Chapter 2 Answers to Review Questions and Exercises

Review Questions

1. Why is information security a management problem? What can management do that technology cannot?

   General management, IT management, and information security management are each responsible for implementing information security that protects the organization's ability to function.

   Decision makers must set policy and operate their organizations in a manner that complies with complex, shifting political legislation concerning the use of technology. Management is responsible for informed policy choices, the enforcement of decisions that affect applications, and the IT infrastructures that support them. Management can also implement an effective information security program to protect the integrity and value of the organization's data.

2. Why is data the most important asset an organization possesses? What other assets in the organization require protection?

   Without data, an organization will lose its record of transactions and its ability to deliver value to customers. Any business, educational institution, or government agency that functions within the modern social context of connected and responsive service relies on information systems to support these services. Protecting data is critical to these efforts.

   Other assets that require protection include the ability of the organization to function, the safe operation of applications, and technology assets.

3. Which management groups are responsible for implementing information security to protect the organization's ability to function?

   General management, IT management, and information security management are each 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, implementing information security actually has more to do with management than technology. Just as managing payroll involves management more than mathematical wage computations, managing information security has more to do with policy and its enforcement than the technology of its implementation.

4. Has the implementation of networking technology created more or less risk for businesses that use information technology? Why?

   Networking is usually considered to create more risk for businesses that use information technology because potential attackers have better access to information systems when they have been networked, especially if they are connected to the Internet.

5. What is information extortion? Describe how such an attack can cause losses, using an example not found in the text.

   When an attacker can control access to an asset, it can be held hostage to the attacker's demands. For example, if attackers gain access to a database and then

encrypt its data, they may extort money or other value from the owner by threatening to share the encryption key and the data with others.

6. Why are employees one of the greatest threats to information security?

   Employees are the greatest threats because they are the people closest to the organization's data and they have access to it. Employees use data in their everyday work activities, and employee mistakes represent a serious threat to the confidentiality, integrity, and availability of data. Employee mistakes can easily lead to the revelation of classified data, entry of erroneous data, accidental data deletion or modification, storage of data in unprotected areas, and failure to protect information.

7. How can you protect against shoulder surfing?

   The best way to avoid shoulder surfing is to avoid accessing confidential information when another person is present. People should limit the number of times they access confidential data, and do it only when they are sure nobody can observe them. Users should be constantly aware of the presence of others when accessing sensitive information.

8. How has the perception of the hacker changed over recent years? What is the profile of a hacker today?

   The classic perception of hackers is frequently glamorized in fictional accounts as people who stealthily manipulate their way through a maze of computer networks, systems, and data to find the information that resolves the dilemma posed in the plot and saves the day. However, in reality, hackers frequently spend long hours examining the types and structures of targeted systems because they must use skill, guile, or fraud to bypass the controls placed on information owned by someone else.

   The perception of a hacker has evolved over the years. The traditional hacker profile was a male, aged 13 to 18, with limited parental supervision who spent all his free time at the computer. The current profile of a hacker is a male or female, aged 12 to 60, with varying technical skill levels, and who can be internal or external to the organization. Hackers today can be expert or unskilled. The experts create the software and schemes to attack computer systems, while the novices merely use software created by the experts.

9. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?

   An expert hacker develops software scripts and codes to exploit relatively unknown vulnerabilities. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems.

   Unskilled hackers use scripts and code developed by skilled hackers. They rarely create or write their own hacks, and are often relatively unskilled in programming languages, networking protocols, and operating systems.

   Protecting against expert hackers is much more difficult, partly because they often use new, undocumented attack code that makes it almost impossible to guard against the attacks at first. Conversely, an unskilled hacker generally uses hacking tools that are publicly available. Therefore, protection against these hacks can be maintained by staying up to date on the latest patches and being aware of tools

that have been published by expert hackers.

10. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?

    Common types of malware are viruses, worms, Trojan horses, logic bombs, and back doors.

    Computer viruses are segments of code that induce other programs to perform actions. Worms are malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication.

    Once a trusting user executes a Trojan horse program, it unleashes viruses or worms to the local workstation and the network as a whole.

11. Why does polymorphism cause greater concern than traditional malware? How does it affect detection?

    Polymorphism causes greater concern because it makes malicious code more difficult to detect. The code changes over time, so commonly used antivirus software, which uses preconfigured signatures for detection, is often unable to detect the new attack. This makes polymorphic threats harder to protect against.

12. What is the most common violation of intellectual property? How does an organization protect against it? What agencies fight it?

    The most common violations involve the unlawful use or duplication of software-based intellectual property, known as software piracy.

    Some organizations have used such security measures as digital watermarks, embedded code, copyright codes, and even the intentional placement of bad sectors on software media. Also, most companies file patents, trademarks, or copyrights, which can allow them to legally pursue violators. Another effort to combat piracy is online registration. During installation, users are asked or even required to register their software to obtain technical support or full use of all features.

    Two major organizations investigate allegations of software abuse: the Software and Information Industry Association (SIIA) and the Business Software Alliance (BSA).

13. What are the various forces of nature? Which type might be of greatest concern to an organization in Las Vegas? Jakarta? Oklahoma City? Amsterdam? Miami? Tokyo?

    Forces of nature, sometimes called acts of God, pose a risk to people's lives and information security. Forces of nature include fire, flood, earthquakes, lightning, mudslides, tornados, hurricanes, typhoons, tsunamis, electrostatic discharge (ESD), and dust contamination.

