INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

Legal and Privacy Issues in Information Security

THIRD EDITION

Joanna Lyn Grama

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Legal and Privacy Issues in Information Security

THIRD EDITION

Joanna Lyn Grama

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Legal and Privacy Issues in Information Security, Third Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

Production Credits
Director of Product Management: Laura Pagluica
Product Manager: Edward Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Paula-Yuan Gregory
Manager, Project Management: Jessica deMartin
Project Specialist: Roberta Sherman
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: S4Carlisle Publishing Services
Project Management: S4Carlisle Publishing Services
Cover Design: Kristin E. Parker
Media Development Editor: Faith Brosnan
Rights Specialist: James Fortney
Cover Image: © mirjanajovic/DigitalVision Vectors/Getty Images
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data
Names: Grama, Joanna Lyn, author.
Title: Legal and privacy issues in information security / Joanna Lyn Grama.
Other titles: Legal issues in information security
Description: Third edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2022] | Includes bibliographical references and index.
Identifiers: LCCN 2020028528 | ISBN 9781284207804 (paperback)
Subjects: LCSH: Information storage and retrieval systems--Law and legislation--United States. | Data protection--Law and legislation--United States. | Information storage and retrieval systems--Security measures--Law and legislation--United States.
Classification: LCC KF1263.C65 G73 2022 | DDC 342.7308/58--dc23
LC record available at https://lccn.loc.gov/2020028528

6048

Printed in the United States of America

24 23 22 21 20 10 9 8 7 6 5 4 3 2 1

Contents

© mirjanajovic/DigitalVision Vectors/Getty Images

To my son, A.J., and my husband, Ananth

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curriculums in Information Technology (IT) Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

This book discusses information security, privacy, and the law. Information security is the practice of protecting information to ensure the goals of confidentiality, integrity, and availability. Information security makes sure that accurate information is available to authorized individuals when it is needed. Governments, private organizations, and individuals all use information security to protect information. Sometimes these organizations do a very good job of protecting information. Sometimes they do not.

When governments, private organizations, and individuals do a poor job of protecting the information entrusted to them, legislatures respond with new laws that require a more structured approach to information security. The U.S. federal government has enacted several laws that focus on protecting different types of information. This third edition takes into account the changing legal and regulatory landscape, and growth in privacy concerns, since this book was first published. Finding out which law applies to a particular situation, or type of data, or how best to think about privacy issues related to specific situations or data, is often confusing.

This book tries to help eliminate that confusion. Part One of the book discusses common concepts in information security, privacy, and the law. These concepts are used throughout the book. Part Two discusses the federal and state laws and legal concepts that affect how governments and organizations think about information security. This part uses laws and case studies to help explain these concepts. A quick-reference list of the federal laws and cases that are discussed in the book is included at the end of the book. Finally, Part Three focuses on how to create an information security program that addresses the laws and compliance requirements discussed throughout the book.

© mirjanajovic/DigitalVision Vectors/Getty Images

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and Sidebars to alert the reader to additional and helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a 2-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

New to This Edition

The text has been updated to address major legal developments since 2015 impacting the practice of information security and privacy, including revised case examples and references to illustrate concepts explained in the text. It has also updated endnotes and references for students who wish to learn more about concepts explained in the book.

Theory Labs

This text is accompanied by Cybersecurity Theory Labs. These hands-on labs provide guided exercises and case studies where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/grama3e.

Acknowledgments

The third time is the charm, as they say! Many talented people worked long hours to make the third edition of this book a reality, and they all have my sincere appreciation. I wish to thank Jones & Bartlett Learning for inviting me back to work on this edition. The competence of the Jones & Bartlett team makes revision work so much easier. Carole Jelen, my literary agent, continues to earn my gratitude for answering my endless questions with grace and good humor.

I am fortunate to have the support of friends and family members in all that I do. I would especially like to thank my friends and colleagues at Vantage Technology Consulting Group for encouraging me when the "writing times" were tough. In addition, the cheer, advice, subject matter review, and emergency cookie packages from friends Cathy Bates, Faith Graham, Pam Hermes, Amy Keene, Kim Lindros, Kim Milford, Matt Morton, Tim O'Brien, Patricia Rosen, David Seidl, Valerie Vogel, and Jon Young were invaluable. You all are the best and I am grateful for your friendship.

Finally, my husband, Ananth, and son, A.J., deserve special thanks for their tireless support. I am a very lucky person. My love, always, to you both.

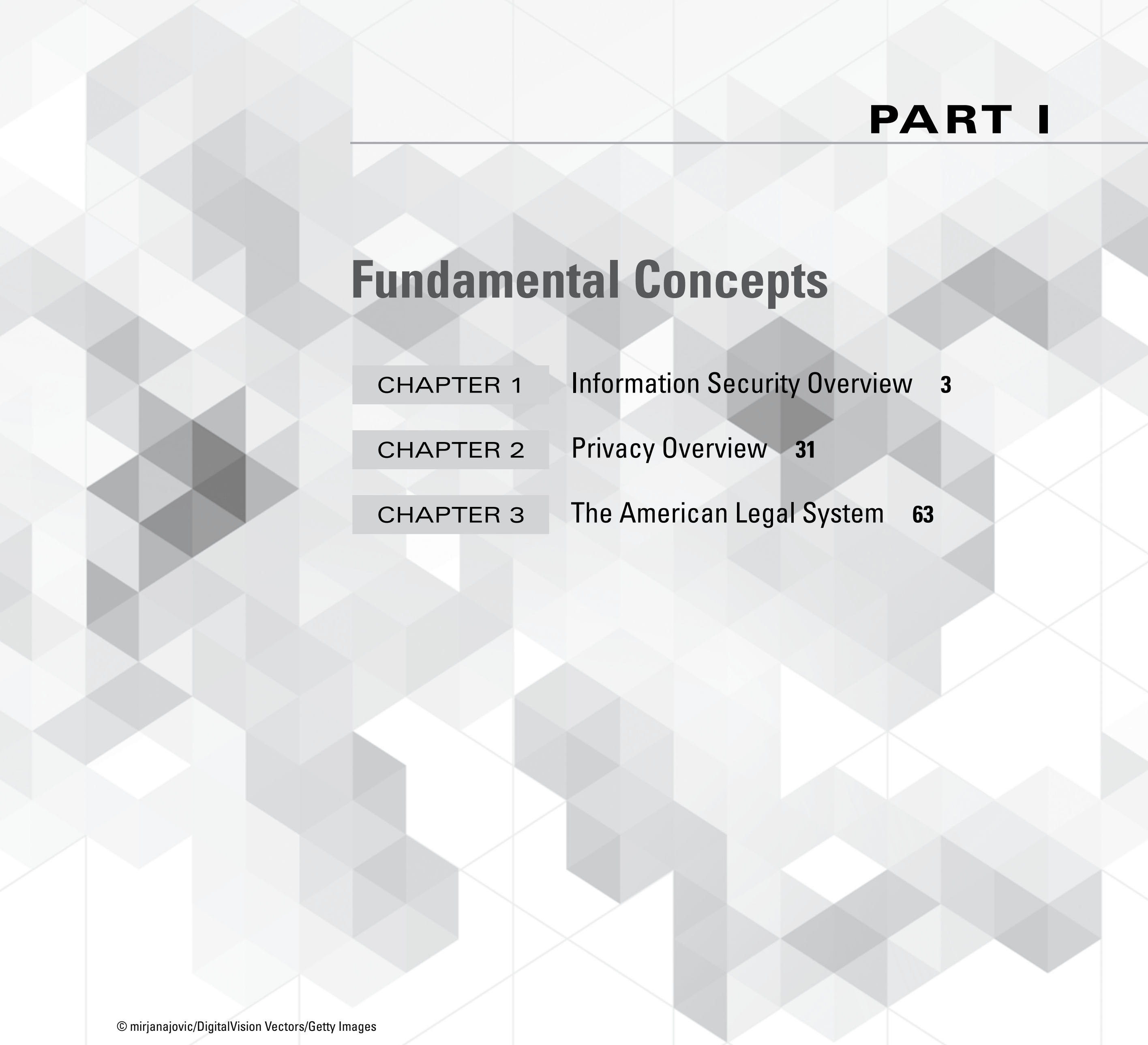
© mirjanajovic/DigitalVision Vectors/Getty Images

About the Author

Joanna Lyn Grama (JD, CISSP, CIPT, CRISC) is an associate vice president at Vantage Technology Consulting Group. She has more than 20 years of experience in higher education with a strong focus on law, IT security policy, compliance, governance, and data privacy issues.

