course Technology text. Instructors can utilize the ultra-efficient QuickTest Wizard to create tests in less than five minutes by taking advantage of Course Technology's question banks, or customize their own exams from scratch.

WebTUTOR™

WebTUTOR™ for Blackboard is a content rich, web-based teaching and learning aid that reinforces and clarifies complex concepts while integrating into your Blackboard course. The WebTUTOR™ platform also provides rich communication tools for instructors and students, making it much more than an online study guide. Features include PowerPoint presentations, practice quizzes, and more, organized by chapter and topic. Whether you want to Web-enhance your class, or offer an entire course online, WebTUTOR™ allows you to focus on what you do best, teaching.

- Instructor Resources CD (ISBN: 1-1111-3822-2)
- WebTUTOR™ on Blackboard (ISBN: 1-1116-4104-8)

CourseMate

Principles of Information Security, Fourth Edition includes CourseMate, a complement to your textbook. CourseMate includes:

- An interactive eBook
- Interactive teaching and learning tools including:
  - Quizzes
  - Flashcards
  - PowerPoint slides
  - Glossary
  - and more
- Engagement Tracker, a first-of-its-kind tool that monitors student engagement in the course

To access these materials online, visit http://login.cengage.com.

CourseMate

- Printed Access Code (ISBN 1-1111-3824-9)
- Instant Access Code (ISBN 1-1111-3825-7)

Author Team

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

Michael Whitman, Ph.D., CISM, CISSP is a Professor of Information Security in the Computer Science and Information Systems Department at Kennesaw State University, Kennesaw, Georgia, where he is also the Coordinator of the Bachelor of Science in Information Security and Assurance degree and the Director of the KSU Center for Information Security Education (*infosec.kennesaw.edu*). Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, Ethical Computing and Information Systems Research Methods. He currently teaches graduate and undergraduate courses in Information Security, and Contingency Planning. He has published articles in the top journals in his field, including *Information Systems Research*, *Communications of the ACM*, *Information and Management*, *Journal of International Business Studies*, and *Journal of Computer Information Systems*. He is a member of the Information

Systems Security Association, the Association for Computing Machinery, and the Association for Information Systems. Dr. Whitman is also the co-author of *Management of Information Security*, *Principles of Incident Response and Disaster Recovery*, *Readings and Cases in the Management of Information Security*, *The Guide to Firewalls and Network Security*, and *The Hands-On Information Security Lab Manual*, all published by Course Technology. Prior to his career in academia, Dr. Whitman was an Armored Cavalry Officer in the United States Army.

Herbert Mattord, M.B.A., 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 as Kennesaw State University in 2002. Professor Mattord is the Operations Manager of the KSU Center for Information Security Education and Awareness (*infosec.kennesaw.edu*), as well as the coordinator for the KSU department of Computer Science and Information Systems Certificate in Information Security and Assurance. During his career as an IT practitioner, he has been an adjunct professor at Kennesaw State University, Southern Polytechnic State University in Marietta, Georgia, Austin Community College in Austin, Texas, and Texas State University: San Marcos. He currently teaches undergraduate courses in Information Security, Data Communications, Local Area Networks, Database Technology, Project Management, Systems Analysis & Design, and Information Resources Management and Policy. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of the practical knowledge found in this textbook was acquired. Professor Mattord is also the co-author of *Management of Information Security*, *Principles of Incident Response and Disaster Recovery*, *Readings and Cases in the Management of Information Security*, *The Guide to Firewalls and Network Security*, and *The Hands-On Information Security Lab Manual*, all published by Course Technology.

Acknowledgments

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

Contributors

Several people and organizations have also contributed materials that were used in the preparation of this textbook, and we thank them for their contributions:

- John W. Lampe—Contributed draft content on several topics in the area of cryptography
- The National Institute of Standards and Technology is the source of many references, tables, figures and other content used in many places in the textbook

Reviewers

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

- Lonnie Decker, Davenport University-Midland
- Jeffrey Smith, Park University
- Dale Suggs, Campbell University

Special Thanks

The authors wish to thank the editorial and production teams at Course Technology. Their diligent and professional efforts greatly enhanced the final product:

- Natalie Pashoukos, Product Manager
- Lynne Raughley, Developmental Editor
- Steve Helba, Executive Editor
- Brooke Greenhouse, Content Project Manager

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

- Charles Cresson Wood
- Our colleagues in the Department of Computer Science and Information Systems, Kennesaw State University

Our Commitment

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

Foreword

Information security is an art, not a science, and the mastery of information security requires a multi-disciplinary knowledge of a huge quantity of information, experience, and skill. You will find much of the necessary information here in this book as the authors take you through the subject in a security systems development life cycle using real-life scenarios to introduce each topic. The authors provide the experience and skill of many years of real life experience, combined with their academic approach, to provide a rich learning experience that they expertly present in this book. You have chosen the authors and the book well.

Since you are reading this book, you are most likely working toward a career in information security or at least have some serious information security interest. You must anticipate that just about everybody hates the constraints that your work of increasing security will put upon them, both the good guys and the bad guys—except for malicious hackers that love the security you install as a challenge to be beaten. I concentrate on fighting the bad guys in security because when security is developed against bad guys it also applies to accidents and errors, but when developed against accidental problems, it tends to be ineffective against enemies acting with intent.

I have spent 35 years of my life working in a field that most people hate but still found it exciting and rewarding working with computers and pitting my wits against malicious people. Security controls and practices include logging on, using passwords, encrypting vital information, locking doors and drawers, motivating stakeholders to support security, and installing pipes to spray water down on your fragile computers in case of fire. These are means of protection that have no benefit except rarely when adversities occur. Good security is when nothing bad happens, and when nothing bad happens, who needs security. So why do we engage in security? Now-a-days we do it because the law says that we must do it like we are required to use seat belts and air bags—especially if we deal with the personal information of others, electronic money, intellectual property, and keeping ahead of the competition.

There is great satisfaction knowing that your employer's information, communications, systems, and people are secure, and getting paid a good salary, being the center of attention in emergencies, and knowing that you are matching your wits against the bad guys all make up for the downsides of your 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 you haven't fixed yet. The enemy has a great advantage over us. He has to find only one vulnerability and one target to attack in a known place, electronically or physically while we must defend from potentially millions of enemies' attacks against all of our assets and vulnerabilities that are no longer in one computer room but are spread all over the world by wire and now by air. It's like playing a game in which you don't know your opponents and where they are, what they are doing, why they are doing it, and are changing the rules as they play. You must be highly ethical, defensive, secretive, and cautious about bragging about the great security that you are employing that might tip off the enemy. Enjoy the few successes that you experience for you will not even know about some of them.

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

They took him out to the rifle range and told him to pretend it is a gun, aim it at the target, and go, bang, bang, bang. He did that. Then they took him out to bayonet practice, and he said, "What do I do with this broom?"

They said, "pretend it is a gun with a bayonet on it and go stab, stab, stab."

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

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

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

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

Remember that when working in security, you are in a virtual army defending your employer and stakeholders from their enemies, and from your point of view they 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 a techie with the challenging job of installing technological controls in systems and networks. Most of your work should be 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 get close to them. I spent a major part of my security career hunting down computer criminals and interviewing them and their victims trying to obtain knowledge from them to do a better job of defending from their attacks. You, likewise, should also use every opportunity to seek them out and get to know them. This experience gives you great cachet as a real and unique expert even with only minimal exposure to 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 the vulnerabilities and assets that you haven't fully protected yet. For example, one of the most common threats is endangerment of assets that means putting information assets in harm's way, yet I rarely find it on threat lists. Endangerment is also one of the most common mistakes that security professionals make. You must be thorough, meticulous, document everything (in case your competence is questioned and to meet the requirements of the Sarbanes—Oxley Law), and keep the documents safely locked away. Be careful and document so that when an adversity hits and you lose the game, you will have proof of having been 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 is due to management failing to give you an adequate budget and support for the security that you know that you need, you must have documented that before the incident occurs. Don't brag about how great your security is, because it can always be beaten. Keep, expand, and use every-day check lists of everything—threats, vulnerabilities, assets, key potential victims and suspects of wrongdoing, security supporters and those that don't bother with security, attacks, enemies, criminal justice resources, auditors, regulators, and legal council. To assist your stakeholders that are the real defenders of their information and systems in managing their security, you must identify what they must protect and measure the real extent of their security. And make sure that those to whom you report and higher management understand the nature of your job and its limitations.

You will have a huge collection of sensitive passwords to do your job. Use the best possible passwords to set a good example, write them down, and keep the list safely in your wallet next to your credit card. Know as much about the systems and networks in your organization as possible and have access to the expert people that know the rest. Make good friends of the local and national criminal justice people, your organization's lawyers, insurance risk managers, human resources people, talent, facilities managers and auditors. Audit is one of the most powerful controls that your organization has. Remember that people hate security and must be properly motivated with penalties and rewards to make it work. Seek ways to make security invisible or transparent to stakeholders, yet effective. Don't recommend or install controls or practices that they won't support, because they will beat you every time by making it look like the controls are effective but 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 and its culture that you must thoroughly understand. As an information security consultant, I was privileged to learn about the culture and secrets of more then 250 of the largest international corporations throughout the world. I had the opportunity to interview and advise the most powerful business giants if even for only a few minutes of their valuable time. You should always be ready to use the five minutes that you get with them once every year or so as your silver bullet to use with top management for the greatest benefit of their security. Carefully learn the limits of their 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 the board of directors intensely and seriously discussing and suppressing my snickering about 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 risk reduction and increased security; they are diligence to avoid negligence, exceeding compliance with all of the laws and standards and auditors, and enablement when security becomes a competitive or a budget issue. To achieve these objectives, you must develop a trusting exchange of the most sensitive security intelligence among your peers in your and other security people's organizations so that you know where your organization stands in protection relative to them. You need to know what the generally accepted current security solutions are and especially those used in your competitors' businesses or other related organizations. Therefore, you need to exchange this highly sensitive information among your peers. If the information exchanged is exposed, it could ruin your and others' careers as well as be a disaster for your or their organizations. Your personal and ethical performance must be spotless, and you must protect your reputation at all costs. Pay particular attention to the ethics section of this book. You must be discrete and careful by testing and growing the ongoing peer trust to facilitate the sharing of sensitive security information. I recommend that you join the Information Systems Security Association and become professionally certified as soon as you are qualified. My favorite is to be a Certificated Information Systems Security Professional (CISSP) offered by the International Information Systems Security Certification Consortium.

Donn B. Parker, CISSP
Los Altos, California

chapter 1

Introduction to Information Security

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

BOOK OF THE FIVE RINGS

For Amy, the day began like any other at the Sequential Label and Supply Company (SLS) help desk. Taking calls and helping office workers with computer problems was not glamorous, but she enjoyed the work; it was challenging and paid well. 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 on average about four times an hour and about 28 times a day. 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 gave some of the facts: the user's name, his phone number, the department in which he worked, where his office was on the company campus, and a list of all the calls he'd made in the past.

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

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

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

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

"Did you try a reboot yet?"

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

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

Amy looked up at the LED tally board on the wall at the end of the room. She saw that there were only two technicians dispatched to deskside support at the moment, and since it was the day shift, there were four available.

"Shouldn't be long at all, Bob."

She hung up and typed her notes into ISIS, the company's Information Status and Issues System. She assigned the newly generated case to the deskside dispatch queue, which would page the roving deskside team with the details in just 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 door of the server room where the company servers were kept in a controlled environment. They all looked worried.

Just then, Amy's screen beeped to alert her of a new e-mail. She glanced down. It beeped again—and again. It started beeping constantly. She clicked on 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, an acquaintance from the Accounting Department. The subject line said, "Wait till you see this." The message body read, "Look what this has to say about our managers' salaries…" Davey often sent her interesting and funny e-mails, and she failed to notice that the file attachment icon was unusual before she clicked it.

Her PC showed the hourglass pointer icon for a second and then the normal pointer reappeared. Nothing happened. She clicked the next e-mail message in the queue. Nothing happened. Her phone rang again. She clicked the ISIS icon on her computer desktop to activate the call management software and activated her headset. "Hello, Tech Support, how can I help you?" She couldn't greet the caller by name because ISIS had not responded.

"Hello, this is Erin Williams in receiving."

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

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

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

Then she saw Charlie running down the hall from the server room. He didn't look worried anymore. He looked frantic.

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

LEARNING OBJECTIVES:

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

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

Introduction

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

This chapter’s opening scenario illustrates that the information risks and controls are not in balance at Sequential Label and Supply. Though Amy works in a technical support role and her job is to solve technical problems, it does not occur to her that a malicious software program, like a worm or virus, might be the agent of the company’s current ills. Management also shows signs of confusion and seems to have no idea how to contain this kind of incident. If you were in Amy’s place and were faced with a similar situation, what would you do? How would you react? Would it occur to you that something far more insidious than a technical malfunction was happening at your company? As you explore the chapters of this book and learn more about information security, you will become better able to answer these questions. But before you can begin studying the details of the discipline of information security, you must first know the history and evolution of the field.