    A major concern to an organization in Las Vegas might be dust contamination. Jakarta poses unusually high risks of losses caused by typhoons, earthquakes, and tsunamis. Tornados are a concern for organizations in Oklahoma City. Organizations in Amsterdam may have concerns about flooding from storm surges that could overtop the city's system of dikes. Miami would be most concerned with hurricanes or tsunamis. Earthquakes would be of concern to organizations in Tokyo.

14. How is technological obsolescence a threat to information security? How can an organization protect against it?

    Technological obsolescence is a security threat caused by management's potential lack of planning and failure to anticipate the technology needed for evolving business requirements. Technological obsolescence occurs when infrastructure becomes outdated, which leads to unreliable and untrustworthy systems. As a result, an organization risks loss of data integrity from attacks.

    One of the best ways to prevent this obsolescence is through proper planning by management. Once discovered, outdated technologies must be replaced. Information technology personnel must help management identify probable obsolescence so that technologies can be replaced or upgraded as needed and in a timely fashion.

15. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?

    Yes, the IP of an organization may be its most valuable asset. Attackers can threaten its economic value by reducing or removing its availability to the owner or by stealing and then selling copies of the asset.

16. What are the types of password attacks? What can a systems administrator do to protect against them?

    The types of password attacks include password crack, brute force, and dictionary attacks.

    Password crack: Attempting to reverse-calculate a password is called "cracking." This attack is used when a copy of the Security Account Manager (SAM) data file can be obtained. A possible password is taken from the SAM file and run through the hashing algorithm in an attempt to guess the actual password.

    Brute force: The application of computing and network resources to try every possible combination of options for a password.

    Dictionary: A form of brute force for guessing passwords. The dictionary attack selects specific accounts and uses a list of common passwords to make guesses.

    To protect against password attacks, security administrators can:

    - Implement controls that limit the number of attempts allowed.
    - Use a "disallow" list of passwords from a similar dictionary.
    - Require use of additional numbers and special characters in passwords.

17. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?

    A denial-of-service (DoS) attack occurs when an attacker sends a large number of connection or information requests to a target. A distributed denial-of-service (DDoS) attack occurs when a coordinated stream of requests is launched against a target from many locations at the same time.

    A DDoS attack is potentially more dangerous and devastating. In most DDoS attacks, numerous machines are first compromised and used as "zombies" to carry out the DoS attack against a single target. DDoS attacks are more difficult to defend against, as there are currently no controls any single organization can apply.

18. For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?

    The attacker must first gain access to a network to install the sniffer.

    Social engineering offers the best way for an attacker to gain access to a network and install a physical sniffer device. By convincing an unwitting employee to identify the location of the networking equipment, the attacker can install the sniffer.

19. What methods does a social engineering hacker use to gain information about a user's login ID and password? How would this method differ if it targeted an administrator's assistant versus a data-entry clerk?

    Social engineering is the process of using social skills to obtain access credentials or other valuable information. For example, attackers can use role playing to represent themselves as people of authority who are requesting information. Other approaches include installing bogus software on user machines to gather access information and using deception to act on the conscience of users.

    Tactics change based on the target. A data-entry clerk could likely be swayed just by mentions of the CEO's name and his anger at not getting requested information promptly. Conversely, someone higher up the chain of command would require more convincing proof, such as additional details regarding a particular project or something as precise as an authorization password or document.

20. What is a buffer overflow, and how is it used against a Web server?

    A buffer overflow occurs when more data is sent to a buffer than it can handle. The overflow can be caused over a network when there is a mismatch in the processing rates between the two communicating entities.

Exercises

1. Consider that an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker breaks into a network, copies a few files, defaces a Web page, and steals credit card numbers, how many different threat categories does the attack fall into?

    - Deliberate acts are the main threat category for this type of attack because the hacker is deliberately trying to cause harm. This attack could fall under different subcategories, such as deliberate acts of espionage or trespass, deliberate acts of sabotage or vandalism, and deliberate acts of theft.
    - Compromises to intellectual property—copying files, defacing a Web page, and stealing credit card numbers.
    - Technical failures. For instance, if part of the organization's software has an unknown trap door, this type of hacker attack could occur.
    - Management failure. This type of hacker attack could happen if management used insufficient planning and foresight to anticipate the technology need for evolving business requirements.

2. Using the Web, research Mafiaboy's exploits. When and how did he compromise sites? How was he caught?

    Mafiaboy's exploits consisted of a series of DDoS attacks on 11 corporate

networks. According to investigators, the attacks caused approximately $1.7 billion in losses to the companies, although the accuracy of that figure is disputed. The attacks made some corporate Web sites and networks difficult to reach. In other cases, they crashed completely, remaining offline from hours to several days. Because the attacks were so large, authorities were prompted to investigate. They found that someone by the name of Mafiaboy was bragging about the attacks on Web sites, message boards, and even his own site. In addition, authorities were able to associate an IP address to the attacks, which in turn was linked to an Internet service provider (ISP). With the ISP's help, authorities linked the IP address to an account whose phone numbers were linked to Mafiaboy's father.

Alternate Answer

Mafiaboy was an example of a teen novice using precoded exploits to launch DDoS attacks against several high-profile Web sites. Mafiaboy's attacks brought down many of the Internet's largest sites. The tools he used are widely available on the Internet and require little computer knowledge, being simple enough for use by script kiddies. Mafiaboy simply ran a computer script that clogged networks full of garbage data. He was deemed an unskilled attacker for several reasons, but primarily because he failed to take basic steps to cover his tracks, such as erasing logs. A series of computer taps led to Mafiaboy's arrest.

Nonetheless, his lack of skills did not stop him from shutting down many prominent Web sites. Mafiaboy gained illegal access to 75 computers in 52 different networks, planted and activated a DoS tool on them, and used it to attack 11 Internet sites by sending up to 10,700 phony information requests in 10 seconds.