Grama is a former member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee (appointed to the Committee by Secretary Janet Napolitano) and served as the chairperson of its technology subcommittee. Grama is also vice president of the board of directors for the central Indiana Information Systems Audit and Control Association (ISACA) chapter; and a member of the International Association for Privacy Professionals (IAPP); the American Bar Association, Section of Science and Technology Law, Information Security Committee; and the Indiana State Bar Association. She is a frequent speaker on a variety of IT security topics, including identity theft, personal information security, and university security and privacy compliance issues.

© mirjanajovic/DigitalVision Vectors/Getty Images



PART I

Fundamental Concepts

© mirjanajovic/DigitalVision Vectors/Getty Images

CHAPTER 1

Information Security Overview

ENSURING THAT INFORMATION is secure is not solely the responsibility of technicians in computer data centers. It also concerns governments, corporations, and private individuals. The digital revolution greatly changed how people communicate and do business. Because information exchanges now take place instantly, and because almost everyone shares data of some kind, you should question how all organizations use and protect data.

This text is about information security and the law. Information security seeks to protect government, corporate, and individual information and is a good business practice. Many organizations today want a reputation for properly protecting their own and their customers' data, because a good reputation can make a company stand out from its competitors, increase sales, or make a government agency seem more trustworthy.

Laws also protect information, especially private personal information. They require that data be protected in certain ways. Laws are not optional; if a law applies to an organization, then the organization must follow the law. Laws make information security more than just a good business practice. They make it a business requirement.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- Why information security is an issue
- What information security is
- What the basic information security concepts are
- What common information security concerns are
- How different types of information require different types of protection
- Which mechanisms protect information security
- How special kinds of data require special kinds of protection

© mirjanajovic/DigitalVision Vectors/Getty Images

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Describe the key concepts and terms associated with information security
- Describe information security goals and give examples of each
- Describe common information security concerns
- Describe mechanisms used to protect information security

Why Is Information Security an Issue?

Every day the news media reports stories such as these:

- Someone attacks a university computer and gains access to the records of over 30,000 students and staff members. These records include names, photographs, and Social Security numbers (SSNs).
- A hospital experiences a cyberattack that prevents hospital staff from accessing computer systems and patient records. Therefore, the hospital must turn away patients until its computer systems and access are restored.
- A bank loses a backup tape, potentially exposing more than 1 million customer records. The tape is never found.
- A company that processes credit cards stores unencrypted account information on its servers. Attackers gain access to the servers, exposing over 40 million accounts.
- An email scam targets an organization by asking employees to verify their account settings. When employees respond, they provide their computer usernames and passwords. Attackers then use those credentials to access and compromise the organization's computer systems.

Organizations use and store a lot of data to conduct their business operations. For many, **information** is one of their most important assets. Organizations use large and complex databases to keep track of customer product preferences, as well as manage the products and services that they offer customers. They also transfer information to other businesses so that both companies can benefit.

Organizations collect data for many reasons. Much of the data they collect is *personal information*, which can be used to identify a person. Personally identifiable information includes the following:

- SSNs
- Driver's license numbers
- Financial account data, such as account numbers or personal identification numbers (PINs)

- Health data and biometric data
- Authentication credentials, such as logon or usernames and passwords

Based on media reports, security breaches appear to be growing both in number and in the severity of damage they cause to organizations. These breaches result in data that is lost, stolen, disclosed without permission, or rendered unusable. A security breach can damage an organization's reputation, which may prompt customers take their business elsewhere. Following a breach, the organization may also have to pay fines and/or defend itself in court. If a security breach is particularly bad, an organization's leaders can face criminal charges.

As noted, an organization that fails to protect its information risks damaging its reputation—or worse. *Information security* is the term that generally describes the types of steps an organization should take to protect its information.

What Is Information Security?

Information security is the study and practice of protecting information. Its main goal is to protect the **confidentiality**, **integrity**, and **availability** of information. Professionals usually refer to this as the *C-I-A triad*, or sometimes the *A-I-C triad*. (A *triad* is a group of three things considered to be a single unit.)

The C-I-A triad appears in **FIGURE 1-1**.

The need to protect information is not a new concept. For instance, Julius Caesar used a simple letter-substitution code to share secrets with his military commanders. Caesar used this type of code, called a *Caesar cipher*, to ensure that his enemies could not read his messages. **Cryptography** is the practice of hiding information so that unauthorized persons cannot

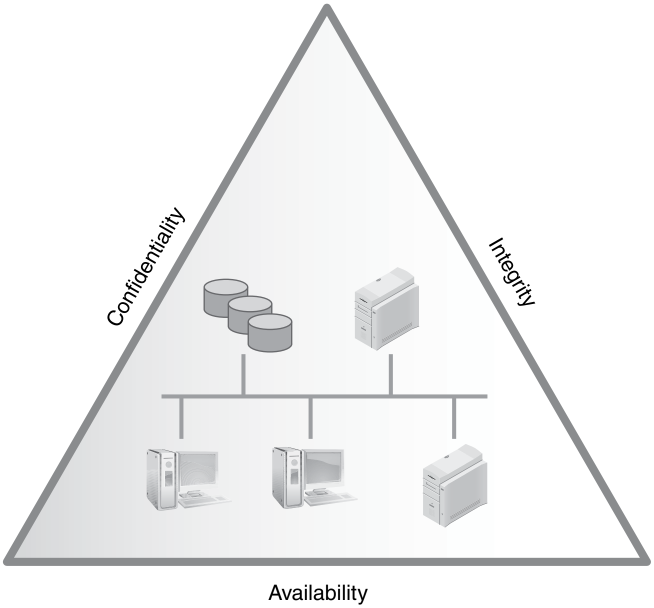


FIGURE 1-1
The C-I-A triad.

read it. Using cryptography preserves confidentiality, because only those with the secret key are able to read an encoded note.

Secret decoder badges were popular during the golden days of radio (about 1920–1950). Business sponsors often paid for decoders to market their products, and radio program fan clubs gave them to their members to promote specific radio shows. These secret decoder badges often used a Caesar cipher.

NOTE

You might think that information security refers only to data stored on a computer. However, it refers to information in both paper and electronic form.

In some ways, however, information security is a relatively new area of study. Modern computing systems have existed only since the 1960s, and the internet did not exist in its current form until almost 1983. The first well-known computer security incident was discovered in 1986, and President Obama created the first "cybersecurity czar" in the federal government in 2009.

The range of information security topics may seem overwhelming. However, it is important to keep in mind that the main goal of information security is to protect the confidentiality, integrity, and availability of data.

What Is Confidentiality?

Confidentiality means that only people with the right permission can access and use information. It also means protecting information from unauthorized access at all stages of its life cycle. You must create, use, store, transmit, and destroy information in ways that protect its confidentiality.

Encryption is one way to make sure that information remains confidential while it is stored and transmitted. The encryption process converts information into code that is unreadable. Only people authorized to view the information can decode and use it, thereby protecting the information's confidentiality. Attackers who intercept an encrypted message cannot read it because they do not have the key to decode it.

Access controls, another way to ensure confidentiality, grant or deny access to information systems. An example of an access control is requiring a password or PIN to access a computer system. Passwords keep unauthorized individuals out of information systems. You also can use access controls to ensure that individuals view only information they have permission to see.

NOTE

Cliff Stoll described the first well-known computer security incident in his book *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Stoll noticed an error in the records of systems connected to the internet's predecessor—the Advanced Research Projects Agency Network (ARPANET). During the investigation, he exposed an international plot to steal information from U.S. computer systems.

Individuals can compromise information confidentiality on purpose or by accident. For example, **shoulder surfing** is a type of intentional attack. It occurs when an attacker secretly looks "over the shoulder" of someone at a computer and tries to discover his or her sensitive information without permission. Shoulder surfing is a visual attack, because the attacker must view the personal information. This term also describes attacks in which a person tries to learn sensitive information by viewing keystrokes on a monitor or keyboard. Attackers use the stolen data to access computer systems and commit identity theft.