The History of Information Security

The history of information security begins with **computer security**. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats—arose during World War II when the first mainframes, developed to aid computations for communication code breaking (see Figure 1-1), were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. 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 more technologically sophisticated computer security safeguards.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the 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 an MOTD

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."[1]

Figure 1-1 The Enigma

Source: Courtesy of National Security Agency

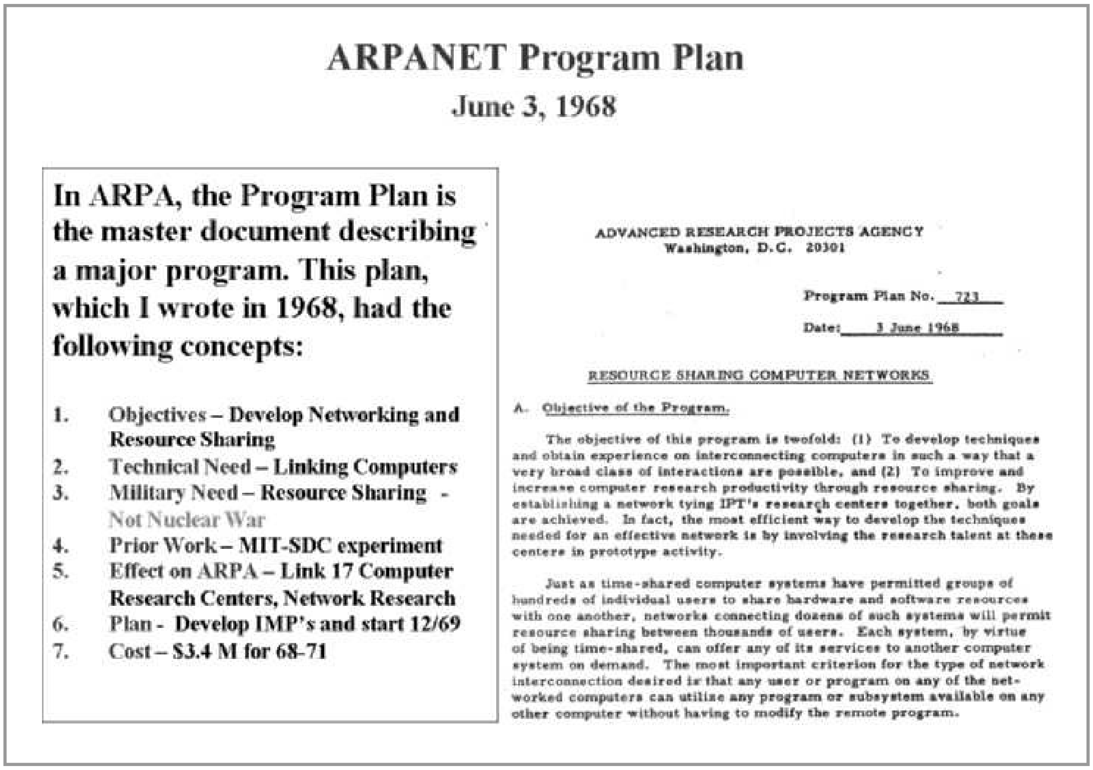
(message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.[2]

The 1960s

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project—which was called ARPANET—from its inception. ARPANET is the predecessor to the Internet (see Figure 1-2 for an excerpt from the ARPANET Program Plan).

The 1970s and 80s

During the next decade, ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. "Bob" Metcalfe, who is credited



ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Figure 1-2 Development of the ARPANET Program Plan[3]

Source: Courtesy of Dr. Lawrence Roberts

with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. 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 referred to as network insecurity.[4] In 1978, a famous study entitled "Protection Analysis: Final Report" was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security, see Table 1-1.

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

The security—or lack thereof—of the 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 for both the military and defense contractors.

Date	Documents
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems*.
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."*[5]
1975	The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the *Federal Register*.
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing 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.[6]
1979	Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for *Computing Machinery* (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the systems.
1984	Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine 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.[7]
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users ... the naive user has no chance."[8]

Table 1-1 Key Dates for Seminal Works in Early Computer Security

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609.[9]

The 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 utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems.[10] This paper signaled a pivotal moment in computer security history—when 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 matters pertaining to information security

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

In mid-1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlro) 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. In fact, it was not until the early 1970s that even the simplest component of security, the password function, became a component of UNIX.

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

The 1990s

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks 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, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks. At first, these connections were based on de facto **standards**, because industry standards for interconnection of networks did not exist at that time. These de facto standards did little to ensure the security of information though as these precursor technologies were widely adopted and became industry standards, some degree of security was introduced. However, early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of 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.

2000 to Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer's stored information is now contingent on the level of security 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 cyber attacks have made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

What Is Security?

In general, **security** is "the quality or state of being secure—to be free from danger."[11] In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

A successful organization should have the following multiple layers of security in place to protect its operations:

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
- **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
- **Operations security**, to protect the details of a particular operation or series of activities
- **Communications security**, to protect communications media, technology, and content
- **Network security**, to protect networking components, connections, and contents
- **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

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 that information.[12] Figure 1-3 shows that information security includes the broad areas of information security management, computer and 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. triangle. The **C.I.A. triangle** has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses 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 new environment of many 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

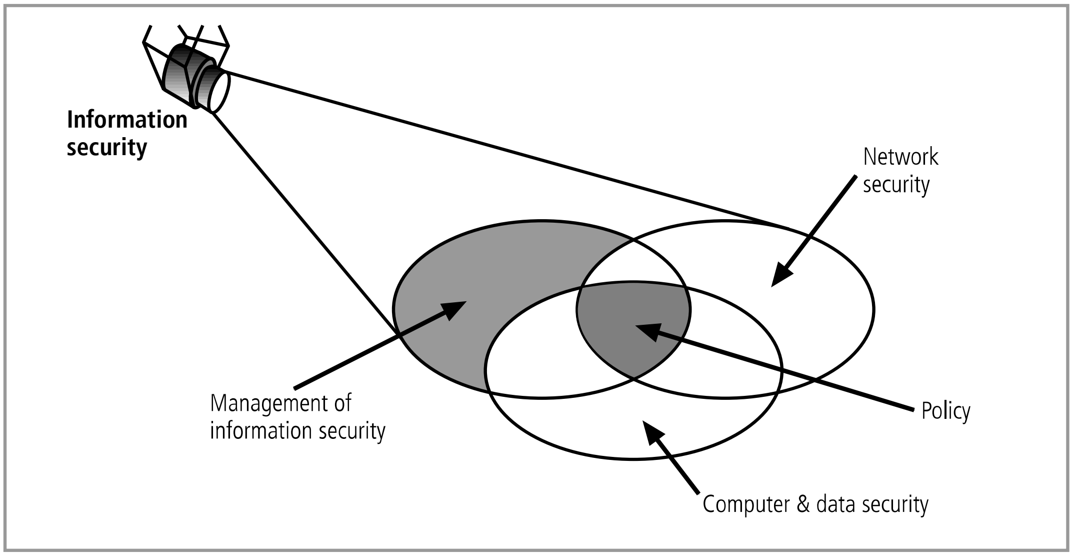


Figure 1-3 Components of Information Security

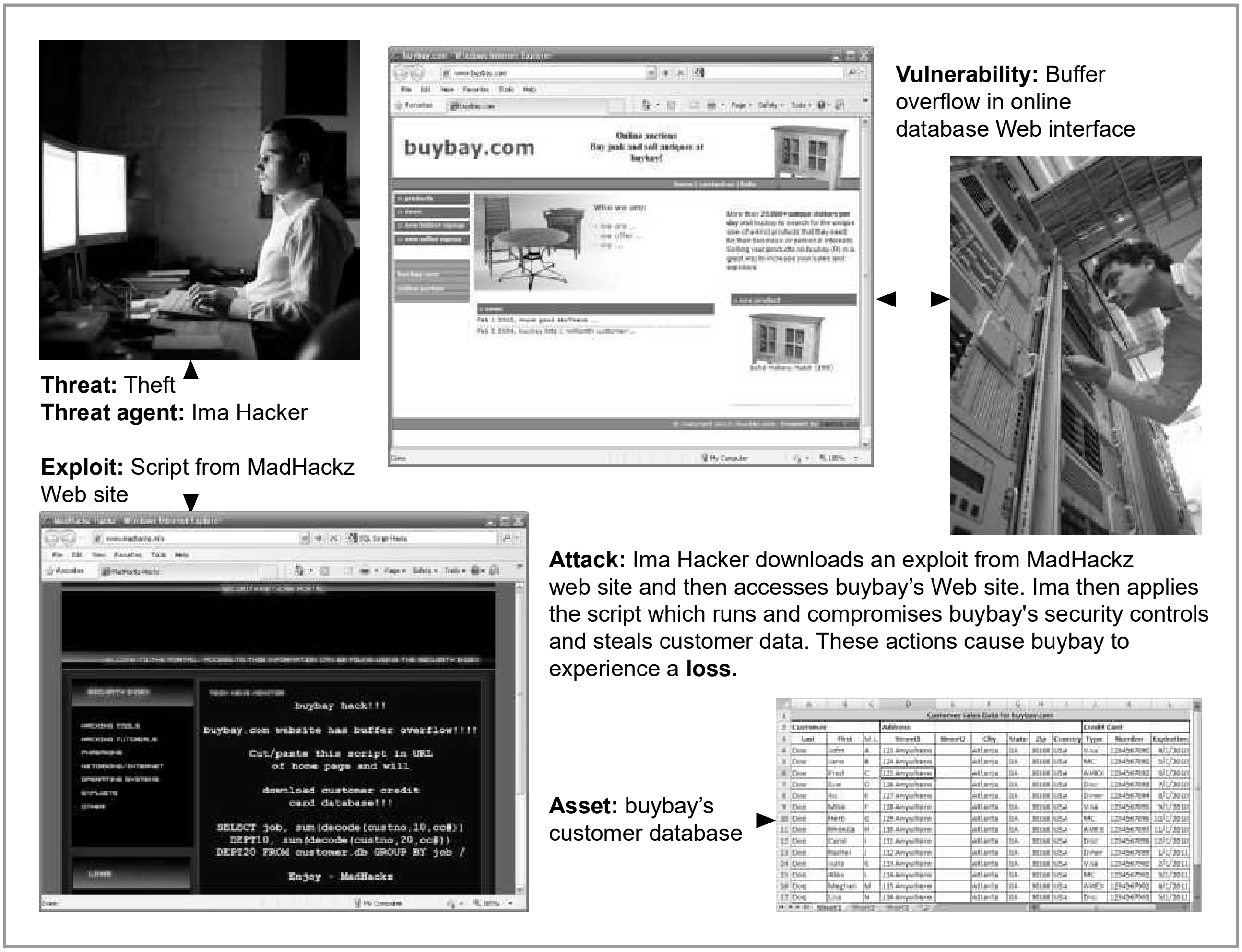
Source: Course Technology/Cengage Learning

section. C.I.A. triangle terminology is used in this chapter because of the breadth of material that is based on it.

Key Information Security Concepts

This book uses a number of terms and concepts that are essential to any discussion of information security. Some of these terms are illustrated in Figure 1-4; all are covered in greater detail in subsequent chapters.

- **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 have 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, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.
- **Attack:** An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone casually reading sensitive information not intended for his or her use is a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a fire in a building is an unintentional attack. A direct attack is a hacker using a personal computer 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.



Threat: Theft
Threat agent: Ima Hacker

Exploit: Script from MadHackz Web site

Vulnerability: Buffer overflow in online database Web interface

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

Asset: buybay's customer database

```
buybay hack!!!

buybay.com website has buffer overflow!!!!

Cut/paste this script in URL
of home page and will

download customer credit
card database!!!

SELECT job, sum(decode(custno,10,cc#))
DEPT10, sum(decode(custno,20,cc#))
DEPT20 FROM customer.db GROUP BY job /

Enjoy - MadHacks
```

buybay.com
Online auctions
Buy junk and sell antiques at buybay!
Customer Sales Data for buybay.com

Figure 1-4 Information Security Terms

Source: Course Technology/Cengage Learning

- **Control, safeguard,** or **countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization. The various levels and types of controls are discussed more fully in the following chapters.
- **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 is 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 known to an attacker is present.
- **Loss:** A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. 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 (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

- **Risk:** The probability that something unwanted will happen. Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept.
- **Subjects** and **objects:** 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, as shown in Figure 1-5. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).
- **Threat:** A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.
- **Threat agent:** The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.
- **Vulnerability:** A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. 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 do. This can depend on circumstances; for example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late. Though information security professionals and end users share an understanding of the characteristics of

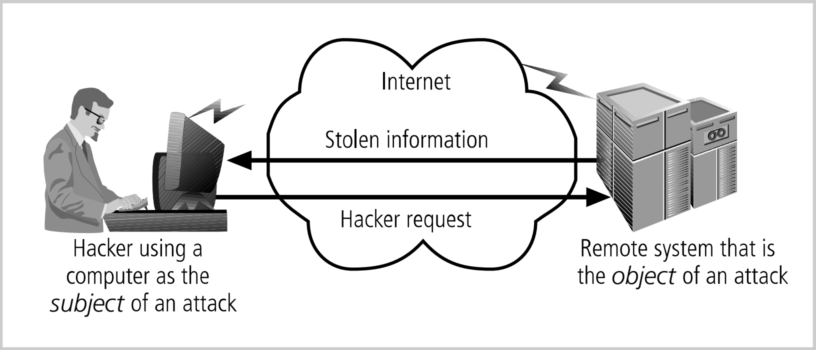

Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of an attack
Remote system that is the *object* of an attack

Figure 1-5 Computer as the Subject and Object of an Attack

Source: Course Technology/Cengage Learning

information, tensions can arise when the need to secure the information from threats conflicts with the end users' need for unhindered access to the information. For instance, end users may perceive a tenth-of-a-second delay in the computation of data to be an unnecessary annoyance. Information security professionals, however, may perceive that tenth of a second as a minor delay that enables an important task, like data encryption. Each critical characteristic of information—that is, the expanded C.I.A. triangle—is defined in the sections below.

Availability **Availability** enables authorized users—persons 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 that patron has free access to the book stacks. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language, which in this case typically means bound in a book and written in English.

Accuracy Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much 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 mistakes, such as bouncing a check.

Authenticity **Authenticity** of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. 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 the origin of the e-mail. 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 often the modified field is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computing systems.

Another variation on spoofing is **phishing**, when an attacker attempts to obtain personal or financial information using fraudulent means, most often by posing as another individual or organization. Pretending to be someone you are not is sometimes called *pretexting* when it is undertaken by law enforcement agents or private investigators. When used in a phishing attack, e-mail spoofing lures victims to a Web server that does not represent the organization it purports to, in an attempt to steal their private data such as account numbers and passwords. The most common variants include posing as a bank or brokerage company, e-commerce organization, or Internet service provider. Even when authorized, pretexting does not always lead to a satisfactory outcome. In 2006, the CEO of Hewlett-Packard

Corporation, Patricia Dunn, authorized contract investigators to use pretexting to "smokeout" a corporate director suspected of leaking confidential information. The resulting firestorm of negative publicity led to Ms. Dunn's eventual departure from the company.[13]

Confidentiality Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, you can use a number of measures, including the following:

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

Confidentiality, like most of the characteristics of information, is interdependent with other characteristics and is most closely related to the characteristic known as privacy. The relationship between these two characteristics is covered in more detail in Chapter 3, "Legal and Ethical Issues in Security."

The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients. Individuals 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, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but there are times when disclosure of confidential information happens by mistake—for example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* the organization. Several cases of privacy violation are outlined in Offline: Unintentional Disclosures.

Other examples of confidentiality breaches are an employee throwing away a document containing 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 the clients, such as names, addresses, and credit card numbers.

As a consumer, you give up pieces of confidential information in exchange for convenience or value almost daily. By using a "members only" 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. The bits and pieces of your information that you disclose are copied, sold, replicated, distributed, and eventually coalesced into profiles and even complete dossiers of yourself and your life. A similar technique is used in a criminal enterprise called **salami theft**. A deli worker knows he or she cannot steal an entire salami, but a few slices here or there can be taken home without notice. Eventually the deli worker has stolen a whole salami. In information security, salami theft occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed—but eventually the employee gets something complete or useable.