Amazon.com, Yahoo!, Buy.com, CNN.com, and more than 1,200 other sites CNN hosts worldwide, including Dell.com and eBay, are among the sites Mafiaboy was able to cripple. The cost to these companies was estimated to be in the millions or even billions of dollars. For a company whose only storefront is Web-based, this type of attack can be a disaster, as thousands of dollars of revenue might be lost per hour of inactivity. Because Amazon.com's Web site was inaccessible for more than a day, the company probably lost several million dollars. Buy.com and Yahoo! offered more concrete numbers; each company lost $1 million every four hours that their networks were inaccessible.

3. Search the Web for "The Official Phreaker's Manual." What information in this manual might help a security administrator to protect a communications system?

   Phone phreaking is the act of using mischievous and mostly illegal methods to avoid paying for a telecommunications invoice, order, transfer, or other service. It often involves usage of illegal boxes and machines to defeat security that is set up to avoid such tactics. This security includes "blocking networks"—networks that under certain conditions may be unable to form a transmission path from one end to the other. In general, all networks used within the Bell Systems are of the blocking type.

   Security administrators could benefit from studying "The Official Phreaker's Manual" because it could allow them to better protect their communications systems. From the system administrator's point of view, this information could reveal many common ways of finding loopholes and alternate methods around

communications system security measures. The manual could also help system administrators use different approaches in implementing a more extensive security program.

4. The chapter discussed many threats and vulnerabilities to information security. Using the Web, find at least two other sources of information about threats and vulnerabilities. Begin with *www.securityfocus.com* and use a keyword search on "threats."

   Possible results are:

   - *http://csrc.ncsl.nist.gov/*—This site describes new security standards and the reasons that organizations should adopt them.
   - *http://icat.nist.gov/icat.cfm*—This site is a searchable index of information on computer vulnerabilities.
   - *http://security1.gartner.com/section.php.id.19.s.1.jsp*—This site features a variety of articles about information security concerns written by industry experts, especially in the corporate world.
   - *www.cerias.purdue.edu/*
   - *www.cert.org/stats*
   - *www.fedcirc.gov/*—Information on reported threats
   - *www.gocsi.com*
   - *www.idc.com*
   - *www.infomaticsonline.co.uk*
   - *www.iss.net/security_center/*
   - *www.microsoft.com/security/*—Microsoft's listing of important announcements for security and privacy
   - *www.riptech.com*
   - *www.securityfocus.com/*—Lists of threats, vulnerabilities, and advisories
   - *www.siliconvalley.com*
   - *www.symantec.com/avcenter/*—Information on the latest viruses and security advisories
   - *www.theregister.co.uk/content/55/index.html*—The Register's listing of the latest threats
   - *www.theregus.com*—New information about the technology industry, including security breaches of information systems in various companies
   - *www.washtimes.com*
   - *http://zdreviews.search.com*
   - *www.security-survey.gov.uk*

5. Using the categories of threats mentioned in this chapter and the various attacks described, review several current media sources and identify examples of each threat.

   Answers will vary.

Chapter 2

The Need for Security

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

Chapter 2 examines the business drivers behind the security analysis design process. It examines current needs for security in organizations and technology. One principle concept is that information security is primarily an issue of management, not technology. Best practices apply technology only after considering the business needs.

The chapter also examines the various threats facing organizations and presents the process of ranking these threats to provide relative priority as the organization begins the security planning process. The chapter continues with a detailed examination of the types of attacks that could occur from these threats, and discusses how they could impact the organization's information and systems. The chapter concludes with a discussion of development failures and errors that result from poor software security efforts.

Chapter Objectives

In this chapter, your students will learn to:

- Discuss the organizational business need for information security
- Explain why a successful information security program is the shared responsibility of an organization's three communities of interest
- List and describe the threats posed to information security and common attacks associated with those threats
- List the common development failures and errors that result from poor software security efforts

Teaching Tips

Introduction

1. Discuss the view that information security is unlike any other aspect of information technology. The primary mission is to ensure things stay the way they are. Point out that if there were no threats to information and systems, we could focus on improving systems that support the information.

2. Explain that organizations must understand the environment in which information systems operate so that their information security programs can address actual and potential problems.

3. Explain to students that information security performs the following four important functions for an organization:
    - Protecting the organization's ability to function
    - Protecting the data and information the organization collects and uses
    - Enabling the safe operation of applications running on the organization's IT systems
    - Safeguarding the organization's technology assets

Business Needs First

Teaching Tip	This is an important point that students need to understand since the concepts in this unit will affect the balance of the text. Students should be encouraged to view information security as one of several means to solve a business problem.

Protecting Functionality

1. Discuss the fact that general management, IT management, and information security management are responsible for implementing information security to protect the ability of the organization to function.

2. Note that "information security is a management issue in addition to a technical issue, it is a people issue in addition to the technical issue."

3. Explain that to assist management in addressing the need for information security, communities of interest must communicate in terms of business impact and the cost of business interruption, and they must avoid arguments expressed only in technical terms.

Protecting Data that Organizations Collect and Use

1. Students should understand that many organizations realize that one of their most valuable assets is their data. Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.

2. Explain that data security, which is protecting data in motion and data at rest, is a critical aspect of information security. An effective information security program is essential to the protection of the integrity and value of the organization's data.

Enabling the Safe Operation of Applications

1. Discuss that today's organizations are under immense pressure to create and operate integrated, efficient, and capable applications. The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the organization's infrastructure.