Social engineering is another type of attack that represents an intentional threat to confidentiality. These attacks rely heavily on human interaction. They take advantage of how people normally talk with one another and interact. It is not a technical attack, but rather involves tricking other people to break security rules and share sensitive information. Social engineering attackers take advantage of human nature, such as kindness, helpfulness, and trust. Because the attackers are so charming, their victims want to help them by providing information. The attacker then uses the information obtained from the victim to try to learn additional sensitive information. The attacker's ultimate goal is to obtain enough information to access computer systems or gain access to protected areas.

FYI

The classic film *The Sting* is a great example of a social engineering scam. In the movie, two con artists, played by Paul Newman and Robert Redford, set up an elaborate plan to con a man out of his money. Their scam, which takes advantage of human nature, relies heavily on manipulating the victim and those around him.

Kevin Mitnick is perhaps one of the best-known computer hackers of all time. In his book *The Art of Deception*, he writes that he gained much of the information he used to compromise computer systems through social engineering. Mitnick said that it was very easy to get information from people if he asked questions in the right way.

Confidentiality compromises also take place by accident. For example, an employee of the U.S. Transportation Security Administration (TSA) posted a redacted copy of a TSA manual on a federal website in December 2009. This manual described how TSA agents should screen airline passengers and luggage. It also contained the technical details of how airport screening machines work. The manual contained pictures of identification cards for average Americans, Central Intelligence Agency employees, and U.S. legislators.

The TSA posted the manual by mistake, and for several months the public had access to the manual online. Although TSA employees had redacted some portions of the manual, the TSA improperly performed technical aspects of the redaction. Therefore, some people were able to uncover the original information with common software tools. Those people then reposted the manual on several other nongovernmental websites. Some of these websites posted the document with all of the original text available.

The manual also highlighted the increase in airport security requirements after the September 11, 2001 terrorist attacks. Once posted, the unredacted material could have been used by attackers to exploit new airport security measures. The TSA argued that posting the manual did not compromise the safety of U.S. air travel. Nonetheless, lawmakers immediately questioned the TSA about the incident and asked how the TSA would mitigate the disclosure. Lawmakers wanted to know how the government could prevent other websites from reposting the unredacted manual. They also asked what the TSA would do to prevent similar mistakes in the future.

What Is Integrity?

Integrity means that information systems and their data are accurate. It ensures that changes cannot be made to data without appropriate permission. If a system has integrity, it means that the data in the system is moved and processed in predictable ways and does not change when it is processed.

Controls that ensure the correct entry of information protect the data's integrity. In a computer system, this means that if a field contains a number, the system checks the values that a user enters to make sure that the user actually entered numbers. Making sure that only authorized users have the ability to move or delete files on information systems also protects integrity. Antivirus software is another example of a control that protects integrity. This type of software checks to make sure that there are no viruses in the system that could harm it or change the data in it.

Information system integrity can be compromised in several ways, either accidentally or intentionally. For example, an employee may accidentally mistype a name or address during data entry. Integrity is compromised if the system does not prevent or check for this type of error. Another common type of accidental compromise of integrity is an employee deleting a file by mistake.

Integrity compromises also can take place intentionally. Employees or external attackers are potential threats. For example, suppose an employee deletes files that are critical to an organization's business. The employee might do this on purpose because of some grievance against the organization. Employees or others affiliated with an organization are sometimes called *insider threats* when they purposefully harm an organization's information systems. **External attackers** also are a concern. They can infect information systems with computer viruses or vandalize a webpage. External attackers who access systems without permission and deliberately change them harm confidentiality and integrity.

In 2007, three Florida A&M University students installed secret keystroke loggers on computers in the university registrar's office. A *keystroke logger* is a device or program that records keystrokes made on a keyboard or mouse, which the students used to obtain the usernames and passwords of registrar employees. For a fee, the hackers modified 650 grades in the computer system for other students, changing many failing scores to an "A." The student hackers also changed the residency status of other students from "out-of-state" to "in-state," which resulted in the out-of-state students paying less tuition.

The university discovered the keystroke loggers during a routine audit. It then found the modified data. Although the university fixed the incorrect data, the student hackers accessed the system and changed the data again. However, the university discovered the hackers' identities through additional security measures such as logging and audit review.

Prosecutors charged the student hackers with breaking federal laws. The court sentenced two of them to 22 months in prison each. In September 2009, it sentenced the third student hacker to 7 years in prison.

The Florida A&M case illustrates how safeguards can be implemented to protect the integrity of computer systems. Routine security audits can detect unauthorized or harmful software on a system.

What Is Availability?

Availability, the security goal of making sure information systems operate reliably, ensures that data is accessible when it needs to be. It also helps to ensure that individuals with proper permission can use systems and retrieve data in a dependable and timely manner.

Organizations need to have information available to conduct their business. When systems work properly, an organization can function as intended. Ensuring availability means that systems and information are available during peak hours when customer demand is high. System maintenance should be scheduled for off hours when customer demand is low.

Availability can be protected in several ways. Information systems must recover quickly from disturbances or failures. Organizations create plans that describe how to repair or recover systems after an incident. These plans specify how long systems may be offline before an organization starts to lose money or fails to meet its business goals. In the worst case, an organization might go out of business if it cannot repair its information systems quickly.

Organizations also can protect system availability by designing systems to have no single points of failure. A **single point of failure** is a piece of hardware or application that is key to the functioning of the entire system. If that single item fails, a critical portion of the system could fail. Single points of failure also can cause the whole system to fail.

An easy example of a single point of failure is a modem, which connects an organization to the internet. If the modem fails, the organization cannot connect to the internet. Thus, if the organization does most of its business online, the modem failure can really hurt its business.

Organizations also can protect availability by using redundant equipment that has extra functional elements designed into it. In the event of a failure, the extra elements make sure that the piece of equipment is still able to operate for a certain period. Backing up systems also ensures their availability.

Attackers target availability in order to harm an organization's business. As an example, a **denial of service (DoS) attack** disrupts information systems so they are no longer available to users. These attacks also can disable internet-based services by consuming large amounts of bandwidth or processing power, as well as disable an organization's website. These services are critical for businesses that sell web-based products and services or provide information via the internet.

Not all DoS attacks directly target information systems and their data. Attackers also target physical infrastructures. For example, an organization can experience a loss of availability if an attacker cuts a network or power cable. The result is the same as a technical DoS attack: Customers and other audiences cannot reach the needed services.

Unplanned outages can also negatively impact availability. An *outage* is an interruption of service. For example, natural disasters may create outages, such as a power outage after an earthquake. Outages also take place if a technician accidentally cuts a service cable.

A website experiencing an increase in use can result in a loss of availability. When Michael Jackson died in 2009, for example, the internet experienced a massive increase in search queries from people trying to find out what had happened to him. The rapid rise in search traffic caused Google to believe it was under a DoS attack. In response to this perceived attack, Google slowed down the processing of "Michael Jackson" queries. Users entering those queries received error messages until Google determined its services were not under attack.

NOTE

Domain Name Service (DNS) providers translate internet domain names into Internet Protocol (IP) addresses. In 2016 the Mirai malware was used to attack a major DNS provider named Dyn. The Dyn attack was one of the largest DoS attacks to date, affecting websites for large companies such as Netflix, Amazon, and the *New York Times*.

The Michael Jackson/Google example shows that organizations can take actions to make sure their information systems are available to their customers. These actions can alert organizations to an issue, prompting them to take steps to correct it.

Basic Information Security Concepts

Several different concepts are helpful in understanding information security and the laws that affect it. Laws that regulate information security often use risk management, the process of understanding the risks that an organization faces and then taking steps to address or mitigate them, to justify them. You will briefly learn about basic risk management concepts and terms here.

Vulnerabilities

A **vulnerability** is a weakness or flaw in an information system. They may be construction or design mistakes, as well as flaws in how an internal safeguard is used or not used. Not using antivirus software on a computer, for instance, is a vulnerability. Vulnerabilities can be *exploited* (used in an unjust way) to harm information security.

There are many different types of vulnerabilities. You can classify them into the following broad categories:

- People
- Process
- Facility
- Technology

People can cause several vulnerabilities. For example, one employee could know too much about a critical function in an organization. This is a violation of the **separation of duties** principle. This rule requires that two or more employees must split critical task functions so that no one employee knows all of the steps of the critical task. When only one employee knows all of the steps of a critical task, that employee can use the information to harm the organization. The harm may go unnoticed if other employees cannot access the same information or perform the same function.

NOTE

A common example of the separation of duties principle is a rule requiring two people to sign organization checks. This is so one person cannot steal from the organization by writing and signing checks made out to himself or herself. Requiring two signatures thus protects the organization.