Integrity Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption,

Offline Unintentional Disclosures

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 during 2004. The perpetrators used stolen identities to create obstensibly 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 on individuals, including names, addresses, and identification numbers. They did so without using any network or computer-based attacks; it was simple fraud.[14] While the the amount of damage has yet to be compiled, the fraud is feared to have allowed the perpetrators to arrange many hundreds of instances of identity theft.

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 that the mishap was caused by a programming error that occurred when patients who used a specific drug produced by the company signed up for an e-mail service to access support materials provided by the company. About 600 patient addresses were exposed in the mass e-mail.[15]

In another incident, the intellectual property of Jerome Stevens Pharmaceuticals, a small prescription drug manufacturer from New York, was compromised when the FDA released documents the company had filed with the agency. It remains unclear whether this was a deliberate act by the FDA or a simple error; but either way, the company's secrets were posted to a public Web site for several months before being removed.[16]

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 size of the file. Another key method of assuring information integrity is **file hashing**, in which a file is read by a special algorithm that uses the value of the bits 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 recorded hash value for that file, 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 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 the error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted.

Utility The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful. For example, to a private citizen U.S. Census data can quickly become overwhelming and difficult to interpret; however, for a politician, U.S. Census data reveals information about the residents in a district, such as their race, gender, and age. This information can help form a politician's next campaign strategy.

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 of possession, a breach of possession does not always result in 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 to sell the customer records to the competition. The removal of the tapes from their secure environment is a breach of possession. But, because the data is encrypted, neither the employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach of confidentiality. Today, people caught selling company secrets face increasingly stiff fines with the likelihood of jail time. Also, companies are growing more and more reluctant to hire individuals who have demonstrated dishonesty in their past.

CNSS Security Model

The definition of information security presented in this text is based in part on the CNSS document called the National Training Standard for Information Systems Security Professionals NSTISSI No. 4011. (See *www.cnss.gov/Assets/pdf/nstissi_4011.pdf*. Since this document was written, the NSTISSC was renamed the Committee on National Security Systems (CNSS)—see *www.cnss.gov*. The library of documents is being renamed as the documents are rewritten.) This document presents a comprehensive information security model and has become a widely accepted evaluation standard for the security of information systems. The model, 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**.[17] The McCumber Cube in Figure 1-6, shows three dimensions. If 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 system security, each of the 27 areas must be properly addressed during the security process. For example, the intersection between technology, integrity, and storage requires a control or safeguard that addresses 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

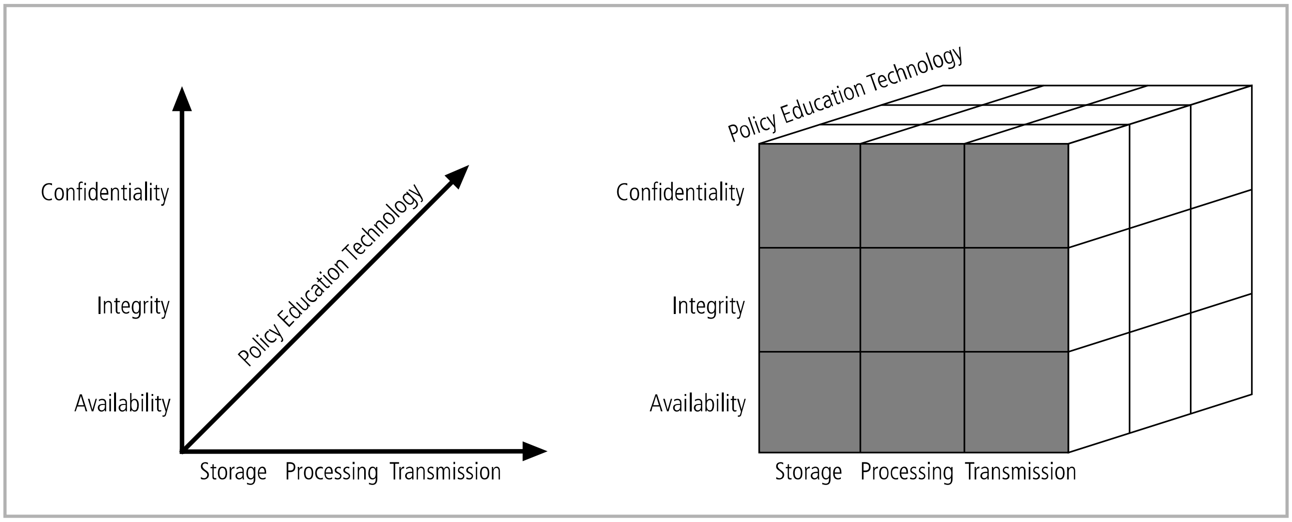

Confidentiality
Integrity
Availability
Policy Education Technology
Storage Processing Transmission
Policy Education Technology
Confidentiality
Integrity
Availability
Storage Processing Transmission

Figure 1-6 The McCumber Cube[18]

Source: Course Technology/Cengage Learning

information by alerting the security administrators to the potential modification of a critical file. What is commonly left out of 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 chapters of this book.

Components of an Information System

As shown in Figure 1-7, an **information system (IS)** is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.

Software

The software component of the IS comprises applications, 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 information technology 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, cost, 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.

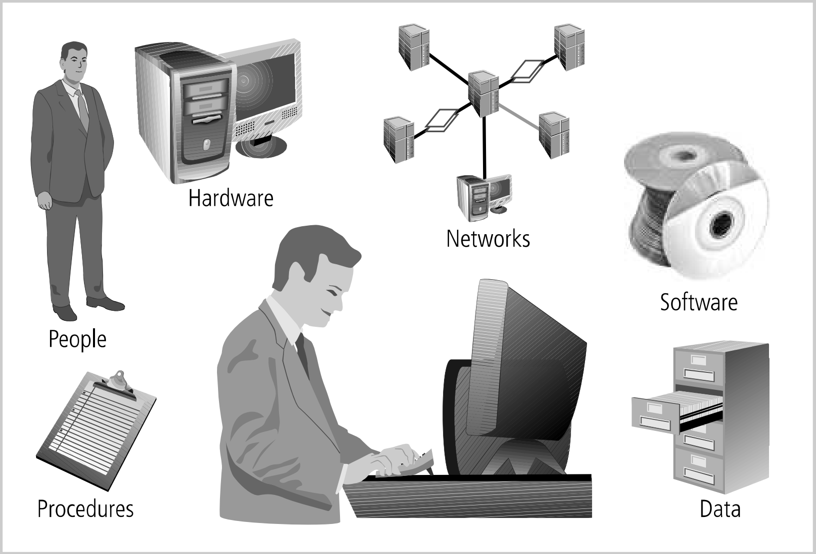


Figure 1-7 Components of an Information System

Source: Course Technology/Cengage Learning

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 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 access to the hardware 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 the target until the target placed his/her computer on the baggage scanner. As the computer was whisked through, the second agent slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, thereby 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, 2001 did tighten the security process at airports, hardware can still be stolen in airports and other public places. Although laptops and notebook computers are worth a few thousand dollars, the information contained in them can be worth a great deal more to organizations and individuals.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

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 invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for thousands of 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 moral of the story is that people can be the weakest link in an organization's information security program. And 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 the actions of people to obtain access information about a system. This topic is discussed in more detail in Chapter 2, "The Need for Security."

Procedures

Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this 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), this bank consultant ordered millions of dollars to be transferred by wire to his own account. Lax security procedures caused the loss of over ten million dollars before the situation was corrected. Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures. 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 the organization only on a need-to-know basis.

Networks

The IS component that created much of the need for increased computer and information security is networking. When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. The physical technology that enables network functions is becoming more and more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough. Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

Balancing Information Security and Access

Even with the best planning and implementation, it is impossible to obtain perfect information security. Recall James Anderson's statement from the beginning of this chapter, which emphasizes the need to balance security and access. Information security cannot be absolute: it is a process, not a goal. It is possible to 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. For instance, when challenged to achieve a TCSEC C-2 level security certification for its Windows operating system, Microsoft had to remove all networking components and operate the computer from only the console in a secured room.[19]

To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats. Figure 1-8 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 too heavy a focus on protecting and administering the information systems. Both information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure the data is available when, where, and how it is needed, with

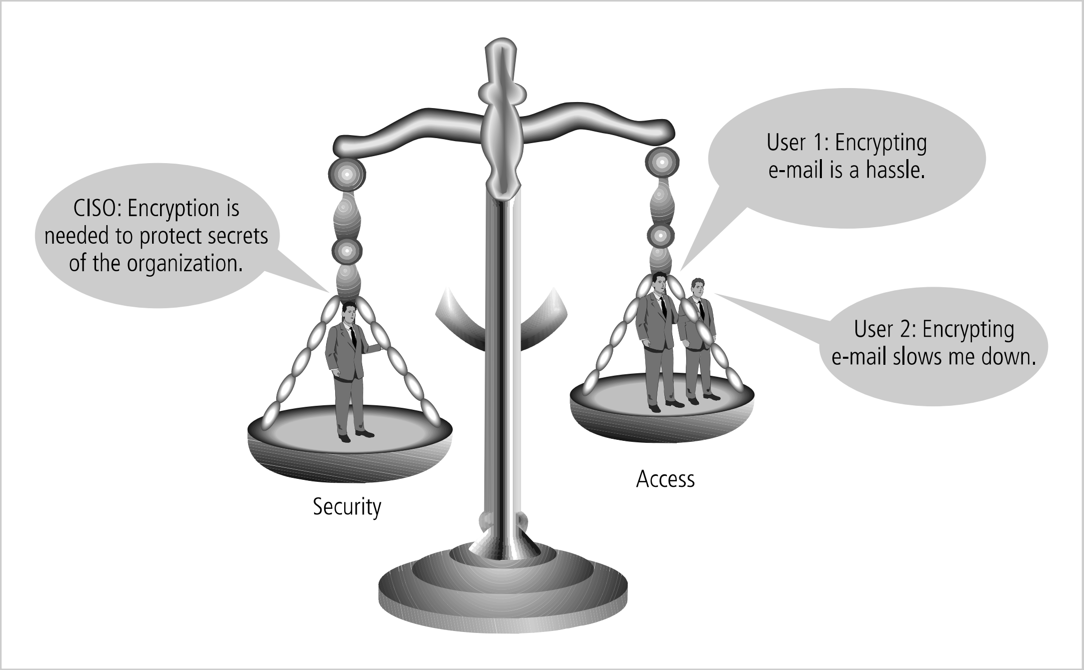

CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down.
Security
Access

Figure 1-8 Balancing Information Security and Access

Source: Course Technology/Cengage Learning

minimal delays or obstacles. In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.

Approaches to Information Security Implementation

The implementation of information security in an organization must begin somewhere, and cannot happen overnight. Securing information assets is in fact an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a **bottom-up approach**. The key advantage of the bottom-up approach is the technical expertise of the individual administrators. 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, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

The **top-down approach**—in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action—has a higher probability of success. 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 referred to as a systems development life cycle.

For any organization-wide effort to succeed, management must buy into and fully support it. The role played in this effort by the champion cannot be overstated. Typically, this champion is an executive, such as a chief information officer (CIO) or the vice president of information technology (VP-IT), who 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. Also critical to the success of this type of project is the involvement and support of the end users. These individuals 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 developmental team, known as the joint application development team (JAD). 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.

The organizational hierarchy and the bottom-up and top-down approaches are illustrated in Figure 1-9.

The Systems Development Life Cycle

Information security must be managed in a manner similar to any other major system implemented in an organization. One approach for implementing an information security system in

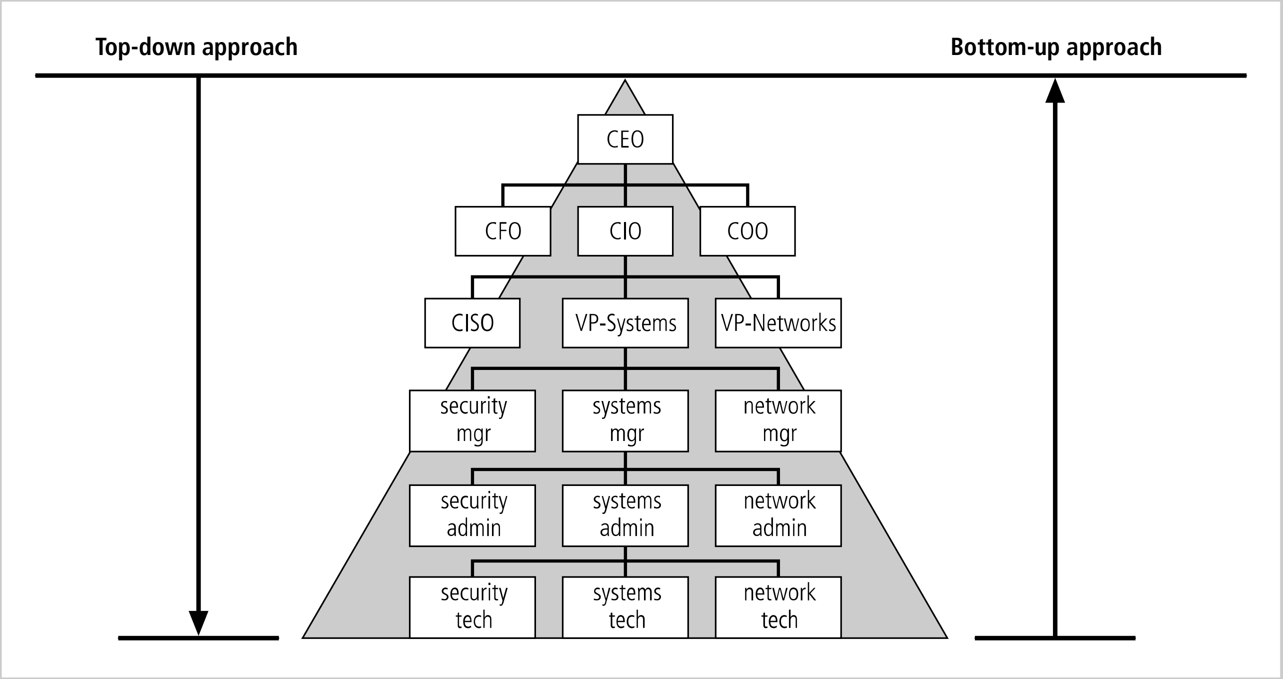


Figure 1-9 Approaches to Information Security Implementation

Source: Course Technology/Cengage Learning

an organization with little or no formal security in place is to use a variation of the systems development life cycle (SDLC): the security systems development life cycle (SecSDLC). To understand a *security* systems development life cycle, you must first understand the basics of the method upon which it is based.