2. Point out to students that once the infrastructure is in place, management must continue to oversee it and not abdicate its responsibility to the IT department.

Safeguarding Technology Assets in Organizations

1. Remind students that to perform effectively, organizations must add secure infrastructure services based on the size and scope of the enterprise.

2. Emphasize that as the organization's network grows to accommodate changing needs, more robust technology solutions may be needed to replace security programs the organization has outgrown.

Teaching Tip	Students need to understand that a successful information security program is a program that engages the business and empowers the business to accomplish its goals while maintaining security of the organization. Data loss is a tangible risk to organizations and managing that risk is something that the security program should strive to manage from a business perspective rather than a state of fear. Consider the following: http://it.toolbox.com/blogs/adventuresinsecurity/fear-trust-and-desire-fertile-ground-for-social-engineers-31078.

Threats and Attacks

1. Remind students that to make sound decisions about information security as well as to create and enforce policies, management must be informed of the various kinds of threats facing the organization and its applications, data, and information systems.

2. Explain that a threat is an object, person, or other entity that represents a constant danger to an asset. Point out that an attack represents an ongoing act against the asset that could result in a loss. Also mention that threat agents use exploits to take advantage of vulnerabilities where controls are not present or are no longer effective.

Teaching Tip	It is quite easy to get the conceptual underpinning of threats and attacks (see the following section) confused. As you teach your students, keep in mind that threats are a latent danger to information assets, whether probable or theoretical. Attacks are ways in which threats are manifested.

3.6 Billion Potential Hackers

1. Discuss the agreement that the threat from external sources increases when an organization cocnnects to the Internet.

Other Studies of Threats

1. Point out to students that according to a recent study and survey, 67.1 precent of responding organizations suffered malware infections.

Teaching Tip	You can point students to Figure 2-1 on page 55 to help them gain a better understanding of Internet usage around the world. Use Table 2-1 through Table 2-4 to help students understand the different categories of threats.

Common Attack Pattern Enumeration and Classification (CAPEC)

1. Introduce students to the CAPEC Web site which can be used by security professionals to understand attacks.

The 12 Categories of Threats

1. Use Table 2-5 to discuss the 12 general categories of threats that represent a clear and present danger to an organization's people, information, and systems.

Compromises to Intellectual Property

1. Explain that many organizations create or support the development of intellectual property (IP) as part of their business operations. Intellectual property is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas."

2. Mention that intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents. Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information. Most common IP breaches involve the unlawful use or duplication of software-based intellectual property, known as software piracy.

Software Piracy

1. Note that in addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: Software & Information Industry Association (SIIA), formerly the Software Publishers Association, and the Business Software Alliance (BSA).

Copyright Protection and User Registration

1. Discuss that enforcement of copyright laws has been attempted through a number of technical security mechanisms, such as digital watermarks, embedded code, and copyright codes.

Deviations in Quality of Service

1. Explain that this category represents situations in which a product or service is not delivered to the organization as expected.

2. Explain that the 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.

Internet Service Issues

1. Point out that Internet service, communications, and power irregularities are three sets of service issues that dramatically affect the availability of information and systems.

2. Describe Internet service issues: for organizations that rely heavily on the Internet and the 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 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 the hardware and operating system software used to operate the Web site.

Communications and Other Service Provider Issues

1. Describe communications and other service provider issues: other utility services can impact 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 properly.

Power Irregularities

1. Describe power irregularities: irregularities from power utilities are common and can lead to fluctuations, such as power excesses, power shortages, and power losses. In the U.S., we are "fed" 120-volt, 60-cycle power usually through 15 and 20 amp circuits.

2. Explain that voltage levels can **spike** (momentary increase), **surge** (prolonged increase), **sag** (momentary decrease), **brownout (**prolonged drop in voltage), **fault** (momentary complete loss of power) or **blackout** (a more lengthy loss of power).

3. Note that because sensitive electronic equipment—especially networking equipment, computers, and computer-based systems—are susceptible to fluctuations, controls should be applied to manage power quality.

Espionage or Trespass

1. Explain that this threat represents a well-known and broad category of electronic and human activities that breach the confidentiality of information.

2. Explain that when an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of espionage or trespass.

3. Point out that some information-gathering techniques are legal and are called competitive intelligence.

4. Note that instances of shoulder surfing occur at computer terminals, desks, ATM machines, smartphones, or other places where a person is accessing confidential information.

Hackers

1. Discuss that the act of trespassing can lead to unauthorized, real, or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

2. Discuss that the classic perpetrator of deliberate acts of espionage or trespass is the hacker. In the gritty world of reality, a hacker uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else. The hacker frequently spends long hours examining the types and structures of the targeted systems.

3. Remind students that there are generally two skill levels among hackers. The first is the expert hacker, who develops software scripts and program exploits used by the second category, the novice, or unskilled hacker.

4. Explain that 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.

5. Point out to students that expert hackers have become bored with directly attacking systems and have turned to writing software. The software they write are automated exploits that allow novice hackers to become script kiddies (or packet monkeys)—hackers of limited skill who use expertly written software to exploit a system, but do not fully understand or appreciate the systems they hack.

6. Discuss the term privilege escalation. Explain that a common example of privilege escalation is called jailbreaking or rooting.

Hacker Variants

1. Explain that there are other terms for system rule breakers:
    - The term **cracker** is now commonly associated with an individual who “cracks” or removes software protection that is designed to prevent unauthorized duplication.
    - A **phreaker** hacks the public telephone network to make free calls, disrupt services, and generally wreak havoc.

Password Attacks

1. Explain that password attacks fall under the category of espionage. Point out that attempting to guess or calculate a password is often called cracking.