Process-based vulnerabilities are flaws or weaknesses in an organization's procedures that an attacker can exploit to harm security. Process-based vulnerabilities include missing steps in a checklist, as well as not having a checklist in the first place. Another process vulnerability is the failure to apply hardware and software vendor patches in a timely manner. A **patch** is a piece of software or code that updates a program to address security or other operational problems. Patches are available for many types of software, including operating systems. Software and information systems may be open to attack if patches are not properly applied.

Facility-based vulnerabilities are weaknesses in physical security. Buildings, equipment, and other property are resources an organization must protect. An example of poor physical security is an organization that does not have a fence around its property. Another is an open server room that any employee can access.

Vulnerabilities also can be technology based. Improperly designed information systems fall into this category. Some design flaws allow people to access information systems without permission. After gaining entry, the person may enter unauthorized code or commands that disrupt the system. Unpatched and outdated applications are technology vulnerabilities. So are improperly configured equipment, such as firewalls or routers.

Customers do not like flaws in the products that they buy. Therefore, they expect vendors to inform them quickly about product flaws. *Vulnerability management* programs make sure that vendors find any flaws in their products and quickly correct them. They also ensure that customers are made aware of problems so they can take protective action. The Microsoft Corporation, for example, issues a monthly security bulletin for customers that lists known vulnerabilities in the company's products. The bulletin also explains how to address them. This bulletin is part of Microsoft's vulnerability management program.

Exploits are successful attacks against a vulnerability. They take place in a period known as the **window of vulnerability**, as shown in FIGURE 1-2. This window opens when someone discovers a vulnerability and closes when a vendor reduces or eliminates it. Exploits take place while the window is open.

The window of vulnerability is a notable concept. In some ways, this window is shrinking fast because more people are interested in information security. Many people have developed the skills to find new vulnerabilities. Often they report them to the company that provides the product or service so the company can fix the vulnerability. Not all people act with good intentions, however: There are also people with the skills needed to find and exploit vulnerabilities who do so for financial gain.

The number of vulnerabilities appears to be growing. The National Vulnerability Database (NVD) recorded almost 52 new vulnerabilities per day in December 2019.[1] One reason for this could be that information systems are becoming larger and more complex. Another possibility is that as more people work together to create new systems, the likelihood of introducing flaws increases. Poor programming practices may be another reason. Vulnerabilities also may be increasing because of a lack of quality controls to make sure that systems are secure and work as intended.

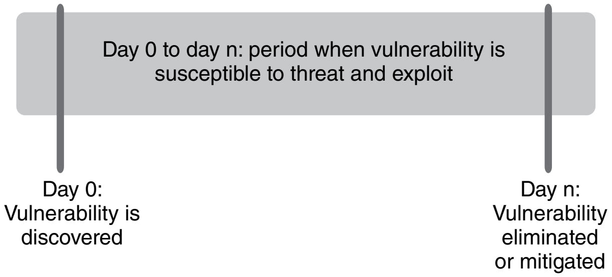

Day 0 to day n: period when vulnerability is susceptible to threat and exploit
Day 0: Vulnerability is discovered
Day n: Vulnerability eliminated or mitigated

FIGURE 1-2

The window of vulnerability.

The number of known vulnerabilities also may be increasing because some developers use well-known programming codes and components to design systems. They also use well-known software in the systems they design. Using familiar components makes it easier for many people to work together on the same project. There are dangers, however. The better known the code, hardware, or software, the greater the chance that an attacker also has the necessary skills to find vulnerabilities in the final product.

NOTE

Some vulnerabilities are exploited almost as soon as they are discovered. The term for this is a **zero-day vulnerability**. It is unique because the vulnerability is exploited before a vendor provides a patch or some other fix.

Threats

Threats are anything that can harm an information system. They are successful exploits against vulnerabilities. A threat source—which is a person or a circumstance—carries out a threat or causes it to take place.

It is worth taking some time to understand how vulnerabilities and threats are related. For example, an organization may have few controls to prevent an employee from deleting critical computer files. This lack of controls is the vulnerability. A well-meaning employee could delete files by mistake. In this case, the employee is the threat source. The threat is the action of deleting the critical files. If the employee deletes the files, a successful exploit of the vulnerability has taken place. If the files are not recoverable, or recoverable only at great expense, the incident harms the organization and its security. In this example, availability and integrity are compromised.

Threats fall into broad categories:

- **Human**—Threats carried out by people. Common examples are internal and external attackers. Even the loss of key personnel in some instances is a type of human threat. People threats include both good actors and bad actors. Good actors include well-meaning employees; bad actors are attackers who intend to harm an organization.
- **Natural**—Uncontrollable events such as earthquakes, tornadoes, fires, and floods. These types of threats are not predictable, and organizations cannot control these types of threats.
- **Technological and operational**—Threats that operate inside information systems to harm information security goals. Malicious code is an example of these threats. Hardware and software failures are technology threats. Improperly running processes are also threats.
- **Physical and environmental**—Facility-based threats. These types of threats can include a facility breach caused by lax physical security. Loss of heating or cooling within a facility is an example of an environmental threat.

Threats are either deliberate or accidental. *Accidental threats* are the results of either unintentional actions or inactions. You can think of accidental threats as mistakes or "acts of God." Unintended equipment failure also is an accidental threat.

Mistakes most often are the result of well-meaning employees. The file deletion example at the beginning of this section is an accidental threat. The TSA employee improperly posting the manual to a website, as mentioned earlier, is also an accidental threat. Organizational policy and security training and awareness can help mitigate such mistakes.

An act of God that disrupts services or compromises information security is an accidental threat. Earthquakes, tornadoes, floods, and wildfires caused by lightning or other natural events, are all examples of acts of God. It is hard for organizations to plan for these types of threats, although they can take basic precautions against some types of natural disasters by building redundant systems. An organization also may choose not to build facilities in areas prone to environmental instability.

All organizations must plan for equipment failure. Sometimes equipment breaks through no fault of its operators. Sometimes it reaches the end of its life and simply stops working. Unfortunately, it is hard for organizations to plan for such failures. This is especially true if the equipment that fails is particularly specialized or expensive. Organizations can mitigate this type of threat by building redundant systems and keeping spare parts on hand.

NOTE

The U.S. government maintains the NVD, a searchable database of known security flaws and weaknesses. It also includes listings of known system problems. The National Cyber Security Division of the U.S. Department of Homeland Security sponsors the NVD. You can find it at http://nvd.nist.gov/home.cfm.

Deliberate threats are intentional actions taken by attackers. Both internal and external attackers are deliberate threats. **Internal attackers** have current relationships with the organization that they are targeting. They can cause a lot of damage in computer systems because they have special knowledge about those systems. Internal attackers are often called malicious insider threats because they use their legitimate access to knowingly harm an organization. Upset employees are often the cause of internal attacks. They might wish to harm the organization by causing a loss of productivity. They also may wish to embarrass the organization or hurt its reputation. These attackers may purposefully delete files or disclose information without permission. They also may intentionally disrupt the availability of information systems.

Internal attackers also can take advantage of lax physical security. They might do this to steal resources such as confidential information. Theft of resources is a problem for many organizations.

In 2007, a former Coca-Cola employee was sentenced to 8 years in prison for stealing Coca-Cola trade secrets. She also was ordered to pay $40,000 in restitution.[2] This employee stole Coca-Cola secrets and tried to sell them to rival Pepsi. Surveillance video showed the employee putting company documents into bags and leaving the building. She did the same thing with a container of a Coca-Cola product sample. All of these actions were violations of Coca-Cola company policies. The theft was discovered when Pepsi informed Coca-Cola.

NOTE

Act of God is a legal term that describes a natural event or disaster for which no person is responsible.

External attackers are another concern. They usually have no current relationship with the organization they are targeting. Some are former employees with special knowledge about the organization. External hackers include spies, saboteurs, and terrorists. Many seek financial gain. Others want to embarrass an organization, make a political statement, or exploit systems for a challenge.

Organizations must take steps to avoid threats. When an employee leaves an organization, the organization should promptly remove his or her access to information systems and to physical

NOTE

It is not possible to identify every security vulnerability, to plan for every threat, or to identify all risks. Even when you identify risks, you cannot limit all risk of harm.

property. Good information security practices also help reduce threats posed by external attackers. These include patching known vulnerabilities in hardware and software. They also include monitoring access to systems and engaging in logging and audit review.