Methodology and Phases

The **systems development life cycle** (**SDLC**) is a methodology for the design and implementation of an information system. A **methodology** is a formal approach to solving a problem by means of a structured sequence of procedures. Using a methodology ensures a rigorous process with a clearly defined goal and increases the probability of success. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected and made accountable for accomplishing the project goals.

The traditional SDLC consists of six general phases. If you have taken a system analysis and design course, you may have been exposed to a model consisting of a different number of phases. SDLC models range from having three to twelve phases, all of which have been mapped into the six presented here. The **waterfall model** pictured in Figure 1-10 illustrates that each phase begins with the results and information gained from the previous phase.

At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources.

Once the system is implemented, it is maintained (and modified) over the remainder of its operational life. Any information systems implementation may have multiple iterations as the cycle is repeated over time. Only by means of constant examination and renewal can

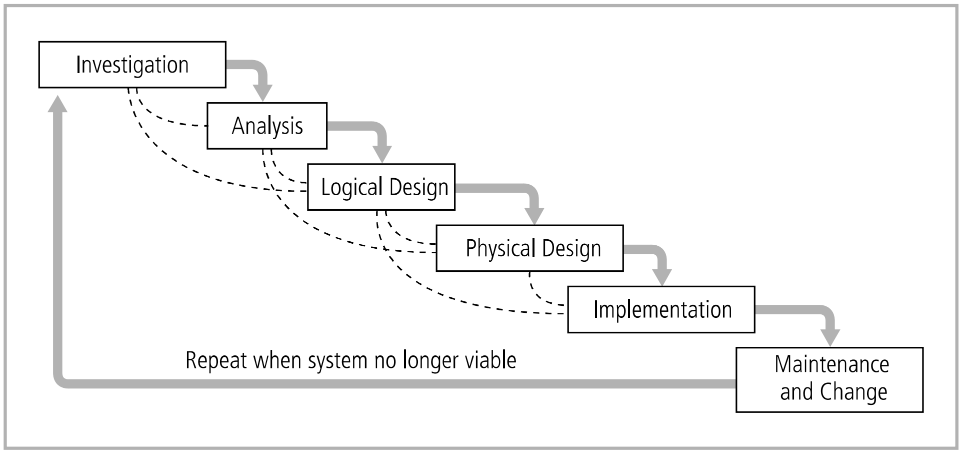


Figure 1-10 SDLC Waterfall Methodology

Source: Course Technology/Cengage Learning

any system, especially an information security program, perform up to expectations in the constantly changing environment in which it is placed.

The following sections describe each phase of the traditional SDLC.[20]

Investigation

The first phase, investigation, is the most important. What problem is the system being developed to solve? The investigation phase begins with an examination of the event or plan that initiates the process. During the investigation phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems. Analysts begin by determining what the new system is expected to do and how it will interact with existing systems. This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

Physical Design

During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

Implementation

In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

Maintenance and Change

The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed. As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.

Securing the SDLC

Each of the phases of the SDLC should include consideration of the security of the system being assembled as well as the information it uses. Whether the system is custom and built from scratch, is purchased and then customized, or is commercial off-the-shelf software (COTS), the implementing organization is responsible for ensuring it is used securely. This means that each implementation of a system is secure and does not risk compromising the confidentiality, integrity, and availability of the organization's information assets. The following section, adapted from NIST Special Publication 800-64, rev. 1, provides an overview of the security considerations for each phase of the SDLC.

> *Each of the example SDLC phases [discussed earlier] includes a minimum set of security steps needed to effectively incorporate security into a system during its*

development. An organization will either use the general SDLC described [earlier] or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

Investigation/Analysis Phases

- *Security categorization—defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.*
- *Preliminary risk assessment—results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.*

Logical/Physical Design Phases

- *Risk assessment—analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.*
- *Security functional requirements analysis—analysis of requirements that may include the following components: (1) system security environment (i.e., enterprise information security policy and enterprise security architecture) and (2) security functional requirements*
- *Security assurance requirements analysis—analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.*
- *Cost considerations and reporting—determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training.*
- *Security planning—ensures that agreed upon security controls, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/ accreditations, and plan of action and milestones).*
- *Security control development—ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development of additional security controls to supplement the*

controls already in place or the modification of selected controls that are deemed to be less than effective.

- *Developmental security test and evaluation—ensures that security controls developed for a new information system are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed—these controls are typically management and operational controls.*
- *Other planning components—ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation by all necessary functional groups within an organization, participation by the certifier and accreditor, and development and execution of necessary contracting plans and processes.*

Implementation Phase

- *Inspection and acceptance—ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables.*
- *System integration—ensures that the system is integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.*
- *Security certification—ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the information system.*
- *Security accreditation—provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.*

Maintenance and Change Phase

- *Configuration management and control—ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.*
- *Continuous monitoring—ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials is an essential activity of a comprehensive information security program.*

- *Information preservation—ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.*
- *Media sanitization—ensures that data is deleted, erased, and written over as necessary.*
- *Hardware and software disposal—ensures that hardware and software is disposed of as directed by the information system security officer.*

Adapted from Security Considerations in the Information System Development Life Cycle.[21]

It is imperative that information security be designed into a system from its inception, rather than added in during or after the implementation phase. Information systems that were designed with no security functionality, or with security functions added as an afterthought, often require constant patching, updating, and maintenance to prevent risk to the systems and information. It is a well-known adage that "an ounce of prevention is worth a pound of cure." With this in mind, organizations are moving toward more security-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but consumer confidence in their products. In early 2002, Microsoft effectively suspended development work on many of its products while it put its OS developers, testers, and program managers through an intensive program focusing on secure software development. It also delayed release of its flagship server operating system to address critical security issues. Many other organizations are following Microsoft's recent lead in putting security into the development process.

The Security Systems Development Life Cycle

The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project. While the two processes may differ in intent and specific activities, the overall methodology is the same. At its heart, implementing information security involves identifying specific threats and creating specific controls to counter those threats. The SecSDLC unifies this process and makes it a coherent program rather than a series of random, seemingly unconnected actions. (Other organizations use a risk management approach to implement information security systems. This approach is discussed in subsequent chapters of this book.)

Investigation

The investigation phase of the SecSDLC begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints. Frequently, this phase begins with an **enterprise information security policy** (**EISP**), which outlines the implementation of a security program within the organization. Teams of responsible managers, employees, and contractors are organized; problems are analyzed; and the scope of the project, as well as specific goals and objectives and any additional constraints not covered in the program policy, are defined. Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design. The EISP is covered in depth in Chapter 5 of this book.

Analysis

In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented legislation making certain computer-related activities illegal. A detailed understanding of these issues is vital. Risk management also begins in this stage. **Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization. Risk management is described in detail in Chapter 4 of this book.

Logical Design

The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions. Also at this stage, the team plans the incident response actions to be taken in the event of partial or catastrophic loss. The planning answers the following questions:

- Continuity planning: How will business continue in the event of a loss?
- Incident response: What steps are taken when an attack occurs?
- Disaster recovery: What must be done to recover information and vital systems immediately after a disastrous event?

Next, a feasibility analysis determines whether or not the project should be continued or be outsourced.

Physical Design

The physical design phase evaluates the information security technology needed to support the blueprint outlined in the logical design generates alternative solutions, and determines a final design. The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of this phase, a feasibility study determines the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design. At this time, all parties involved have a chance to approve the project before implementation begins.

Implementation

The implementation phase in of SecSDLC is also similar to that of the traditional SDLC. The security solutions are acquired (made or bought), tested, implemented, and tested again. Personnel issues are evaluated, and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval.

Maintenance and Change

Maintenance and change is the last, though perhaps most important, phase, given the current ever-changing threat environment. Today's information security systems need constant

Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Steps unique to the security systems development life cycle
Phase 1: Investigation	• Outline project scope and goals • Estimate costs • Evaluate existing resources • Analyze feasibility	• Management defines project processes and goals and documents these in the program security policy
Phase 2: Analysis	• Assess current system against plan developed in Phase 1 • Develop preliminary system requirements • Study integration of new system with existing system • Document findings and update feasibility analysis	• Analyze existing security policies and programs • Analyze current threats and controls • Examine legal issues • Perform risk analysis
Phase 3: Logical Design	• Assess current business needs against plan developed in Phase 2 • Select applications, data support, and structures • Generate multiple solutions for consideration • Document findings and update feasibility analysis	• Develop security blueprint • Plan incident response actions • Plan business response to disaster • Determine feasibility of continuing and/or outsourcing the project
Phase 4: Physical Design	• Select technologies to support solutions developed in Phase 3 • Select the best solution • Decide to make or buy components • Document findings and update feasibility analysis	• Select technologies needed to support security blueprint • Develop definition of successful solution • Design physical security measures to support techno logical solutions • Review and approve project
Phase 5: Implementation	• Develop or buy software • Order components • Document the system • Train users • Update feasibility analysis • Present system to users • Test system and review performance	• Buy or develop security solutions • At end of phase, present tested package to management for approval
Phase 6: Maintenance and Change	• Support and modify system during its useful life • Test periodically for compliance with business needs • Upgrade and patch as necessary	• Constantly monitor, test, modify, update, and repair to meet changing threats

Table 1-2 **SDLC and SecSDLC Phase Summary**

monitoring, testing, modification, updating, and repairing. Applications systems developed within the framework of the traditional SDLC are not designed to anticipate a software attack that requires some degree of application reconstruction. In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary. As new threats emerge and old threats evolve, the information security profile of an organization must constantly adapt to prevent threats from successfully penetrating sensitive data. This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.

Table 1-2 summarizes the steps performed in both the systems development life cycle and the security systems development life cycle. Since the security systems development life cycle is based on the systems development life cycle, the steps in the cycles are similar, and thus those common to both cycles are outlined in column 2. Column 3 shows the steps unique to the security systems development life cycle that are performed in each phase.

Security Professionals and the Organization

It takes a wide range of professionals to support a diverse information security program. As noted earlier in this chapter, 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. But administrative support is also essential to developing and executing specific security policies and procedures, and technical expertise is of course essential to implementing the details of the information security program. The following sections describe the typical information security responsibilities of various professional roles in an organization.

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 the strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the organization as a whole into strategic information plans for the information systems or data processing 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.

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 a similar title. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to 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 placement of the CISO and supporting security staff in organizational hierarchies is the subject of current debate across the industry.[22]

Information Security Project Team

The information security **project team** should consist of a number of individuals 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 security project 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 be a departmental line manager or staff unit manager, 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 the 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 applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

The three types of data ownership and their respective responsibilities are outlined below:

- **Data owners:** Those responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners usually determine the level of data classification (discussed later), 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 are responsible for the storage, maintenance, and protection of the information. 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 users:** End users who work with the information to perform their assigned roles supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

Communities of Interest

Each organization develops and maintains its own unique culture and values. Within each **organizational culture**, there are communities of interest that develop and evolve. As defined here, a **community of interest** is 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. While there can be many different communities of interest in an organization, 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; in practice, this is often not the case.

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 resources 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, 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 and functioning as expected. In information security such technologists are sometimes called *security artisans*.[23] 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 of the transistors in a CPU, the interaction of the various digital devices, and the memory storage units on the circuit boards, it's a miracle these things 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 there are many manuals to support individual systems, there is no manual for implementing 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 these faults.

The faults that remain are usually the result of technology malfunctioning for any one of a thousand possible 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 some of the components of art and science and adds another dimension to the discussion. Social science examines the behavior of individuals as they interact with systems, whether these are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people that interact with the system, intentionally or otherwise. End users who need the very information the security personnel are trying to protect may be the weakest link in the security chain. By understanding some of the 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.

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-Boats Codes, 1939–1943* by David Kahn, 1991, Houghton Mifflin.
- Glossary of Terms Used in Security and Intrusion Detection by SANS Institute. This 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 can be accessed online at *www.faqs.org/rfcs/rfc2828.html*.

Chapter Summary

- Information security evolved from the early field of computer security.
- Security is protection from danger. There are a number of types of security: physical security, personal security, operations security, communications security, national security, and network security, to name a few.
- Information security is the protection of information assets that use, store, or transmit information from risk through the application of policy, education, and technology.
- The critical characteristics of information, among them confidentiality, integrity, and availability (the C.I.A. triangle), must be protected at all times; this protection is implemented by multiple measures (policies, education training and awareness, and technology).
- Information systems are made up of six major components: 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, whereby individuals choose security implementation strategies.
- The traditional systems development life cycle (SDLC) is an approach to implementing a system in an organization and has been adapted to provide the outline of a security systems development life cycle (SecSDLC).
- The control and use of data in the organization is accomplished by
  - Data owners—responsible for the security and use of a particular set of information
  - Data custodians—responsible for the storage, maintenance, and protection of the information
  - Data users—work with the information to perform their daily jobs supporting 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 also comprises many aspects of social science.

Review Questions

1. What is the difference between a threat agent and a threat?
2. What is the difference between vulnerability and exposure?
3. How is infrastructure protection (assuring the security of utility services) related to 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. triangle? What are they used for?
6. If the C.I.A. triangle 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 system is the father of almost all modern multiuser systems?
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. Why is a methodology important in the implementation of information security? How does a methodology improve the process?
13. Which members of an organization are involved in the security system development life cycle? Who leads the process?
14. How can the practice of information security be described as both an art and a science? How does security as a social science influence its practice?
15. Who is ultimately responsible for the security of information in the organization?
16. What is the relationship between the MULTICS project and the early development of computer security?
17. How has computer security evolved into modern information security?
18. What was important about Rand Report R-609?
19. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these wishes are carried out?
20. Who should lead a security team? Should the approach to security be more managerial or technical?

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 areas previously unexamined?
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 occupying that cell.
3. Consider the information stored on your personal computer. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.
4. Using the Web, identify the chief information officer, chief information security officer, and systems administrator for your school. Which of these individuals represents the data owner? Data custodian?
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.

Case Exercises

The next day at SLS found everyone in technical support busy restoring computer systems to their former state and installing new virus and worm control software. Amy found herself learning how to install desktop computer operating systems and applications as SLS made a heroic effort to recover from the attack of the previous day.