2. Discuss the four approaches to password cracking:
   - Brute force
   - Dictionary attacks
   - Rainbow tables
   - Social engineering password attacks

Forces of Nature

1. Discuss how forces of nature, *force majeure*, or acts of God pose some of the most dangerous threats, because they are unexpected and can occur with very little warning.

2. Explain that these threats can disrupt not only the lives of individuals, but also the storage, transmission, and use of information. Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations.

3. Discuss the following examples of force of nature threats:
   a. Fire
   b. Flood
   c. Earthquake
   d. Lightning
   e. Landslides or mudslides
   f. Tornados or severe windstorms
   g. Hurricanes, typhoons, and tropical depressions
   h. Tsunamis
   i. Electrostatic discharge (ESD)
   j. Dust contamination
   k. Solar activity

Human Error or Failure

1. Describe this category and note that includes the possibility of acts performed without intent or malicious purpose by an individual who is an employee of an organization.

2. Discuss the fact that employees constitute one of the greatest threats to information security, as they are the individuals closest to the organizational data. 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.

3. Note that many threats can be prevented 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.

Teaching Tip	Systems fail for a variety of reasons, but proper procedures that ensure the ability to recover to a known good state. The most important aspect of any information security program is to ensure that the organization has a comprehensive continuity planning process.

Social Engineering

1. Note that within the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

2. Explain that people are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices...and somebody can call an unsuspecting employee and obtain a wealth of information.

3. Discuss the social engineering attack known as the advance-fee fraud (AFF).

4. Explain that phishing is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.

5. Note that a variant is spear phishing, a label that applies to any highly targeted phishing attack. While normal phishing attacks target as many recipients as possible, a spear phisher sends a message that appears to be from an employer, a colleague, or other legitimate correspondent, to a small group, or even one specific person.

6. Discuss that phishing attacks use two primary techniques, often used in combination with one another: URL manipulation and Web site forgery.

7. Point out another form of social engineering is called pretexting, which is sometimes referred to as phone phishing.

Information Extortion

1. Describe how the threat of information extortion involves the possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement to not disclose the information. Extortion is common in credit card number theft.

2. Explain that the latest type of attack in this category is known as ransomware, which is a malware attack on the host system that denies access to the user and then offers to provide a key to allow access back to the user's system and data for a fee.

Sabotage or Vandalism

1. Note that equally popular today is the assault on an organization's Web site. 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.

2. Emphasize that these threats can range from petty vandalism by employees to organized sabotage against an organization.

Online Activism

1. Explain that organizations frequently rely on image to support the generation of revenue, and vandalism to a Web site can erode consumer confidence, thus reducing the organization's sales and net worth. Compared to Web site defacement, vandalism within a network is more malicious in intent and less public.

2. Explain that security experts are noticing a rise in another form of online vandalism, **hacktivist** or **cyberactivist** operations. A more extreme version is referred to as **cyberterrorism**.

3. Compare cyberterrorism to more positive online activism, such as using Facebook, Twitter, etc. to perform fundraising and raise awareness of social issues.

Quick Quiz 1

1. True or False: The three communities of interest are general management, operations management, and information security management.
   Answer: False

2. Hackers of limited skill who use expertly written software to attack a system are known as which of the following?
   a. cyberterrorists
   b. script kiddies
   c. jailbreakers
   d. social engineers
   Answer: B

3. Which of the following 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?
   a. Information extortion
   b. Technological extortion
   c. Insider trading
   d. Information hording
   Answer: A

4. Which type of attacker will hack systems to conduct terrorist activities via network or Internet pathways?

a. Cyberhackers
b. Electronic terrorists
c. Cyberterrorists
d. Electronic hackers

Answer: C

5. True or False: Cyberterrorism has thus far been largely limited to acts such as the defacement of NATO Web pages during the war in Kosovo.
   Answer: True

Software Attacks

1. Emphasize that an attack is a deliberate act that exploits a vulnerability to compromise a controlled system. This attack can consist of specially crafted software that attackers trick users into installing on their systems.

Teaching Tip	You should pause now to ensure that students understand the difference between threats, vulnerabilities, exploits, and attacks. Verify that students understand how these terms combine and transition.

Malware

1. Describe malware as malicious code or malicious software. Point out that other attacks that use software, like redirect attacks and denial-of-service attacks, also fall under this threat.

2. Note that the malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

3. Explain that the polymorphic, or multivector, worm is a state-of-the-art attack system. Point out that these attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

4. Point out to students that when an attack makes use of malware that is not yet known by the anti-malware software companies, it is said to be a zero-day attack.

5. Describe other forms of malware including covert software applications—bots, spyware, and adware—that are designed to work out of sight of users, or via an apparently innocuous user action. Use Table 2-7 to review some of the most dangerous malware attacks to date.

Virus

1. Explain that a computer virus consists of code segments that perform malicious actions. Point out to students that one of the most common methods of virus transmission is via e-mail attachments.

2. Mention that viruses can be classified by how they spread themselves. Discuss the most common types of information system viruses, which are the macro virus and the boot virus.

3. Explain the classification known as memory-resident and non-memory-resident viruses. Note that resident viruses are capable of reactivating when the computer is booted and continuing their actions until the system is shut down.

Worms

1. Describe worms as viruses that can continue replicating themselves until they completely fill available resources. Use Figure 2-15 to discuss the Nimda and Sircam worms.

Trojan Horses

1. Explain that Trojan horses are frequently disguised as helpful or necessary pieces of software, such as the readme.exe files often includes with shareware or freeware. Use Figure 2-17 in your discussion.