Risks

A **risk** is the likelihood that a threat will exploit a vulnerability and cause harm to the organization. These impacts from threats vary but can generally be sorted into six categories:

- **Financial**—Risks that affect financial resources or financial operations
- **System/Service**—Risks that impact how an organization provides information technology (IT) systems and services
- **Operational**—Risks that affect the normal operation of information systems and services
- **Reputational**—Risks that negatively affect an organization's reputation or brand
- **Compliance**—Risks that relate to a possible violation of a law, regulation, or organizational policy
- **Strategic**—Risks that may have a lasting impact on an organization's long-term viability

You can measure impact in terms of money costs or by perceived harm to the organization.

Not all risks receive or require the same level of attention from an organization. Organizations engage in complex risk analysis and risk management programs to classify and respond to risks. A brief overview of some risk analysis and management terms is included here.

Risk analysis is the process of reviewing known vulnerabilities and threats. Organizations generally classify the probability that a threat will exploit a vulnerability as low, medium, or high. They then attempt to assess the impact of a successful exploit. An organization should address risks that have large impacts on the organization and its information security.

All organizations must assess risk, as well as respond to it. Organizations have several options for responding to risk. Common responses include:

- Risk avoidance
- Risk mitigation
- Risk transfer
- Risk acceptance

Organizations apply safeguards to respond to vulnerabilities, threats, and, ultimately, risk. A safeguard is any protective action that reduces exposure to vulnerabilities or threats. A risk response strategy determines how safeguards should be applied.

Organizations can try to get rid of risk by applying safeguards to fix vulnerabilities and control threats. **Risk avoidance** is the process of applying safeguards to avoid a negative impact. A risk avoidance strategy seeks to eliminate all risk. This is often very difficult or expensive.

Organizations also can mitigate risk to reduce, but not eliminate, a negative impact. This response strategy is called **risk mitigation**. Using this strategy, organizations apply safeguards to vulnerabilities and threats to lower risk to an acceptable level. The amount of risk left over after applying safeguards is called **residual risk**.

Organizations also transfer risk. In a strategy of **risk transfer**, an organization passes its risk to another entity, at which point the risk impact is borne by the other entity. An organization might choose this type of strategy when the cost of mitigating risk is more expensive than transferring it. For example, organizations could purchase cyber liability insurance in response to a potential risk. By purchasing these policies, which have grown popular in the last several years, the organization transfers its risk to the insurance company, which bears the cost of any risk impact. While the terms of these insurance policies vary, they can cover losses caused by unauthorized access to information systems, system interruption, and crime.

An organization also can decide to deliberately take no action against an identified risk, which is called **risk acceptance**. This type of strategy means that avoiding, mitigating, or transferring risk is not part of the organization's risk response plan. Organizations do not take decisions to accept risk lightly, but may choose to accept the risk if the cost of the risk itself is less than the cost to avoid, mitigate, or transfer the risk.

Safeguards

A **safeguard** reduces the harm posed by information security vulnerabilities or threats and may eliminate or reduce the risk of harm. They are **controls** or countermeasures, terms that can be used interchangeably.

FYI

A passphrase is a long password that is made of a sequence of words or text. Unlike passwords, which are usually shorter, passphrases are usually 20 characters or more. The best passphrases are easy to remember. However, they should be hard to guess—for example, they should not be famous quotes from popular books.

Safeguards belong to different classifications according to how they work. These classification levels are:

- Administrative
- Technical
- Physical

Administrative safeguards are rules implemented to protect information and information systems. These safeguards usually take the form of organizational policies, which state the rules of the workplace. Laws and regulations may influence these safeguards. One common administrative safeguard is the workplace rule of **need to know**.

By applying need to know, an employer gives employees access only to the data they need to do their jobs. An employee does not receive access to any other data even if he or she has appropriate clearance. Using need-to-know principles makes it harder for unauthorized access to occur and protects confidentiality. There eventually should be technical enforcement of these principles. However, the first step is specifying that a workplace will follow them.

Technical safeguards, also called *logical safeguards*, are the rules that state how systems will operate and are applied in the hardware and software of information systems. Technical safeguards include automated logging and access-control mechanisms, firewalls, and antivirus programs. Using automated methods to enforce password strength is a technical control.

One technical safeguard that companies use to protect information security is the access control rule of **least privilege**. This rule, which is very similar to the need-to-know rule, means that systems should always run with the least amount of permissions needed to complete tasks. For example, some operating systems allow administrators to set up different privilege levels for system users. This helps enforce least privilege concepts. Users with administrative privileges can access all system functions, and therefore can fully manipulate and modify the system and its resources.

Local users, in contrast, have fewer privileges. They are able to use only some programs or applications. They cannot add, modify, delete, or manipulate the computer system. *Power users* have more privileges than local users but fewer privileges than administrators do. Power users may use and access many functions of the computer system. However, they may not modify critical functions of the operating system.

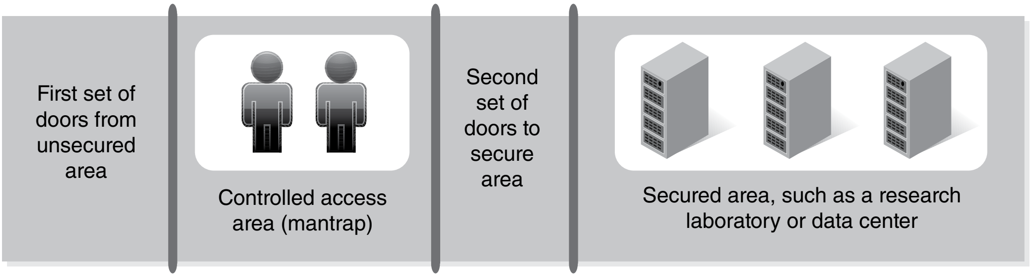
Physical safeguards are actions that an organization takes to protect its actual, tangible resources. These safeguards keep unauthorized individuals out of controlled areas and people away from sensitive equipment. Common physical safeguards are:

- Key-card access to buildings
- Fences
- Doors
- Locks
- Security lighting
- Video surveillance systems
- Security guards
- Guard dogs

A more sophisticated example of a physical security control is a **mantrap**, as shown in **FIGURE 1-3**. A mantrap is a method of controlled entry into a facility that provides access to secure areas such as a research lab or data center. This method of entry has two sets of doors on either end of a small room. When a person enters a mantrap through one set of doors, the first set must close before the second set can open. This process effectively "traps" a person in the small room.

FIGURE 1-3

An example of a mantrap.


First set of doors from unsecured area
Controlled access area (mantrap)
Second set of doors to secure area
Secured area, such as a research laboratory or data center

Often a person must provide different credentials at each set of mantrap doors. For example, the first set of doors might allow access to the mantrap via a card reader, in which an employee scans an identification badge to gain entry. The second set of doors then may require a different method to open, such as entering a PIN on a keypad. Technicians often configure mantraps so that both sets of doors lock if a person cannot provide the appropriate credentials at the second set of doors. When locked in a mantrap, the person must await "rescue" by a security guard or another official.

Mantraps are not just for highly sensitive data centers or labs. Some apartment buildings apply a modified mantrap concept to building entry. In these buildings, any individual can access the lobby area of the apartment building. However, only people with keys or access cards may pass through a locked security door and enter the building's interior. Usually, only residents have the proper credentials to enter the interior. Guests to the building need to use an intercom or telephone system to contact the resident they want to visit. The apartment resident can then "buzz" guests through the locked door to allow access to the building's interior.

You also can classify safeguards based on how they act. These classification levels are:

- Preventive
- Detective
- Corrective

Preventive controls are safeguards used to prevent security incidents. These controls keep an incident from happening. For example, door locks are a preventive safeguard, because they help keep intruders out of the locked area. Fencing around a building is a similar preventive control. Teaching employees how to avoid information security threats is another preventive control.

Detective controls are safeguards put in place in order to detect, and sometimes report, a security incident while it is in progress. Examples of detective controls include logging system activity and reviewing the logs. Log review can look for unauthorized access or other security anomalies that require attention. An *anomaly* is something strange or unusual—activity that is not normal.

Corrective safeguards are automated or manual controls put in place in order to limit the damage caused by a security incident. Some types of databases allow an administrator to "roll back" to the last known good copy of the database in the event of an incident. Corrective controls also can be quite simple: locking doors inadvertently left unlocked, for example.