Questions:

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

Endnotes

1. *Bletchley Park—Home of the Enigma machine*. Accessed 15 April 2010 from *http://churchwell.co.uk/bletchley-park-enigma.htm.*
2. Peter Salus. "Net Insecurity: Then and Now (1969–1998)." *Sane '98 Online*. 19 November 1998. Accessed 26 March 2007 from *www.nluug.nl/events/sane98/aftermath/salus.html.*
3. Roberts, Larry. "Program Plan for the ARPANET." Accessed 26 March 2007 from *www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.*
4. Roberts, Larry. "Program Plan for the ARPANET." Accessed 8 February 2007 from *www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.*

5. Schell, Roger R., Downey, Peter J., and Popek, Gerald J. *Preliminary Notes on the Design of Secure Military Computer System*. January 1973. File, MCI-73-1, ESD/AFSC, Hanscom AFB, Bedford, MA 01731.

6. Bisbey, Richard, Jr., and Hollingsworth, Dennis. *Protection Analysis: Final Report*. May 1978. Final report, ISI/SR-78-13, USC/Information Sciences Institute, Marina Del Rey, CA 90291.

7. Grampp, F. T., and Morris, R. H. "UNIX Operating System Security." *AT&T Bell Laboratories Technical Journal* 63, no. 8 (1984): 1649–1672.

8. Peter Salus. "Net Insecurity: Then and Now (1969–1998)." *Sane '98 Online*. 19 November 1998. Accessed 26 March 2007 from *www.nluug.nl/events/sane98/aftermath/salus.html*.

9. Willis Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." *Rand Online*. 10 October 1979. Accessed 8 February 2007 from *www.rand.org/pubs/reports/R609-1/R609.1.html*.

10. Willis Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." *Rand Online*. 10 October 1979. Accessed 8 February 2004 from *www.rand.org/publications/R/R609.1/R609.1.html*.

11. Merriam-Webster. "security." *Merriam-Webster Online*. Accessed 8 February 2007 from *www.m-w.com/dictionary/security*.

12. National Security Telecommunications and Information Systems Security. *National Training Standard for Information Systems Security (Infosec) Professionals*. 20 June 1994. File, 4011. Accessed 8 Feb 2007 from *www.cnss.gov/Assets/pdf/nstissi_4011.pdf*.

13. Lemos, R. "HP's pretext to spy," *Security Focus Online*. Accessed 21 June 2007 from *www.securityfocus.com/brief/296*.

14. "ChoicePoint Data Theft Affected Thousands." *Wall Street Journal* (Eastern edition). 22 February 2005. New York, 1.

15. Dash, J. "ACLU Knocks Eli Lilly for Divulging E-Mail Addresses," *Computerworld* 35, no. 28 (9 July 2001): 6.

16. CyberCrime Staff. "FDA Flub." *G4*. Accessed 8 February 2007 from *www.g4tv.com/techtvvault/features/39450/FDA_Flub.html*.

17. Wikipedia. "The McCumber Cube." Accessed 16 February 2007 from *http://en.wikipedia.org/wiki/McCumber_cube*.

18. 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.

19. Microsoft. "C2 Evaluation and Certification for Windows NT (Q93362)." *Microsoft Online*. 1 November 2006. Accessed 25 January 2007 from *http://support.microsoft.com/default.aspx?scid=kb;en-us;93362*.

20. Adapted from Sandra D. Dewitz. *Systems Analysis and Design and the Transition to Objects*. 1996. New York: McGraw Hill Publishers, 94.

21. Grance, T., Hash, J., and Stevens, M. *Security Considerations in the Information System Development Life Cycle*. NIST Special Publication 800-64, rev. 1. Accessed 16 February 2007 from *http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf*.

22. Mary Hayes. "Where The Chief Security Officer Belongs." *InformationWeek* no. 877 (25 February 2002): 38.

23. D. B. Parker. *Fighting Computer Crime*. 1998. New York: Wiley Publishing, 189.

chapter 2

The Need for Security

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

WILLIAM SHAKESPEARE (1564–1616),
KING HENRY, IN HENRY V, ACT 4, SC. 1, L. 6-7.

Fred Chin, CEO of sequential label and supply, 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 their quarterly meeting.

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

Gladys replied, "I think we have a real problem, and we need to put together a real solution, not just a quick patch like the last time." Eighteen months ago, the network had been infected by an employee's personal USB drive. To prevent this from happening again, all users in the company were banned from using USB drives.

Fred wasn't convinced. "Can't we just add another thousand dollars 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 have some experience at other firms and I've been researching information security, and 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 expenses and lost production from the worm 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 setting up a computer security solution, we need to develop an information security program. We need a thorough review of our policies and practices, and we need to establish an ongoing risk management program. There are some other things that are part of the process as well, but these would be a good start."

"Sounds expensive," said Fred.

Charlie looked at Gladys, then answered, "Well, there will be some extra expenses for specific controls and software tools, and we may have to slow down our product development projects a bit, but the program will be more of a change in our attitude about security than 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 spend any money."

Fred thought about this for a few seconds. "OK. 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 appoint or hire a person to be responsible for information security."

"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: procedures, data, networks, our staff, and computers."

"I see," Fred said. "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."

LEARNING OBJECTIVES:

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

- Demonstrate that organizations have a business need for information security
- Explain why a successful information security program is the responsibility of both an organization's general management and IT management
- Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate *threats* to the information within systems from *attacks* against the information within systems
- Describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure and reliable

Introduction

Unlike any other information technology program, the primary mission of an information security program is to ensure that systems and their contents remain the same. Organizations expend hundreds of thousands of dollars and thousands of man-hours to maintain their information systems. If threats to information and systems didn't exist, these resources could be used to improve the systems that support the information. However, attacks on information systems are a daily occurrence, and the need for information security grows along with the sophistication of such attacks.

Organizations must understand the environment in which information systems operate so that their information security programs can address actual and potential problems. This chapter describes this environment and identifies the threats it poses to organizations and their information.

Business Needs First

Information security performs four important functions for an organization:

1. Protecting the organization's ability to function
2. Enabling the safe operation of applications running on the organization's IT systems
3. Protecting the data the organization collects and uses
4. Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

Both general management and IT management are responsible for implementing information security 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, in fact, implementing information security has more to do with *management* than with *technology*. Just as managing payroll has more to do with management than with mathematical wage computations, managing information security has more to do with policy and its enforcement than with 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.

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, electronic mail (e-mail), and instant messaging (IM) applications. Organizations acquire these elements from a service provider or they build 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.

Protecting Data that Organizations Collect and Use

Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Any business, educational institution, or government agency operating 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 motion* and *data at rest* are both critical aspects 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.

Safeguarding Technology Assets in Organizations

To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool. When an organization grows, it must develop additional security services. For example, organizational growth could lead to the need for public key infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

Chapter 8 describes PKI in more detail, but for now know that PKI involves the use of digital certificates to ensure the confidentiality of Internet communications and transactions. Into each of these digital certificates, a certificate authority embeds an individual's or an organization's public encryption key, along with other identifying information, and then cryptographically signs the certificate with a tamper-proof seal, thus verifying the integrity of the data within the certificate and validating its use.

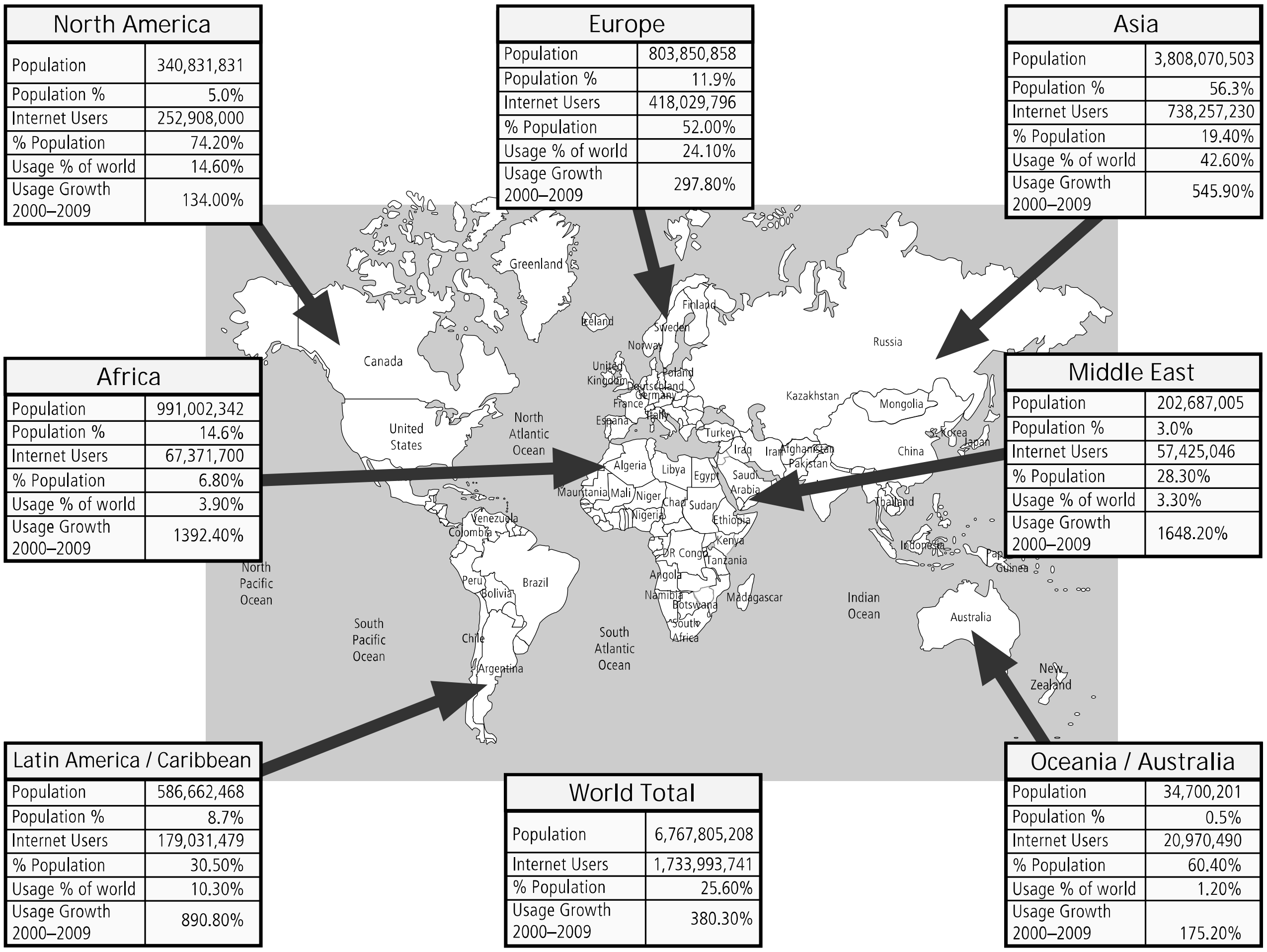
In general, as an organization's network grows to accommodate changing needs, more robust technology solutions should replace security programs the organization has outgrown. An example of a robust solution is a firewall, a mechanism that keeps certain kinds of network traffic out of a private network. Another example is caching network appliances, which are devices that store local copies of Internet content, such as Web pages that are frequently accessed by employees. The appliance displays the cached pages to users, rather than accessing the pages from the server each time.

Threats

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 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. In the context of information security, a **threat** is an object, person, or other entity that presents an ongoing danger to an asset.

To investigate the wide range of threats that pervade the interconnected world, researchers have interviewed practicing information security personnel and examined information security literature. While the categorizations may vary, threats are relatively well researched and, consequently, fairly well understood. There is wide agreement that the threat from external sources increases when an organization connects to the Internet. The number of Internet users continues to grow; about 26 percent of the world's 6.8 billion people—that is, 1.7 billion people—have some form of Internet access. Figure 2-1 shows Internet usage by continent.

The Computer Security Institute (CSI) Computer Crime and Security Survey is a representative study. The 2009 CSI study found that 64 percent of organizations responding to the survey suffered malware infections, with only 14 percent indicating system penetration by an outsider. Organizations reported losses of approximately $234,244 per respondent, down from an all-time high of more than $3 million in 2001. The figures haven't topped



North America	
Population	340,831,831
Population %	5.0%
Internet Users	252,908,000
% Population	74.20%
Usage % of world	14.60%
Usage Growth 2000–2009	134.00%

Europe	
Population	803,850,858
Population %	11.9%
Internet Users	418,029,796
% Population	52.00%
Usage % of world	24.10%
Usage Growth 2000–2009	297.80%

Asia	
Population	3,808,070,503
Population %	56.3%
Internet Users	738,257,230
% Population	19.40%
Usage % of world	42.60%
Usage Growth 2000–2009	545.90%

Africa	
Population	991,002,342
Population %	14.6%
Internet Users	67,371,700
% Population	6.80%
Usage % of world	3.90%
Usage Growth 2000–2009	1392.40%

Middle East	
Population	202,687,005
Population %	3.0%
Internet Users	57,425,046
% Population	28.30%
Usage % of world	3.30%
Usage Growth 2000–2009	1648.20%

Latin America / Caribbean	
Population	586,662,468
Population %	8.7%
Internet Users	179,031,479
% Population	30.50%
Usage % of world	10.30%
Usage Growth 2000–2009	890.80%

World Total	
Population	6,767,805,208
Internet Users	1,733,993,741
% Population	25.60%
Usage Growth 2000–2009	380.30%

Oceania / Australia	
Population	34,700,201
Population %	0.5%
Internet Users	20,970,490
% Population	60.40%
Usage % of world	1.20%
Usage Growth 2000–2009	175.20%

Figure 2-1 World Internet Usage[3]

Source: Course Technology/Cengage Learning

Offline
Violating Software Licenses

Adapted from "Bootlegged Software Could Cost Community College"[8]

By Natalie Patton, *Las Vegas Review Journal*, September 18, 1997.

Ever heard of the software police? The Washington-based Software Publishers Association (SPA) copyright watchdogs were tipped off that a community college in Las Vegas, Nevada was using copyrighted software in violation of the software licenses. The SPA spent months investigating the report. Academic Affairs Vice President Robert Silverman said the college was prepared to pay some license violation fines, but was unable to estimate the total amount of the fines. The college cut back on new faculty hires and set aside over 1.3 million dollars in anticipation of the total cost.

The audit was intensive, examining every computer on campus, including faculty machines, lab machines, and the college president's computer. Peter Beruk, SPA's director of domestic antipiracy cases, said the decision to audit a reported violation is only made when there is overwhelming evidence to win a lawsuit, as the SPA has no policing authority and can only bring civil actions. Most of the investigated organizations settle out of court, agreeing to pay the fines, to avoid costly court battles.

The process begins with an anonymous tip, usually from an individual inside the organization. Of the hundreds of tips the SPA receives each week, only a handful are selected for onsite visits. If the audited organizations have license violations they are required to destroy illegal copies, repurchase software they wish to keep (at double the retail price), and pay the proper licensing fees for the software that was used illegally.