Polymorphic Threats

1. Explain that a polymorphic threat evolves and changes size and other external file characteristics in order to elude detection by antivirus software programs.

Virus and Worm Hoaxes

1. Explain that a more devious approach to attacking computer systems is the transmission of a virus hoax. Discuss how these types of hoaxes waste user's time and cause networks to overload.

Back Doors

1. Discuss how using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Point out that these doors are often referred to as a maintenance hook.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

1. Explain that a denial-of-service attack begins when an attacker sends a large number of connection or information requests to a target. So many requests are made that the target system cannot handle them successfully along with other legitimate requests for service. This may result in the system crashing or simply becoming unable to perform ordinary functions.

2. Define a distributed denial-of-service attack as one in which a coordinated stream of requests is launched against a target from many locations at the same time.

3. Explain how compromised machines are turned into bots or zombies which can be directed remotely by the attacker in order to participate in the attack.

E-mail Attacks

1. Note that spam is unsolicited commercial e-mail. While many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks.

2. Explain that mail bombing is another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target.

Communications Interception Attacks

1. Explain that common software-based communications attacks include several subcategories designed to intercept and collect information in transit. Point out to students that the emergence of the Internet of Things (IoT) increases the possibility of these types of attacks.

Packet Sniffer

1. Describe a sniffer as a program or a device that can monitor data traveling over a network. It can be used both for legitimate network management functions and for stealing information from a network.

Spoofing

1. Emphasize that spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages to a computer containing an IP address that indicates that the messages are coming from a trusted host.

Pharming

1. Explain that pharming is “the redirection of legitimate Web traffic to an illegitimate site for the purpose of obtaining private information.”

2. Note that pharming may also exploit the Domain Name Server (DNS) by causing it to transform the legitimate host name into the invalid site’s IP address. This form of pharming is also known as “DNS cache poisoning.”

Man-in-the-Middle

1. Explain that an attacker sniffs packets from the network, modifies them, and inserts them back into the network. Point out that in a **TCP hijacking attack,** the attacker uses address spoofing to impersonate other legitimate entities on the network. Mention that this is also known as session hijacking.

Teaching Tip	Many students will find this the most interesting part of the chapter. Make sure you cover the ethical and legal implications of these attack descriptions.

Technical Hardware Failures or Errors

1. Emphasize that technical hardware failures or errors occur when a manufacturer distributes to users equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable or unavailable service.

2. Discuss that some errors are terminal in that they result in the unrecoverable loss of the equipment. Some errors are intermittent in that they only periodically manifest themselves, resulting in faults that are not easily repeated.

The Intel Pentium CPU Failure

1. Discuss the Intel Pentium II chip failure. Point out that it is one of the best-known hardware failures to date.

Mean Time Between Failure

1. Explain that in hardware terms, failures are measured in mean time between failure (MTBF) and mean time to failure (MTTF). Point out that MTBF and MTTF are sometimes used interchangeably.

Technical Software Failures or Errors

1. Explain that this category involves threats that come from purchasing software with unknown, hidden faults. Large quantities of computer code are written, debugged, published, and sold before all of their bugs are detected and resolved.

2. Discuss how combinations of certain software and hardware can reveal new bugs. Sometimes these items aren’t errors, but rather are purposeful shortcuts left by programmers for benign or malign reasons.

Teaching Tip	Explain that the most important aspect of a security program is the use of the organization's planning and policy development process. Planning is the foundation of information security empowering an organization to achieve and maintain a secure state. Consider reviewing NIST 800-100 (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf) for a discussion of the overall management process.

The OWASP Top 10

1. Discuss the Open Web Application Security Project (OWASP) that was founded in 2001 as a nonprofit consortium. Point out that every 3 years the group publishes a list of "The Ten Most Critical Web Application Security Risks".

The Deadly Sins in Software Security

1. Explain that some software development problems result in software that is difficult or impossible to deploy in a secure fashion. There are 24 problem areas or categories in software development (which is also called software engineering).

2. Describe buffer overruns, which are when buffers are used when there is a mismatch in the processing rates between two entities involved in a communication process. A buffer overrun (or buffer overflow) is an application error that occurs when more data is sent to a program buffer than it is designed to handle. During a buffer overrun, an attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

3. Explain that effective software has the ability to catch and resolve exceptions, which are unusual situations that require special processing.

4. Define command injection and explain that a command injection problems occur when user input is passed directly to a compiler or interpreter. The underlying issue is the developer's failure to ensure that command input is validated before it is used in the program.

5. Define cross-site scripting (XSS), which occurs when an application running on a Web server gathers data from a user in order to steal it. An attacker can use weaknesses of the Web server environment to insert commands into a user's browser session so that users ostensibly connected to a friendly Web server are, in fact, sending information to a hostile server.

6. Explain that failure to handle errors can cause a variety of unexpected system behaviors. Programmers are expected to anticipate problems and prepare their application code to handle them.

7. Describe the failure to protect network traffic and explain that with the growing popularity of wireless networking comes a corresponding increase in the risk that wirelessly transmitted data will be intercepted. Most wireless networks are installed and operated with little or no protection for the information that is broadcast between the client and the network wireless access point. Without appropriate encryption (such as that afforded by WPA), attackers can intercept and view your data. Traffic on a wired network is also vulnerable to interception in some situations.

8. Explain the failure to store and protect data securely. Programmers are responsible for integrating access controls into, and keeping secret information out of, programs. Access controls regulate who, what, when, where and how individuals and systems interact with data.