TABLE 1-1 summarizes the safeguards described in this section.

TABLE 1-1 A Safeguards Matrix

SAFEGUARD TYPE	PREVENTIVE	DETECTIVE	CORRECTIVE
Administrative	Organization hiring policy	Organization periodic background checks policy	Discipline policy
Technical (Logical)	Least privilege principle	Antivirus software	Updating firewall rules to block an attack
Physical	Locks on doors to critical areas	Burglar alarms	Locking a door that was inadvertently left unlocked

Choosing Safeguards

Organizations may have difficulty choosing safeguards, so they use reference guides to help with this task. Two of the most common guides are the "ISO/IEC 27002:2013, Information Technology—Security Techniques—Code of Practice for Information Security Controls" (2013) and "NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations" (2013).

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) first published ISO/IEC 27002 in December 2000. These two groups work together to create standards for electronic technologies. ISO/IEC 27002 has 14 major sections. Each discusses a different category of information security safeguards or controls. They explain why organizations should use the listed controls and how to use them. Security practitioners often use ISO/IEC 27002 as a practical guide for developing security standards and best practices.

"NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations" was published in 2013 (and updated in 2015) by the National Institute of Standards and Technology (NIST). This document states the minimum safeguards required in order to create an effective information security program. NIST developed this guidance specifically for federal agency use on federal information systems. Many nongovernmental organizations also use the document to help guide their own information security programs. Revision 5 of this guidance, currently titled "Security and Privacy Controls for Information Systems and Organizations," was published in 2017. This draft was still undergoing the review process at the time this chapter was written.

What Are Common Information Security Concerns?

Information security practitioners have their hands full. This section describes some of the concerns that practitioners deal with daily.

Shoulder Surfing

As mentioned previously in this chapter, shoulder surfing occurs when an attacker looks over the shoulder of another person at a computer to discover sensitive information that the attacker has no right to see. This is not a technical exploit. The attacker could be attempting to learn usernames and passwords or discover sensitive information by viewing keystrokes on a monitor or keyboard. Shoulder surfing is a concern at public places such as automated teller machines (ATMs) or self-service credit card terminals at grocery stores.

Shoulder surfing can also can be a concern at airports, coffee shops, and other places with wireless access. Computer users may attempt to access email accounts, bank accounts, and other sensitive information while in these public places. Usually the computer user is focusing on their computing device and not paying attention to the people around them. While the user's guard is down, they may not notice that the coffee drinker at the next table is shoulder surfing and recording the computer user's sensitive information.

Social Engineering

Social engineering describes an attack that relies heavily on human interaction. It is not a technical attack. This type of attack involves tricking other people and taking advantage of their human nature to break normal security procedures and gain sensitive information.

These attacks are sometimes simple to carry out. For instance, an attacker telephones a large organization and identifies himself as a member of that same organization's technology group. He has a conversation with the person who answered the phone.

Technical TIP

You can guard against shoulder surfing attacks by shielding keypads with your hands. You also can hide an ATM screen by blocking it with your body so that attackers cannot view the screen. Laptop privacy guards and privacy shields also work well. These shields, which are placed over a monitor when computing in public places, restrict viewing angles so a person can only see the information on a monitor or screen when directly in front of it. Organizations may wish to purchase these types of privacy guards for workers who frequently travel. That way the person can work on business data in public places, such as an airport, while not worrying about shoulder surfing attacks.

The attacker might ask about that person's internet connectivity or computing equipment. The person answering the call, who is inclined to be helpful and participate in the conversation, trusts the attacker because he said that they both work for the same organization.

The attacker may ask for the person's username, identification number, or logon name at the end of the call, claiming that this is for verification purposes. The person answering the call might provide that information because it seems to be a reasonable request. Without much effort, the attacker has gained information that could be used to access organizational resources. This is a social engineering attack.

Phishing and Targeted Phishing Scams

Phishing is a form of internet fraud that takes place in electronic communications where attackers attempt to steal valuable information from their victims. These attacks can take place via email, instant messages, or internet chat rooms. These attackers are *phishing* for confidential information, including:

- Credit card numbers
- SSNs
- User logon credentials
- Passwords

A phishing attack may look similar to a legitimate message from a known organization that is familiar to the intended victim. It may also attempt to look similar to a message from well-known organizations such as banks or large corporations, or even the company that the intended victim works for.

Phishing messages usually request that the recipients click on a uniform resource locator (URL) to verify their account details. When the victim clicks on the URL, a website opens that looks similar to a legitimate site and prompts the victim to enter personal information to verify his or her identity. In reality, the site that the victim navigated to is a fake website, often a copy of a trusted site, designed only to capture the victim's personal information.

Spear phishing is a targeted phishing scam in which attackers may target a particular organization. This is a more sophisticated form of attack where a message might look as if it is from a highly trusted and authentic source. Attackers often research the targeted organization to make their messages look authentic. This background research is easy because of the wealth of information on the internet. Spear phishing messages may use an organization's logo or terms specific to it in their attempt to obtain information about the targeted organization, such as logons and passwords to the organization's information systems.

Whaling is a type of targeted phishing scam in which attackers target corporate executives. The federal judiciary circulated an alert in 2008 that warned that some corporate executives had received a scam email that claimed to be a grand jury subpoena. However, the email was not a real subpoena. Executives unintentionally downloaded malware onto their computer systems when they clicked on a link in the "subpoena" email.

Business email compromise (BEC) attacks are sophisticated phishing scams that target recipients who are responsible for processing payments at organizations. The goal of these types of attacks is to conduct unauthorized money transfers. The U.S. Federal Bureau of Investigation reported that BEC attacks led to the loss of over $12.5 billion across the world from October 2013 to May 2018.[3]

FYI

The Morris worm was one of the first internet computer worms. Robert Morris Jr., a student at Cornell University in 1988, created the worm. His experimental piece of code spread very quickly and infected some computers multiple times. Ultimately, over 6,000 computers were infected. It also overwhelmed government and university networked systems. Morris was charged with violating the 1986 Computer Fraud and Abuse Act. He was convicted and sentenced to a $10,000 fine, 400 hours of community service, and 3 years' probation.

Malware

Malware is a general term that refers to any type of software that performs some sort of harmful, unauthorized, or unknown activity. The term *malware* is a combination of the words *malicious* and *software*. Malware is usually a computer virus or worm, or a combination of one or more viruses or worms.

Computer viruses are programs that spread by infecting applications on a computer. These types of programs are called viruses because they resemble biological viruses. They copy themselves in order to infect a computer. Viruses can spread over a computer network or the internet. They also can spread from computer to computer on infected disks, CDs, DVDs, or universal serial bus (USB) thumb drives. When the infected virus code is executed, it tries to place itself into uninfected software.

A computer worm is similar to a virus. Unlike a virus, however, a computer worm is a self-contained program that does not require external assistance to propagate. Some well-known internet worms include the Morris worm, SQL Slammer, and Blackworm.

A Trojan horse is a subset of malware that pretends to be a legitimate and desirable software file that a user wants. In reality, it is malicious. A Trojan horse spreads when a user downloads the seemingly legitimate file. While the user believes a legitimate file is downloading, the Trojan horse is actually loading. This type of malware is especially prevalent on social networking sites. Accepting virtual "gifts" on these sites can often expose users to nasty surprises.

Ransomware is a subset of malware that prevents organizations and users from accessing data or information systems until they pay a ransom. The ransomware may encrypt data to make it inaccessible, or it may lock information systems, until an organization pays the attacker to decrypt the data or unlock the system. Ransomware is not new, but its use across all industries has been growing.

Spyware and Keystroke Loggers

Spyware and keystroke loggers are also forms of malware. Spyware is any technology that secretly gathers information about a person or organization. Many users inadvertently download spyware with other programs from the internet. Spyware hides on a system, where it collects information about individuals and their internet browsing habits. Cookies set by websites can allow spyware to track the sites that a person visits. This is especially dangerous because some cookies can contain website logon and password information. Spyware can slow computer systems, hog resources, and use network bandwidth. Some spyware programs install other programs on a computer system, which can make a computer system open to other attacks.