In this case, the community college president suggested the blame for the community college's violations belonged to faculty and students who may have downloaded illegal copies of software from the Internet or installed software on campus computers without permission. Some of the faculty suspected that the problem lay in the qualifications and credibility of the campus technology staff. The president promised to put additional staff and rules in place to prevent a reoccurrence of such license violations.

of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business.

Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**. Many individuals and organizations do not purchase software as mandated by the owner's license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, he or she has violated the copyright. The Offline, *Violating Software Licenses*, describes a classic case of this type of copyright violation. Software licenses are strictly enforced by a number of regulatory and private organizations, and software publishers use several control mechanisms to prevent copyright infringement. In addition to the laws against software piracy, two watchdog organizations investigate allegations of software abuse: the Software & Information Industry Association (SIIA) at *www.siia.net*, formerly known as the Software Publishers Association, and the Business Software Alliance (BSA) at *www.bsa.org*. A BSA survey in May 2006 revealed that as much as a third of all software in use globally is pirated. Additional details on these organizations and how they operate to protect IP rights are provided in Chapter 3.

A number of technical mechanisms—digital watermarks and embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool, a license agreement window that usually pops up during the installation of new software, establishes that the user has read and agrees to the license agreement.

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

Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**, or sometimes **malware**. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

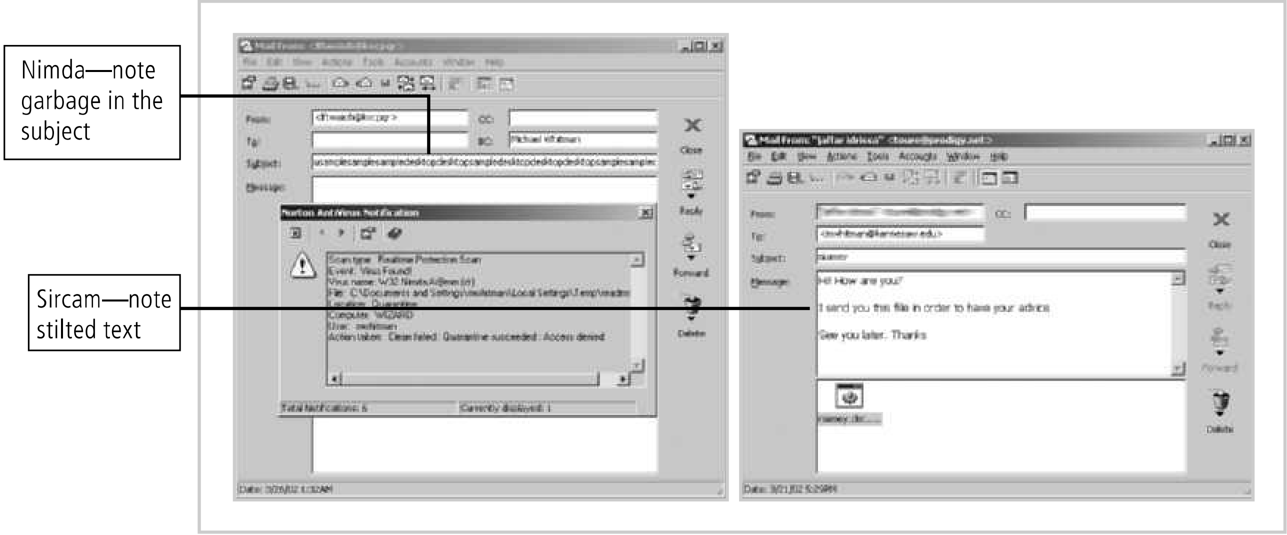
Prominent among the history of notable incidences of malicious code are the denial-of-service attacks conducted by Mafiaboy (mentioned earlier) on Amazon.com, CNN.com, ETrade.com, ebay.com, Yahoo.com, Excite.com, and Dell.com. These software-based attacks lasted approximately four hours, and are reported to have resulted in millions of dollars in lost revenue.[9] The British Internet service provider Cloudnine is believed to be the first business “hacked out of existence” in a denial-of-service attack in January 2002. This attack was similar to denial-of-service attacks launched by Mafiaboy in February 2000.[10]

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

One of the most common methods of virus transmission is via e-mail attachment files. Most organizations block e-mail attachments of certain types and also filter all e-mail for known viruses. In earlier times, viruses were slow-moving creatures that transferred viral payloads through the cumbersome movement of diskettes from system to system. Now, computers are networked, and e-mail programs prove to be fertile ground for computer viruses unless suitable controls are in place. The current software marketplace has several established vendors, such as Symantec Norton Anti-Virus and McAfee VirusScan, that provide applications to assist in the control of computer viruses.

Among the most common types of information system viruses are the **macro virus**, which is embedded in automatically executing macro code used by word processors, spread sheets, and database applications, and the **boot virus**, which infects the key operating system files located in a computer's boot sector.

Worms Named for the Tapeworm in John Brunner's novel *The Shockwave Rider*, a **worm** is a malicious program that replicates itself constantly, without requiring another program environment. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth. Read the Offline on Robert Morris and the worm he created to learn about the damage a worm can cause. Code Red, Sircam, Nimda ("admin" spelled backwards), and Klez are examples of a class of worms that combines multiple modes of attack into a single package. Figure 2-2 shows sample e-mails containing the Nimda and Sircam worms. These newer worm variants contain multiple exploits that can use any of the many predefined distribution vectors to programmatically distribute the worm (see the section on polymorphism later in this chapter for more details). The Klez virus, shown in Figure 2-3, delivers a double-barreled payload: it has an attachment that contains the worm, and if the e-mail is viewed on an HTML-enabled


Nimda—note garbage in the subject

Sircam—note stilted text

Norton AntiVirus Notification

Scan type: Realtime Protection Scan
Event: Virus Found!
Virus name: W32.Nimda.A@mm (dr)
File: C:\Documents and Settings\mwhitman\Local Settings\Temp\readme
Location: Quarantine
Computer: WIZARD
User: mwhitman
Action taken: Clean failed : Quarantine succeeded : Access denied

Total Notifications: 6 Currently displayed: 1

To: <mwhitman@kennesaw.edu>

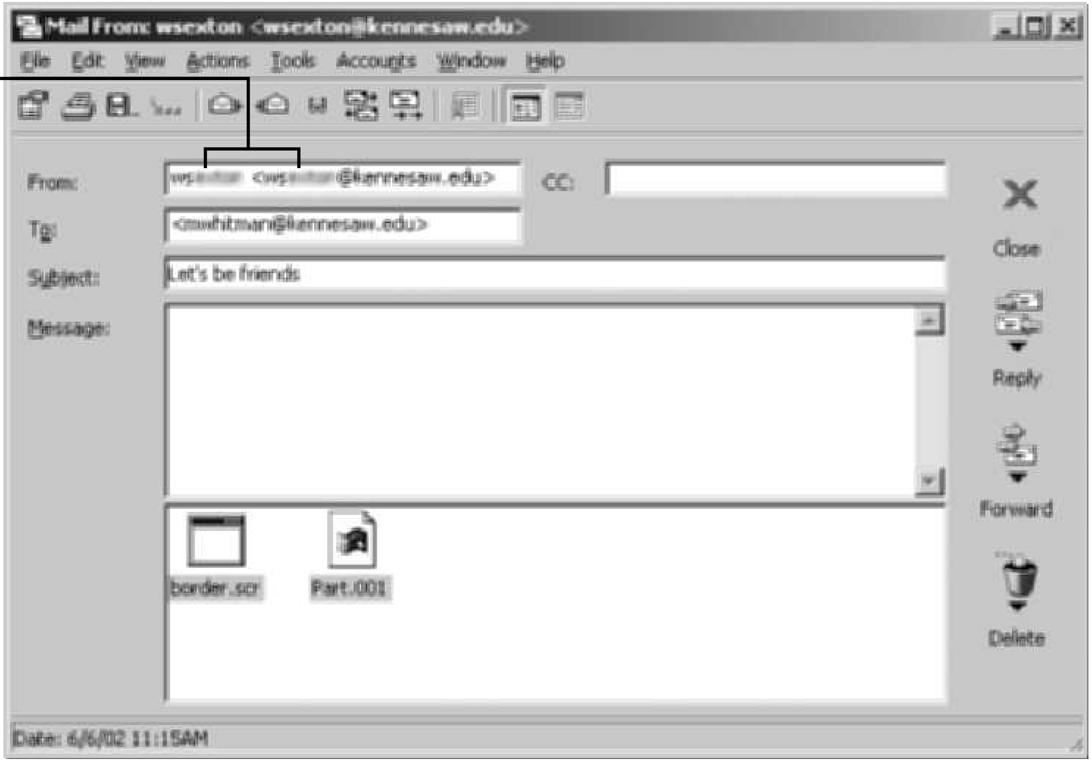
Message: Hi! How are you?

I send you this file in order to have your advice

See you later. Thanks

Figure 2-2 Nimda and Sircam Viruses

Source: Course Technology/Cengage Learning



Note the matching e-mail alias and e-mail address

Mail From: wsexton <wsexton@kennesaw.edu>
File Edit View Actions Tools Accounts Window Help
Close
Reply
Forward
Delete

From: ws[redacted] <ws[redacted]@kennesaw.edu>

CC:

To: <mwhitman@kennesaw.edu>

Subject: Let's be friends

Message:

border.scr

Part.001

Date: 6/6/02 11:15AM

Figure 2-3 Klez Virus

Source: Course Technology/Cengage Learning

browser, it attempts to deliver a macro virus. News-making attacks, such as MS-Blaster, MyDoom, and Netsky, are variants of the multifaceted attack worms and viruses that exploit weaknesses in the leading operating systems and applications.

The complex behavior of worms can be initiated with or without the user downloading or executing the file. Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. Furthermore, a worm can deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected. Worms also take advantage of open shares found on the network in which an infected system is located, placing working copies of the worm code onto the server so that users of those shares are likely to become infected.

Trojan Horses **Trojan horses** are software programs that hide their true nature and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages. Unfortunately, like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user. Figure 2-4 outlines a typical Trojan horse attack. Around January 20, 1999, Internet e-mail users began receiving e-mail with an attachment of a Trojan horse program named Happy99.exe. When the e-mail attachment was opened, a brief multimedia program displayed fireworks and the message "Happy 1999." While the fireworks display was running, the Trojan horse program was installing itself into the user's system. The program continued to propagate itself by following up every e-mail the user sent with a second e-mail to the same recipient that contained the Happy99 Trojan horse program.

Offline
Robert Morris and the Internet Worm[11]

In November of 1988, Robert Morris, Jr. made history. He was a postgraduate student in at Cornell, who had invented a self-propagating program called a worm. He released it onto the Internet, choosing to send it from MIT to conceal the fact that the worm was designed and created at Cornell. Morris soon discovered that the program was reproducing itself and then infecting other machines at a speed much faster than he had envisaged. There was a bug.

Finally, many of machines across the U.S. and the world stopped working or became unresponsive. When Morris realized what was occurring he reached out for help. Contacting a friend at Harvard, they sent a message to system administrators at Harvard letting them know what was going on and giving guidance on how to disable the worm. But, since the networks involved were jammed from the worm infection, the message was delayed to the point it had no effect. It was too little too late. Morris' worm had infected many computers including academic institutions, military sites, and commercial concerns. The cost estimate for the infection and the aftermath was estimated at roughly $200 per site.

The worm that Morris created took advantage of flaws in the sendmail program. It was a widely known fault that allowed debug features to be exploited, but few organizations had taken the trouble to update or patch the flaw. Staff at The University of California at Berkeley and MIT had copies of the program and reverse-engineered them determine how it functioned. The teams of programmers worked nonstop and, after about twelve hours, devised a method to slow down the infection. Another method was also discovered at Purdue and widely published. Ironically, the response was hampered by the clogged state of the email infrastructure caused by the worm. After a few days, things slowly started to regain normalcy and everyone wondered where this worm had originated. Morris was identified in a article in the New York Times as the author, even though it was not confirmed at that time.

Morris was convicted under the Computer Fraud and Abuse Act and was sentenced to a fine, probation, community service, and court costs. His appeal was rejected in March of 1991.

Back Door or Trap Door A virus or worm can have a payload that installs a **back door** or **trap door** component in a system, which allows the attacker to access the system at will with special privileges. Examples of these kinds of payloads include Subseven and Back Orifice.

Polymorphic Threats One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A **polymorphic threat** is one that over time

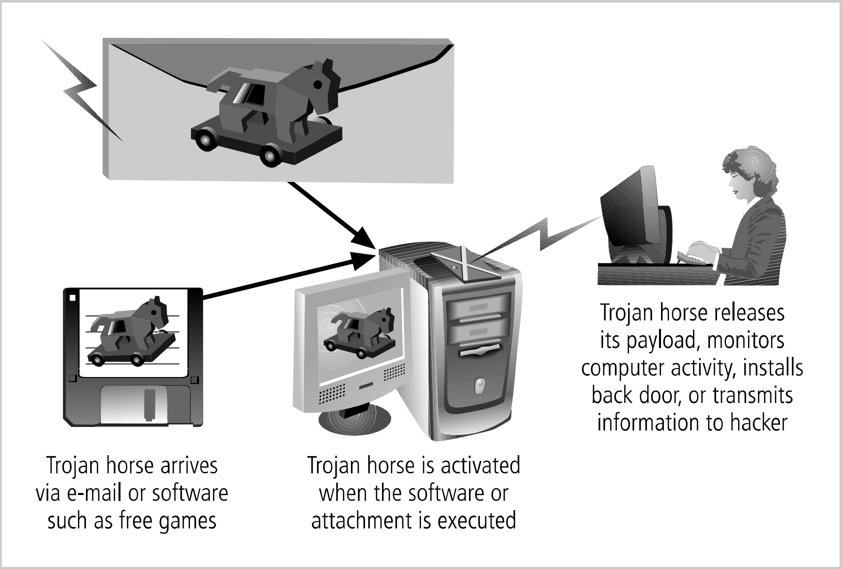


Figure 2-4 Trojan Horse Attack

Source: Course Technology/Cengage Learning

changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

Virus and Worm Hoaxes As frustrating as viruses and worms are, perhaps more time and money is spent on resolving **virus hoaxes**. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist. When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software.

A number of Internet resources enable individuals to research viruses to determine if they are fact or fiction. For the latest information on real, threatening viruses and hoaxes, along with other relevant and current security information, visit the CERT Coordination Center at *www.cert.org*. For a more entertaining approach to the latest virus, worm, and hoax information, visit the Hoax-Slayer Web site at *www.hoax-slayer.com*.