9. Discuss the failure to use cryptographically strong random numbers. Many computer systems use random number generators. These “random” number generators use a mathematical algorithm, based on a seed value and another system component (such as the computer clock) to simulate a random number. Those who understand the workings of such a “random” number generator can predict particular values at particular times.

10. Describe format string problems. Computer languages are often equipped with built-in capabilities to reformat data while they’re outputting it. The formatting instructions are usually written as a “format string.” An attacker may embed characters meaningful as formatting directives into malicious input. If this input is then interpreted by the program as formatting directives, the attacker may be able to access information or overwrite very targeted portions of the program’s stack with data of the attacker’s choosing.

11. Define improper file access. If attackers change the expected location of a file, by intercepting and modifying a program code call, they can force a program to use their own files rather than the files the program is supposed to use. The potential for damage or disclosure is extreme, so it is critical to protect the location of the files, as well as the method and communications channels by which these files are accessed.

12. Discuss the improper use of SSL. Programmers use Secure Socket Layer (SSL) to transfer sensitive data such as credit card numbers and other personal information between a client and server. SSL and its successor, Transport Layer Security (TLS), both need certificate validation to be truly secure. Failure to use secure HTTP, to validate the Certificate Authority and then validate the certificate itself, or to validate the information against a Certificate Revocation list (CRL), can compromise the security of SSL traffic.

13. Explain that information leakage is one of the most common methods of obtaining inside and classified information is directly or indirectly from an individual, usually an employee. By warning employees against disclosing information, organizations can protect the secrecy of their operation.

14. Discuss integer bugs (Overflows/Underflows). Although paper-and-pencil can deal with arbitrary numbers of digits, the binary representations used by computers are of a particular fixed length. “Integer bugs fall into four broad classes: overflows, underflows, truncations, and signedness errors. Integer bugs are usually exploited indirectly—that is, triggering an integer bug enables an attacker to corrupt other areas of memory, gaining control of an application.”

15. Explain the issue of neglecting change control. Developers use a process known as change control to ensure that the working system delivered to users represents the intent of the developers. Change control processes ensure that developers do not work at cross purposes by altering the same programs or parts of programs at the same time. They also ensure that only authorized changes are introduced and that all changes are adequately tested before being released.

16. Discuss the importance of integrating security and usability, adding training and awareness, and ensuring solid controls in order to contribute to the security of information.

17. Explain that a race condition is the failure of a program that occurs when an unexpected ordering of events in the execution of the program results in a conflict over access to the same system resource.

18. Describe SQL Injection. SQL injection occurs when developers fail to properly validate user input before using it to query a relational database. The possible effects of the ability to “inject” SQL of the attacker’s choosing into the program are not just limited to improper access to information, but could potentially allow an attacker to drop tables or even shut down the database.

19. Discuss trusting network address resolution.
    - The Domain Name Service (DNS) is a function of the World Wide Web that converts a URL into the IP address of the Web server host.
    - DNS cache poisoning involves compromising a DNS server and then changing the valid IP address associated with a domain name to one which the attacker chooses, usually a fake Web site designed to obtain personal information, or one that accrues some sort of benefit to the attacker—for example, redirecting shoppers from a competitor’s Web site.
    - Most DNS attacks are made against organizational primary and secondary domain name servers, local to the organization and part of the distributed DNS system. Other attacks attempt to compromise the DNS servers further up the DNS distribution mode—those of Internet Service Providers or backbone connectivity providers.
    - The DNS system relies on a process of automated updates that can be exploited. Attackers most commonly compromise segments of the DNS by either attacking the name of the name server and substituting their own DNS primary name server or by responding before an actual DNS can.

20. Explain unauthenticated key exchange, which is one of the biggest challenges in private key systems. Private key systems involve two users sharing the same key, is the need to get the key to the other party securely. An attacker can physically intercept a key in transit or intercept it digitally. Interception online can be accomplished by writing a variant of a public key system and placing it out as "freeware" or by corrupting or intercepting the function of someone else's public key encryption system, perhaps by posing as a public key repository.

21. Discuss the use of magic URLs and hidden forms.
    - Because HTTP is a stateless protocol and computer programs on either end of the communication channel cannot rely on guaranteed delivery of any message, it is difficult for software developers to track a user's exchanges with a Web site over multiple interactions.
    - Too often, sensitive state information is simply included in a "magic" URL (e.g., the authentication ID is passed as a parameter in the URL for the exchanges that will follow) or included in hidden form fields on the HTML page.
    - If this information is stored as plain text, an attacker can harvest the information from a magic URL as it travels across the network or use scripts on the client to modify information in hidden form fields.

22. Explain the use of weak password-based systems. Failure to require sufficient password strength and to control incorrect password entry is another severe security issue. Password policy can specify the number and type of characters, frequency of mandatory changes, and reusability of old passwords. The number of incorrect entries that can be submitted by a user can also be regulated to further improve the level of protection. The strength of a password directly impacts its ability to withstand a brute force attack. Using nonstandard password components (like the 8.3 rule—at least eight characters, with at least one letter, number and nonalphanumeric character) can greatly enhance the strength of the password.

23. Discuss Web client-related vulnerability (XSS). Client-side cross-site scripting errors can cause problems that allow an attacker to send malicious code to the user's computer by inserting the script into a normal Web site.

24. Mention to students that the same cross-site scripting attacks that can infect a client system can also be used to attack Web servers. Cross-site request forgery (XSRF or CSRF) attacks cause users to attack servers they access legitimately.

Teaching Tip	Technical vulnerabilities aside, the most secure systems cannot overcome the actions of users outside the system. Discuss with students how many times they have "worked around" limitations imposed by the security of systems.