A keystroke logger is a device or program that records keystrokes made on a keyboard or mouse. Attackers secretly install keystroke loggers and then are able to recover computer keyboard entries and sometimes even mouse clicks from them. They can review the data retrieved from a keystroke logger to find sensitive information such as usernames, passwords, and other confidential user information. The student hackers in the Florida A&M example discussed earlier in this chapter used a keystroke logger, which allowed them to obtain computer access credentials from data the logger collected. Keystroke loggers can be software-based or they can be a physical device that plugs into a computer or is hidden in a keyboard.

Logic Bombs

A logic bomb is harmful code intentionally left on a computer system that lies dormant for a certain period. When specific conditions are met, it "explodes" and carries out its malicious function. Programmers can create logic bombs that explode on a certain day or when a specific event occurs. Attackers also program logic bombs to explode in response to no action; for example, a logic bomb may explode when its creator does not log onto the target computer system for a predetermined number of days.

Upset employees sometimes use logic bombs. In October 2008, for example, Fannie Mae fired an employee from his Unix engineer position but failed to disable his computer access to Fannie Mae systems until nearly 4 hours after his firing. The engineer allegedly tried to hide a logic bomb in the computer system during that time. This logic bomb was set to activate the morning of January 31, 2009, and designed to delete 4,000 Fannie Mae servers when activated.

Fannie Mae IT professionals accidentally found the logic bomb 5 days after the former employee planted the "explosive." The employee was indicted in January 2009 for unauthorized computer access. In October 2010 he was convicted in U.S. federal court of computer sabotage and sentenced to 3 years in prison.

Backdoors

A backdoor, also called a *trapdoor*, is a way to access a computer program or system that bypasses normal mechanisms. Programmers sometimes install a backdoor to access a program quickly during the development process to troubleshoot problems. This is especially helpful when developing large and complex programs. Programmers usually remove backdoors when the programming process is over. However, they can easily forget about the backdoors if they do not follow good development practices.

A backdoor is a security vulnerability regardless of its initial purpose. Attackers search for system backdoors to exploit them. Sometimes attackers install backdoors on systems they want to visit again. Attackers can have virtually unhindered access to a system through a backdoor.

NOTE

The computer worm MyDoom, first discovered in January 2004, installed backdoors on infected Microsoft Windows computers. Attackers could then send spam email from the infected machines, which helped to spread the worm. Some versions of the MyDoom worm also blocked access to popular antivirus software vendor websites. This made it very hard to remove the worm.

Denial of Service Attacks

You learned about DoS attacks that disrupt information systems earlier in the chapter. Attackers do this so that the systems are not available for legitimate users. These attacks can disable an organization's web page or internet-based services.

A **distributed denial of service (DDoS) attack** is another form of DoS attack that occurs when attackers use multiple systems to attack a targeted system. These attacks really challenge the targeted system, because it often cannot ward off an attack coming from hundreds or thousands of different computers. A DDoS attack sends so many requests for services to a targeted system that the system or website is overwhelmed and cannot respond.

In a DDoS attack, the attacker takes control of multiple systems to coordinate the attack. They call this type of attack "distributed" because it involves multiple systems to launch the attack. Usually the attacker exploits security vulnerabilities in many machines. The attacker then directs the compromised machines to attack the target. Another term for these compromised machines is *zombies*. Major websites are often DDoS attack victims. These systems handle a lot of traffic by design and pose an attractive target for DDoS attackers seeking to compromise a system's availability.

NOTE

In 2013, Google Ideas and Arbor Networks created a live data visualization of DDoS attacks around the world. In January 2020 the United States was one of the most popular destination countries for these types of attacks. To see the map, visit www.digitalattackmap.com.

Information security deals with these types of issues every day. Organizations can implement safeguards to help decrease the impact of such attacks.

What Are the Mechanisms That Ensure Information Security?

Protecting information is not easy. It is often expensive and time consuming to do well. The security of a system relates to the time taken to implement safeguards and their cost. Highly secure information systems take significant time and expense to create. Alternatively, if an organization wants to implement secure systems quickly, it must be prepared to spend money. If it wants to keep time and money costs low, it must be prepared for lower security.

Laws and Legal Duties

Most organizations are subject to several laws. Although this text focuses on laws that affect information security, these are not the only types of laws organizations must follow. For example, they may have to follow workplace safety laws and fair labor standards. Other laws may include those dealing with equal employment opportunity, hazardous materials disposal, and transportation. An organization must make sure that it follows all of the laws that apply to it.

Industry sector is a term that describes a group of organizations that share a similar industry type. They often do business in the same area of the economy. In the United States, Congress enacts laws by industry sector. These laws address the protection of data used by organizations in a particular industry, such as finance or health care. Even the federal government has laws that it must follow to secure certain types of information. Some of these laws have very specific requirements.

Organizations also must follow general legal duties. For example, executives must act reasonably and in the best interest of the organization. This means they must use good judgment when making decisions for the organization.

Contracts

The action of paying someone to do work on your behalf is called outsourcing. Many organizations outsource IT functions to save money. Outsourced functions can include data center hosting, email facilities, and data storage.

For example, it is very expensive for organizations to build their own data center. It is often cheaper for some of them to rent equipment space in another organization's data center.

An organization cannot avoid its legal duties by outsourcing functions. It must enter into a contract with the company to which it is outsourcing. A *contract* is a legal agreement between two or more parties that sets the ground rules for their relationship. The parties use a contract to define their relationship and state their

NOTE

Data centers are not inexpensive. In January 2010, Facebook, a social networking application and website, announced plans to build its first data center. In 2018 the company reported that it had 15 data centers, with more planned. The company estimates that it has 2.45 billion active monthly users around the world, requiring sizable server and data storage needs.

obligations. Organizations must include specific security clauses and safeguards in outsourcing contacts to make sure they meet their legal obligations.

Organizational Governance

An organization's governance documents form the basis for its information security program. These documents include:

- Policies
- Standards
- Procedures
- Guidelines

They show the organization's vow to protect its own information and that which is entrusted to it. Policies are the top level of governance documents. A *policy* tells an organization how it must act and the consequences for failing to act properly. It is important for an organization's management team to support its policies, because policies often fail without that top-level support.

NOTE

As discussed earlier in the chapter, a policy is an administrative safeguard.

Standards state the activities and actions needed to meet policy goals. They state the safeguards necessary to reduce risks and meet policy requirements. Standards do not refer to particular technologies, operating systems, or types of hardware or software.

Procedures are step-by-step checklists that explain how to meet security goals. Procedures are the lowest level of governance documents. They often are tailored to a certain type of technology. They also can be limited to the activities of specific departments, or even specific users in departments. Procedures are revised often as technology changes.

Guidelines, which are recommended actions and guides for employees, tell users about information security concerns and suggest ways to deal with them. Guidelines should be flexible for use in many situations.

Data Protection Models

One way that organizations put their governance documents into practice is by creating data protection models. In addition to following relevant laws for certain types of data, an organization might also protect data based upon its sensitivity to the organization. Not all information has the same level of sensitivity. An organization must weigh the sensitivity of information against the way in which it wants to use that information. To do this easily, an organization might choose to create data protection models to classify the different types of information it uses.

To create a data protection model, an organization first creates data classification levels. These levels serve as the basis for specifying certain types of safeguards for different categories of data. Information that would not harm the organization with its disclosure might be labeled *public* information. This would be the lowest classification of data and would typically have no special rules for its use.

Information that would harm the organization, its reputation, or its **competitive edge** if publicly disclosed might be called *confidential*. Another term that is often used for this type of information is *restricted*.

Organizations take many steps to protect this type of information. For example, they create rules that prevent unauthorized access to it. Other rules might address the sharing and storage of this information and its disposal.

NOTE

Because businesses compete for customers and money, they must distinguish themselves from their competitors. A competitive edge is the designs, blueprints, or features that make one organization's products or services unique. Protecting competitive edge is one of the functions of information security.

An organization must carefully review its data and put it in the proper classification level. For example, if an organization has advertising materials that it freely gives to its customers, it would probably assign these materials to the "public" category. The organization has no special rules for how employees should protect this information, so employees are able to freely use, copy, and share this type of information. The organization also might have design blueprints for its products. These documents contain the secrets that make the organization's products special. This type of material is labeled "restricted." Employees are limited in how they can use, copy, or share this information.

Data classification is a common way to think about protecting data. The general rule for protecting information is that the more sensitive or confidential the information, the fewer people that should have access to it. Very sensitive information should have more safeguards, whereas information that is not as sensitive does not need such extensive protection.