Deviations in Quality of Service

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

Internet Service Issues In organizations that rely heavily on the Internet and the World Wide Web to support continued operations, Internet service provider failures can considerably undermine the availability of information. Many organizations have sales staff and telecommuters working at remote locations. When these offsite employees cannot contact the host systems, they must use manual procedures to continue operations.

When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services as well as for the hardware and operating system software used to operate the Web site. These Web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service Level Agreement (SLA)**. When a service provider fails to meet the SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications and Other Service Provider Issues Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services. The loss of these services can impair the ability of an organization to function. For instance, most facilities require water service to operate an air-conditioning system. Even in Minnesota in February, air-conditioning systems help keep a modern facility operating. If a wastewater system fails, an organization might be prevented from allowing employees into the building.

Power Irregularities Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses. This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment. In the United States, we are supplied 120-volt, 60-cycle power usually through 15 and 20 amp circuits. When voltage levels **spike** (experience a momentary increase), or **surge** (experience a prolonged increase), the extra voltage can severely damage or destroy equipment. Equally disruptive are power shortages from a lack of available power. A momentary low voltage or **sag**, or a more prolonged drop in voltage, known as a **brownout**, can cause systems to shut down or reset, or otherwise disrupt availability. Complete loss of power for a moment is known as a **fault**, and a more lengthy loss as a **blackout**. Because sensitive electronic equipment—especially networking equipment, computers, and computer-based systems—are vulnerable to fluctuations, controls should be applied to manage power quality. With small computers and network systems, quality power-conditioning options such as surge suppressors can smooth out spikes. The more expensive uninterruptible power supply (UPS) can protect against spikes and surges as well as against sags and even blackouts of limited duration.

Espionage or Trespass

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

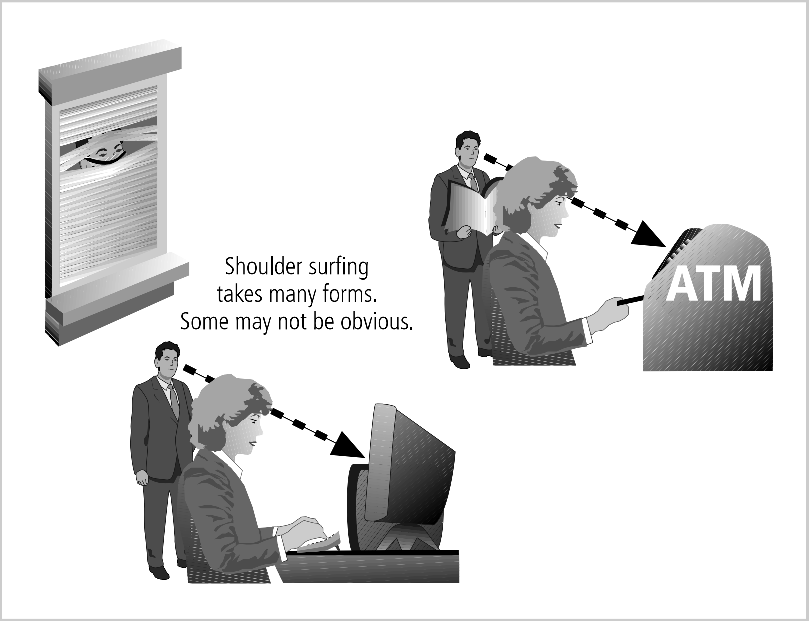


Figure 2-5 Shoulder Surfing

Source: Course Technology/Cengage Learning

American organizations. When foreign governments are involved, these activities are considered espionage and a threat to national security. Some forms of espionage are relatively low tech. One example, called **shoulder surfing**, is pictured in Figure 2-5. This technique is used in public or semipublic settings when individuals gather information they are not authorized to have by looking over another individual's shoulder or viewing the information from a distance. Instances of shoulder surfing occur at computer terminals, desks, ATM machines, on the bus or subway where people use smartphones and tablet PCs, or other places where a person is accessing confidential information. There is unwritten etiquette among professionals who address information security in the workplace. When someone can see another person entering personal or private information into a system, the first person should look away as the information is entered. Failure to do so constitutes not only a breach of etiquette, but an affront to privacy as well as a threat to the security of confidential information.

Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter. Controls sometimes mark the boundaries of an organization's virtual territory. These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace. Sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access.

The classic perpetrator of espionage or trespass is the hacker. **Hackers** are "people who use and create computer software [to] gain access to information illegally."[12] Hackers are frequently glamorized in fictional accounts as people who stealthily manipulate a maze of computer networks, systems, and data to find the information that solves the mystery or saves the day. Television and motion pictures are inundated with images of hackers as heroes or heroines. However, the true life of the hacker is far more mundane (see Figure 2-6). In the

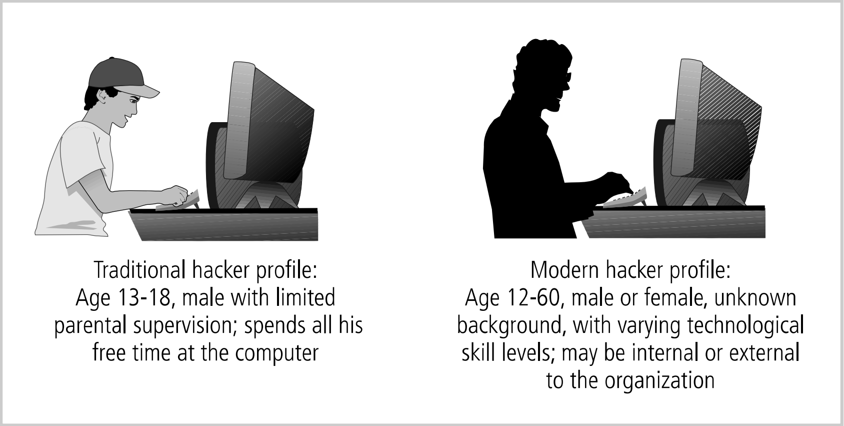

Traditional hacker profile:
Age 13-18, male with limited parental supervision; spends all his free time at the computer
Modern hacker profile:
Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

Figure 2-6 Hacker Profiles

Source: Course Technology/Cengage Learning

real world, a hacker frequently spends long hours examining the types and structures of the targeted systems and uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else.

There are generally two skill levels among hackers. The first is the **expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in the second category, the novice or **unskilled hacker**. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system. As described in the Offline section, Hack PCWeek expert hackers are extremely talented individuals who usually devote lots of time and energy to attempting to break into other people's information systems.

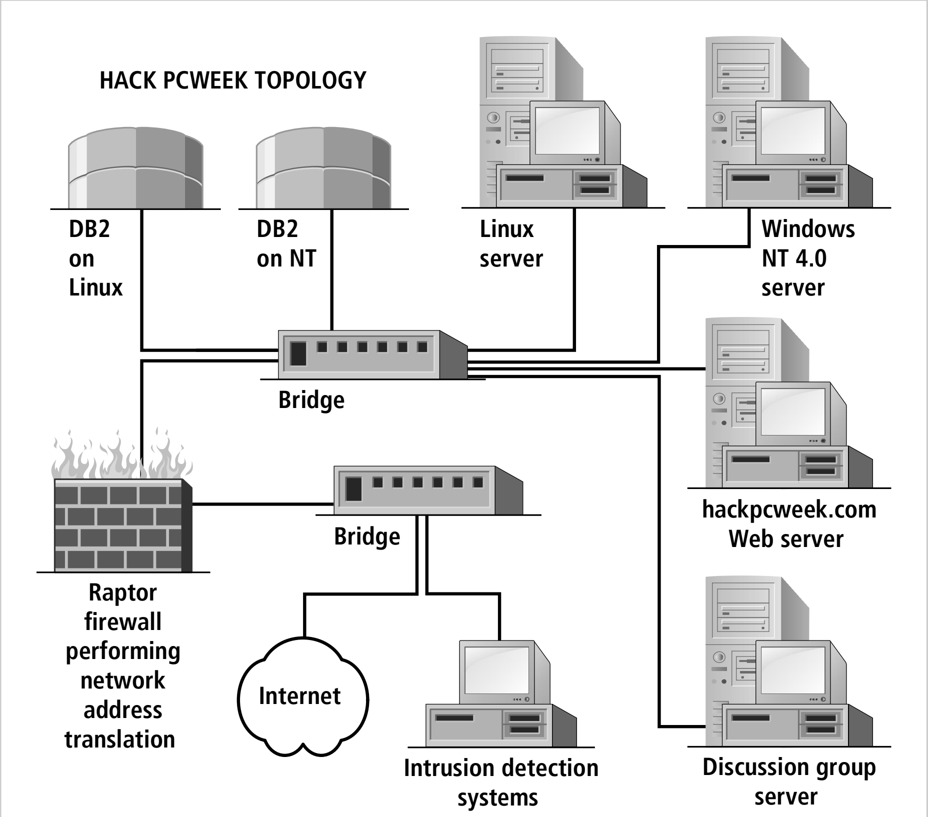
Once an expert hacker chooses a target system, the likelihood that he or she will successfully enter the system is high. Fortunately for the many poorly protected organizations in the world, there are substantially fewer expert hackers than novice hackers.

Expert hackers, dissatisfied with attacking systems directly, have turned their attention to writing software. These programs are automated exploits that allow novice hackers to act as **script kiddies**—hackers of limited skill who use expertly written software to attack a system—or **packet monkeys**—script kiddies who use automated exploits to engage in distributed denial-of-service attacks (described later in this chapter). The good news is that if an expert hacker can post a script tool where a script kiddie or packet monkey can find it, then systems and security administrators can find it, too. The developers of protection software and hardware and the service providers who keep defensive systems up to date also keep themselves informed of the latest in exploit scripts. As a result of preparation and continued vigilance, attacks conducted by scripts are usually predictable and can be adequately defended against.

In February 2000, a juvenile hacker named Mafiaboy, who was responsible for a series of widely publicized denial-of-service attacks on prominent Web sites, pled guilty to 56 counts of computer mischief and was sentenced to eight months in juvenile detention, and to pay $250 to charity.[13] His downfall came from his inability to delete the system logs that tracked his activity, and his need to brag about his exploits in chat rooms.

Offline
Hack PCWeek

On September 20, 1999, PCWeek did the unthinkable: It set up two computers, one Linux-based, one Windows NT-based, and challenged members of the hacking community to be the first to crack either system, deface the posted Web page, and claim a $1000 reward. Four days later the Linux-based computer was hacked. Figure 2-7 shows the configuration of the *www.hackpcweek.com* Web site, which is no longer functional. The article below provides the technical details of how the hack was accomplished not by a compromise of the root operating system, but by the exploitation of an add-on CGI script with improper security checks.



The topology of the honeynet used for this exercise was designed to be similar to that which an administrator might put into a real production site. It was built without esoteric defenses, sticking to standard firewall and network approaches.

Figure 2-7 Hack PCWeek Configuration

Source: Course Technology/Cengage Learning

In just under 20 hours, the hacker, known as JFS and hailing from Gibraltar (a.k.a the Rock), used his advanced knowledge of the Common Gateway Interface protocol (CGI) to gain control over the target server. He began as most attackers do, with a standard port scan, finding only the HTTP port 80 open. A more detailed analysis of the web servers revealed no additional information.

"Port scanning reveals TCP-based servers, such as telnet, FTP, DNS, and Apache, any of which are potential access points for an attacker. Further testing revealed that most of the potentially interesting services refused connections, with Jfs speculating that TCP wrappers was used to provide access control. The Web server port, 80/TCP, had to be open for Web access to succeed. JFS next used a simple trick. If you send GET X HTTP/1.0 to a Web server, it will send back an error message (unless there is a file named X) along with the standard Web server header. The header contains interesting facts, such as the type and version or the Web server, and sometimes the host operating system and architecture… As the header information is part of the Web server standard, you can get this from just about any Web server, including IIS."

Web Citation (from Cached page: http://cc.bingj.com/cache.aspx?q=JFS+hack+PC+week&d=4567500289476568&mkt=en-US&setlang=en-US&w=a53e4143,65aaf858; accessed November 6, 2010)

He then methodically mapped out the target, starting with the directory server, using the publicly offered WWW pages. He identified commercial applications and scripts. Since he had learned nothing useful with the networking protocol analyses, he focused on vulnerabilities in the dominant commercial application served on the system, PhotoAds. He was able to access the source code as it was offered with the product's sale. With this knowledge JFS was able to find, identify and look at the environment configuration script, but little else.

Not stopping, JFS started his effort to exploit known server-side vulnerabilities such as the use of script includes and mod_PERL embedded commands. When that did not pan out with his first attempt, he kept on, trying this process out with every field to find that a PERL regexp was in place to filter out most input before it was processed. JFS was able to locate just one user-assigned variable that wasn't being screened properly for malformed content. This single flaw encouraged him to keep up his effort.

JFS had located an ENV variable in the HTTP REFERER that was left unprotected. He first tried to use it with a server-side include or mod_PERL embedded command to launch some code of his choosing. Too bad for him that these services were not configured on the machine.

JFS continued to poke and prod though the system configuration, looking specifically for vulnerabilities in the PhotoAds CGI scripts. As he turned his attention he began looking at open() and system() calls. Dead end.

JFS tried post commands, but it stripped out one of the necessary components of the hack string, the % sign making the code fail to function. He then tried uploading files, but the file name variable was again being filtered by a regexp, and they were

(*continued*)

just placed into a different directory and renamed anyway. He tried and eventually gave up getting around the rename function.

After extensive work to create a C-based executable and smuggle it into the server, constantly battling to minimize the file size to the 8, 190 byte size restriction imposed on the get command, JFS hit another dead end, and turned his attention to gaining root access.

"Using the bugtraq service, he found a cron exploit for which patches hadn't been applied. He modified the hack to get a suidroot. This got him root access—and the ability to change the home page to the chilling: "This site has been hacked. JFS was here".[14]

Game over.

There are other terms for system rule breakers that may be less familiar. The term **cracker** is now commonly associated with an individual who *cracks* or removes software protection that is designed to prevent unauthorized duplication. With the removal of the copyright protection, the software can be easily distributed and installed. The terms hacker and cracker in current usage denote criminal intent.

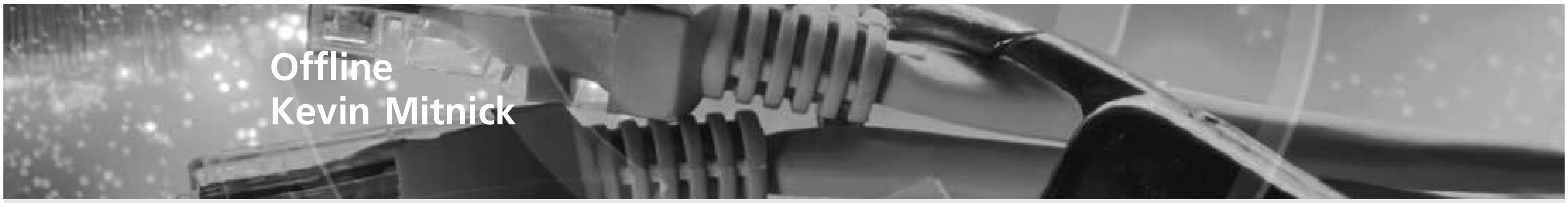
A **phreaker** hacks the public telephone network to make free calls or disrupt services. Phreakers grew in fame in the 1970s when they developed devices called blue boxes that enabled free calls from pay phones. Later, red boxes were developed to simulate the tones of coins falling in a pay phone, and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

The most notorious hacker in recent history is Kevin Mitnick, whose history is highlighted in the previous Offline.

Forces of Nature

Forces of nature, *force majeure*, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information. Some of the more common threats in this group are listed here.

- **Fire**: In this context, usually a structural fire that damages a building housing computing equipment that comprises all or part of an information system, as well as smoke damage and/or water damage from sprinkler systems or firefighters. This threat can usually be mitigated with fire casualty insurance and/or business interruption insurance.
- **Flood**: An overflowing of water onto an area that is normally dry, causing direct damage to all or part of the information system or to the building that houses all or part of the information system. A flood might also disrupt operations through interruptions in



Offline
Kevin Mitnick

Among the most notorious hackers to date is Kevin Mitnick. The son of divorced parents, Kevin Mitnick grew up in an unremarkable middle-class environment. Kevin got his start as a phreaker with a local group of juvenile enthusiasts. Eventually this group expanded their malicious activities and began to target computer companies. After attacking and physically breaking into the Pacific Bell Computer Center for Mainframe Operations, the group was arrested when a former girlfriend of one of the members turned them in. A 17-year-old, Mitnick was convicted of the destruction of data and theft of equipment, and sentenced to three months in juvenile detention and a year's probation.

Mitnick spent the next few years sharpening his hacking and phreaking skills and surviving run-ins with the police. He was arrested again in 1983 at the University of Southern California, where he was caught breaking into Pentagon computers over ARPANET. He received six months in another juvenile prison. He disappeared a few years later, after a warrant was issued for his arrest for breaking into a credit agency computer database. In 1987, he was eventually convicted of using illegal telephone cards and sentenced to 36 months probation. His next hacking battle pitched him against the FBI. His knowledge of the telephone system frustrated their efforts to apprehend him until his best friend turned him in. His unusual defense of computer addiction resulted in a one-year prison sentence and six months counseling. By 1992, it seemed that Mitnick had reverted to a relatively normal life until an episode of illegal database use was traced back to him. After an FBI search of his residence, he was charged with illegally accessing a phone company's computer and associating with a former criminal associate. But this time Kevin Mitnick disappeared before his trial.[15]

In 1995, he was finally tracked down and arrested. Because he was a known flight risk, he was held without bail for nearly five years, eight months of it in solitary confinement. Afraid he would never get to trial, he eventually pleaded guilty to wire fraud, computer fraud, and intercepting communications. He is now free on probation and was required, until January 2003, to get permission to travel or use any technology. His newest job is on the lecture circuit, where he speaks out in support of information security and against hacking.[16]

access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with flood insurance and/or business interruption insurance.

- **Earthquake**: A sudden movement of the earth's crust caused by the release of stress accumulated along geologic faults or by volcanic activity. Earthquakes can cause direct damage to all or part of the information system or, more often, to the building that houses it, and can also disrupt operations through interruptions in access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with specific casualty insurance and/or business interruption insurance, but is usually a separate policy.

- **Lightning**: An abrupt, discontinuous natural electric discharge in the atmosphere. Lightning usually directly damages all or part of the information system an/or its power distribution components. It can also cause fires or other damage to the building that houses all or part of the information system, and disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can usually be mitigated with multipurpose casualty insurance and/or business interruption insurance.
- **Landslide or mudslide**: The downward sliding of a mass of earth and rock directly damaging all or part of the information system or, more likely, the building that houses it. Land- or mudslides also disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.
- **Tornado or severe windstorm**: A rotating column of air ranging in width from a few yards to more than a mile and whirling at destructively high speeds, usually accompanied by a funnel-shaped downward extension of a cumulonimbus cloud. Storms can directly damage all or part of the information system or, more likely, the building that houses it, and can also interrupt access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.
- **Hurricane or typhoon**: A severe tropical cyclone originating in the equatorial regions of the Atlantic Ocean or Caribbean Sea or eastern regions of the Pacific Ocean (typhoon), traveling north, northwest, or northeast from its point of origin, and usually involving heavy rains. These storms can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding (see above). These storms may also disrupt operations by interrupting access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.
- **Tsunami**: A very large ocean wave caused by an underwater earthquake or volcanic eruption. These events can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. Tsunamis may also cause disruption to operations through interruptions in access or electrical power to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.
- **Electrostatic discharge (ESD)**: Usually, static electricity and ESD are little more than a nuisance. Unfortunately, however, the mild static shock we receive when walking across a carpet can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. The cost of ESD-damaged electronic devices and interruptions to service can range from only a few cents to several millions of dollars for critical systems. Loss of production time in information processing due

to ESD impact is significant. While not usually viewed as a threat, ESD can disrupt information systems, but it is not usually an insurable loss unless covered by business interruption insurance.

- **Dust contamination**: Some environments are not friendly to the hardware components of information systems. Because dust contamination can shorten the life of information systems or cause unplanned downtime, this threat can disrupt normal operations.

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage, and they must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans.

Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Regardless of the cause, even innocuous mistakes can produce extensive damage. For example, a simple keyboarding error can cause worldwide Internet outages:

> *In April 1997, the core of the Internet suffered a disaster. Internet service providers lost connectivity with other ISPs due to an error in a routine Internet router-table update process. The resulting outage effectively shut down a major portion of the Internet for at least twenty minutes. It has been estimated that about 45 percent of Internet users were affected. In July 1997, the Internet went through yet another more critical global shutdown for millions of users. An accidental upload of a corrupt database to the Internet's root domain servers occurred. Since this provides the ability to address hosts on the net by name (i.e., eds.com), it was impossible to send e-mail or access Web sites within the .com and .net domains for several hours. The .com domain comprises a majority of the commercial enterprise users of the Internet.*[17]

One of the greatest threats to an organization's information security is the organization's own employees. Employees are the threat agents closest to the organizational data. Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data—even, as Figure 2-8 suggests, relative to threats from outsiders. This is because employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information. Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat to the protection of the information as is the individual who seeks to exploit the information, because one person's carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party. An example of the latter is the performance of key recovery actions in PKI systems. Many military applications have robust, dual-approval controls built in.

Figure 2-8 Acts of Human Error or Failure

Source: Course Technology/Cengage Learning

Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

Information Extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft. For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information. The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers. When the company refused to pay the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community. His Web site became so popular he had to restrict access.[18]

Another incident of extortion occurred in 2008 when pharmacy benefits manager Express Scripts, Inc. fell victim to a hacker who demonstrated that he had access to seventy-five customer records and claimed to have access to millions. The perpetrator demanded an undisclosed amount of money. The company notified the FBI and offered a $1 million reward for the arrest of the perpetrator. Express Scripts notified the affected customers, as required by various state information breach notification laws. Express Scripts was obliged to pay undisclosed expenses for the notifications, as well as for credit monitoring services that the company was required by some state laws to buy for its customers.[19]

Missing, Inadequate, or Incomplete Organizational Policy or Planning

Missing, inadequate, or incomplete organizational policy or planning makes an organization vulnerable to loss, damage, or disclosure of information assets when other threats lead to attacks. Information security is, at its core, a management function. The organization's executive leadership is responsible for strategic planning for security as well as for IT and business functions—a task known as governance.

Missing, Inadequate, or Incomplete Controls

Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks.

For example, if a small organization installs its first network using small office/home office (SOHO) equipment (which is similar to the equipment you might have on your home network) and fails to upgrade its network equipment as it becomes larger, the increased traffic can affect performance and cause information loss. Routine security audits to assess the current levels of protection help to ensure the continuous protection of organization's assets.

Sabotage or Vandalism

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

Although not necessarily financially devastating, attacks on the image of an organization are serious. Vandalism to a Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation. For example, in the early hours of July 13, 2001, a group known as Fluffi Bunni left its mark on the front page of the SysAdmin, Audit, Network, Security (SANS) Institute, a cooperative research and education organization. This event was particularly embarrassing to SANS Institute management, since the Institute provides security instruction and certification. The defacement read, "Would you really trust these guys to teach you security?"[20]

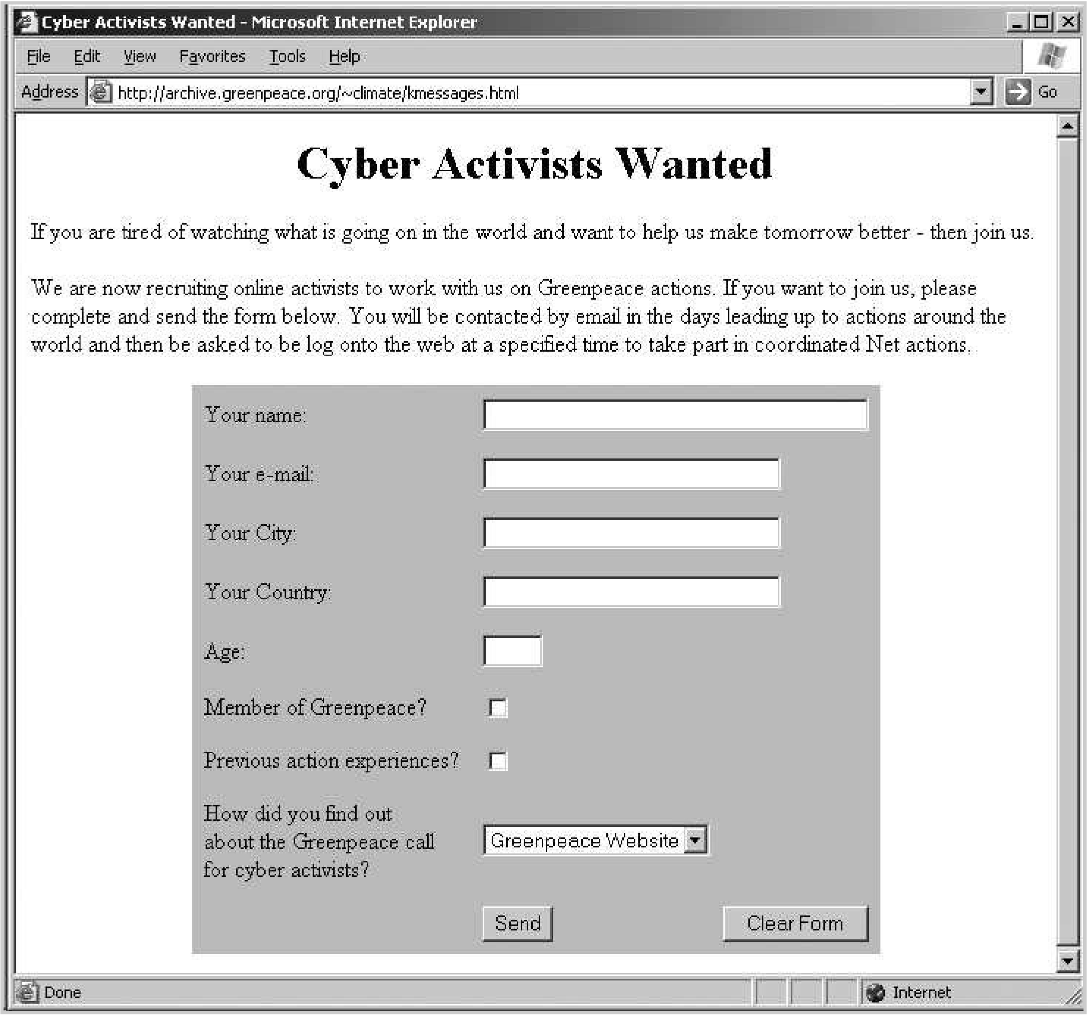
There are innumerable reports of hackers accessing systems and damaging or destroying critical data. Hacked Web sites once made front-page news, as the perpetrators intended. The impact of these acts has lessened as the volume has increased. The Web site that acts as the clearinghouse for many hacking reports, *Attrition.org*, has stopped cataloging all Web site defacements, because the frequency of such acts has outstripped the ability of the volunteers to keep the site up to date.[21]

Compared to Web site defacement, vandalism within a network is more malicious in intent and less public. Today, security experts are noticing a rise in another form of online vandalism, **hacktivist** or **cyberactivist** operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency. For example, in November 2009, a group calling itself "anti-fascist hackers" defaced the Web site of holocaust denier and Nazi sympathizer David Irving. They also released his private e-mail correspondence, secret locations of events on his speaking tour, and detailed information about people attending those events, among them members of various white supremacist organizations. This information was posted on the Web site WikiLeaks, an organization that publishes sensitive and classified information provided by anonymous sources.[22]

Figure 2-9 illustrates how Greenpeace, a well-known environmental activist organization, once used its Web presence to recruit cyberactivists.

A much more sinister form of hacking is **cyberterrorism**. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways. The United States and other governments are developing security measures intended to protect the critical computing and communications networks as well as the physical and power utility infrastructures.

> *In the 1980s, Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term "cyberterrorism" to refer to the convergence of cyberspace and terrorism. Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents."*[23]


Cyber Activists Wanted - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://archive.greenpeace.org/~climate/kmessages.html
Go
Done
Internet

Cyber Activists Wanted

If you are tired of watching what is going on in the world and want to help us make tomorrow better - then join us.

We are now recruiting online activists to work with us on Greenpeace actions. If you want to join us, please complete and send the form below. You will be contacted by email in the days leading up to actions around the world and then be asked to be log onto the web at a specified time to take part in coordinated Net actions.

Your name: ______

Your e-mail: ______

Your City: ______

Your Country: ______

Age: ______

Member of Greenpeace? □

Previous action experiences? □

How did you find out about the Greenpeace call for cyber activists? Greenpeace Website

Send Clear Form

Figure 2-9 Cyber Activists Wanted

Source: Course Technology/Cengage Learning