Another part of protecting information involves reviewing security goals in the C-I-A triad. All organizations must decide which goals are most important to them. For some organizations, making sure their data is available and accurate is the most important goal. These organizations use controls that ensure that correct data is always available to their customers.

Military or government organizations may place a higher value on confidentiality and integrity goals because they value secrecy and accuracy. It is usually very important to them that sensitive data not fall into the wrong hands. It is equally important that their data be correct, because key personnel rely on it when making decisions. These organizations use controls that ensure that data is accurate and protected from unauthorized access.

U.S. National Security Information

The U.S. government also classifies its data and specifies rules for using classified information. President Barack Obama signed *Executive Order 13526* in December 2009, which describes a system for classifying national security information. The Order establishes three classification levels—confidential, secret, and top secret. The difference between the levels is the amount of harm that could be caused to U.S. security if the data were disclosed to an unauthorized person.

- *Confidential* describes information that could cause damage to U.S. security if disclosed to an unauthorized person. This is the lowest data classification level.
- *Secret* describes information that could cause serious damage to U.S. security if disclosed to an unauthorized person.
- *Top secret* is the highest classification level. This type of information could cause exceptionally grave damage to U.S. security if disclosed to an unauthorized person.

The Order also sets forth the rules to follow when using national security information. Among other rules, it states how the information must be marked and identified. It also gives instructions on how long it must remain classified. In addition, the Order specifies when to release such information to the public.

Voluntary Organizations

Individuals and organizations may belong to voluntary membership groups that seek to promote information security. Group members often have rules that they agree to follow. These rules usually set forth behavior expectations and are usually ethical in nature. They sometimes are called a code of practice or code of ethics.

Whole organizations also participate in voluntary membership groups and agree to follow the terms of codes of conduct. For example, the Internet Commerce Association (ICA) adopted a code of conduct for its member organizations in 2007 to provide for fair practice in the domain name industry. Its rules require protection of intellectual property rights, as well as for members to abide by internet fraud laws, including laws to stop the spread of phishing scams. You can learn more about the code at www.internetcommerce.org/about-us/code-of-conduct/.

Do Special Kinds of Data Require Special Kinds of Protection?

The United States does not have one comprehensive data protection law. Therefore, many laws focus on different types of data found in different industries. They also focus on how that data is used. Several federal agencies regulate compliance with these types of laws.

The Health Insurance Portability and Accountability Act (HIPAA) regulates some kinds of health information. The Department of Health and Human Services (HHS) and Office of Civil Rights (OCR) oversee HIPAA compliance. The Gramm-Leach-Bliley Act (GLBA) protects some types of consumer financial information. The Federal Trade Commission (FTC) ensures compliance. **TABLE 1-2** lists several important laws, the information they regulate, and the agency that enforces them. Many of these laws will be further explored in this book.

TABLE 1-2 Laws That Influence Information Security

NAME OF LAW	INFORMATION REGULATED	REGULATING AGENCY
Gramm-Leach-Bliley Act	Consumer financial information	Federal Trade Commission
Red Flags Rule	Consumer financial information	Federal Trade Commission
Payment Card Industry Standards*	Credit card information	Credit card issuers via contract provisions
Health Insurance Portability and Accountability Act	Protected health information	Department of Health and Human Services
Children's Online Privacy Protection Act	Information from children under the age of 13	Federal Trade Commission
Children's Internet Protection Act	Internet access in certain schools and libraries	Federal Communications Commission
Family Educational Rights and Privacy Act	Student educational records	U.S. Department of Education
Sarbanes-Oxley Act	Corporate financial information	Securities and Exchange Commission
Federal Information Systems Management Act	Federal information systems	Office of Management and Budget, and Department of Homeland Security
State breach notification acts	State information systems containing protected health information	Varies among states

*The Payment Card Industry (PCI) Standards are not a law. Organizations that wish to accept credit cards for payment of goods and services must follow these standards.

CHAPTER SUMMARY

Information security is the study and practice of protecting information, which is important because information is valuable. Organizations need data to conduct business. Governments need information to protect their citizens. Individuals need information to interact with businesses and government agencies, as well as stay in touch with friends and family over the web. Information is a critical resource that must be protected.

The main goal of information security is to protect the confidentiality, integrity, and availability of information. Basic information security concepts include vulnerabilities, threats, risks, and safeguards.

KEY CONCEPTS AND TERMS

Administrative safeguard
Availability
Competitive edge
Confidentiality
Control
Cryptography
Denial of service (DoS) attack
Distributed denial of service (DDoS) attack
Exploit
External attacker
Information
Information security
Integrity
Internal attacker
Least privilege
Malware
Mantrap
Need to know
Patch
Physical safeguard
Residual risk
Risk
Risk acceptance
Risk avoidance
Risk mitigation
Risk transfer
Safeguard
Separation of duties
Shoulder surfing
Single point of failure
Social engineering
Technical safeguard
Threat
Vulnerability
Window of vulnerability
Zero-day vulnerability

CHAPTER 1 ASSESSMENT

1. What are the goals of an information security program?

A. Authorization, integrity, and confidentiality
B. Availability, authorization, and integrity
C. Availability, integrity, and confidentiality
D. Availability, integrity, and safeguards
E. Access control, confidentiality, and safeguards

2. An employee can add other employees to the payroll database. The same person also can change all employee salaries and print payroll checks for all employees. What safeguard should you implement to make sure that this employee does not engage in wrongdoing?

A. Need to know
B. Access control lists
C. Technical safeguards
D. Mandatory vacation
E. Separation of duties

3. An organization obtains an insurance policy against cybercrime. What type of risk response is this?

A. Risk mitigation
B. Residual risk
C. Risk elimination
D. Risk transfer
E. Risk management

4. Which of the following is an accidental threat?

A. A backdoor into a computer system
B. A hacker
C. A well-meaning employee who inadvertently deletes a file
D. An improperly redacted document
E. A poorly written policy

5. What is the window of vulnerability?

A. The period between the discovery of a vulnerability and mitigation of the vulnerability
B. The period between the discovery of a vulnerability and exploiting the vulnerability
C. The period between exploiting a vulnerability and mitigating the vulnerability
D. The period between exploiting a vulnerability and eliminating the vulnerability
E. A broken window

6. A technical safeguard is also known as a ________.

7. Which of the following is not a threat classification?
   A. Human
   B. Natural
   C. Process
   D. Technology and operational
   E. Physical and environmental

8. What information security goal does a DoS attack harm?
   A. Confidentiality
   B. Integrity
   C. Authentication
   D. Availability
   E. Privacy

9. Which of the following is an example of a model for implementing safeguards?
   A. ISO/IEC 27002
   B. NIST SP 80-553
   C. NIST SP 800-3
   D. ISO/IEC 20072
   E. ISO/IEC 70022

10. Which of the following is not a type of security safeguard?
    A. Corrective
    B. Preventive
    C. Detective
    D. Physical
    E. Defective

11. It is hard to safeguard against which of the following types of vulnerabilities?
    A. Information leakage
    B. Flooding
    C. Buffer overflow
    D. Zero-day
    E. Hardware failure

12. What are the classification levels for the U.S. national security information?
    A. Public, sensitive, restricted
    B. Confidential, secret, top secret
    C. Confidential, restricted, top secret
    D. Public, secret, top secret
    E. Public, sensitive, secret

13. Which safeguard is most likely violated if a system administrator logs into an administrator user account in order to surf the internet and download music files?
    A. Need to know
    B. Access control
    C. Least privilege principle
    D. Using best available path
    E. Separation of duties

14. Which of the following are vulnerability classifications?
    A. People
    B. Process
    C. Technology
    D. Facility
    E. All of these are correct.

15. What is a mantrap?
    A. A method to control access to a secure area
    B. A removable cover that allows access to underground utilities
    C. A logical access control mechanism
    D. An administrative safeguard
    E. None of these is correct.

ENDNOTES

1. National Vulnerability Database, *NVD Dashboard*. https://nvd.nist.gov/general/nvd-dashboard (accessed January 19, 2020).
2. CNBC, "Ex-Coca-Cola Worker Sentenced to 8 Years in Trade Secrets Case," May 2007. https://www.cnbc.com/id/18824080 (accessed January 19, 2020).
3. Federal Bureau of Investigation, "Business E-Mail Compromise: The 12 Billion Dollar Scam," July 2018. https://www.ic3.gov/media/2018/180712.aspx (accessed January 20, 2020).