Technological Obsolescence

1. Discuss how antiquated or outdated infrastructure leads to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

2. Explain that proper planning by management should prevent technology from becoming obsolete. However, when obsolescence is identified, management must take immediate action.

Theft

1. Define theft as the illegal taking of another's property. Within an organization, that property can be physical, electronic or intellectual.

2. Discuss how physical theft can be controlled quite easily. Many measures can be taken, including locking doors, training security personnel, and installing alarm systems.

3. Explain that electronic theft, however, is a more complex problem to manage and control. Organizations may not even know it has occurred.

Quick Quiz 2

1. True or False: Warnings of attacks that are not valid are usually called hoaxes.
   Answer: True

2. Using a known or previously installed access mechanism is known as which of the following?
   a. hidden bomb
   b. vector
   c. spoof
   d. back door

   Answer: D

3. True or False: When a program tries to reverse-calculate passwords, this is known as a brute force spoof.
   Answer: False

4. What is another name for a man-in-the-middle attack?
   a. TCP hijacking
   b. mail bombing
   c. spoofing
   d. denial of service

   Answer: A

5. Which of the following is an application error that occurs when more data is sent to a program buffer than it is designed to handle?
   a. buffer underrun
   b. buffer overrun
   c. heap overflow
   d. heap attack

   Answer: B

6. What can occur when developers fail to properly validate user input before using it to query a relational database?
   Answer: SQL injection

7. True or False: The Domain Name System (DNS) is a function of the World Wide Web that converts a URL (Uniform Resource Locator) like www.course.com into the IP address of the Web server host.
   Answer: True

Class Discussion Topics

1. What is the difference between a threat and an attack?

2. How do exploits relate to vulnerabilities?

3. Is there an ethically acceptable reason to study and use the various attack methods described in this chapter?

Additional Projects

1. Using the Internet, browse www.cert.org and find the most recent CERT advisory. Have students report on any recent vulnerabilities posted on the site.

2. Using the Internet, find and read the SANS/FBI Top 20 Vulnerabilities. Assign each student one of the 20 vulnerabilities listed and have them identify the threat group and threat category it warns about.

Additional Resources

1. Cross-site scripting FAQ
   http://www.cgisecurity.com/xss-faq.html

2. Governing for Enterprise Security Implementation Guide
   http://www.cert.org/governance/ges-xteam.html

3. Build Security In: Secure Software Development Lifecycle
   https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/326-BSI.html

4. Build Security In: Making the Case for Software Assurance
https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/685-BSI.html

5. Verizon Data Breach Investigations Report (2016)
www.verizonenterprise.com/verizon-insights-lab/dbir/2016

Key Terms

- **10.4 password rule:** an industry recommendation for password structure and strength that specifies passwords should be at least 10 characters long and contain at least one uppercase letter, one lowercase letter, one number, and one special character
- **Advance-fee fraud (AFF):** a form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer.
- **Adware:** malware intended to provided undesired marketing and advertising, including popups and banners on a user's screen.
- **Attack:** an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
- **Availability disruption:** an interruption of service, usually from a service provider, which causes an adverse event within an organization.
- **Back door:** a malware payload that provides access to a system by bypassing normal access controls.
- **Blackout:** a long-term interruption (outrage) in electrical power availability.
- **Boot virus:** also known as a boot sector virus, a type of virus that targets the boot sector or Master Boot Record (MBR) of a computer system's hard drive or removable storage media.
- **Bot:** an abbreviation of robot; an automated software program that executes certain commands when it receives a specific input. *See also Zombie*.
- **Brownout:** a long-term decrease in electrical power availability.
- **Brute force password attack:** an attempt to guess a password by attempting every possible combination of characters and numbers in it.
- **Buffer overrun (or buffer overflow):** an application error that occurs when more data is sent to a program buffer than it is designed to handle.
- **Command injection:** an application error that occurs when user input is passed directly to a compiler or interpreter without screening for content that may disrupt or compromise the intended function.
- **Competitive intelligence:** the collection and analysis of information about an organization's business competitors through legal and ethical means to gain business intelligence and competitive advantage.
- **Cracker:** a hacker who intentionally removes or bypasses software copyright protection designed to prevent unauthorized duplication or use.
- **Cracking:** attempting to reverse-engineer, remove, or bypass a password or other access control protection, such as the copyright protection on software. *See Cracker*.

- **Cross site scripting (XSS):** a web application fault that occurs when an application running on a Web server inserts commands into a user's browser session and causes information to be sent to a hostile server.
- **Cyberactivist:** see *Hacktivist*.
- **Cyberterrorist:** a hacker who attacks systems to conduct terrorist activities via networks or internet pathways.
- **Cyberwarfare:** formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state.
- **Data**: items of fact collected by an organization.
- **Data security:** commonly used as a surrogate for information security, data security is the focus of protecting data or information in its various states-at rest (in storage), in processing, and in transmission (over networks).
- **Database:** a collection of related data stored in a structured form and usually managed by a database management system.
- **Database security:** a subset of information security that focuses on the assessment and protection of information stored in data repositories like database management systems and storage media.
- **Denial-of-service (DoS) attack:** an attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.
- **Dictionary password attack:** a variation of the brute force attack that attempts to narrow the range of possible passwords guessed by using a list of common passwords and possibly including attempts based on the target's personal information.
- **Distributed denial-of-service (DDoS):** a form of DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.
- **Domain Name System (DNS) cache poisoning:** the intentional hacking and modification of a DNS database to redirect legitimate traffic to illegitimate Internet locations.
- **Downtime:** the percentage of time a particular service is not available; the opposite of uptime.
- **Expert hacker:** a hacker who uses extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information.
- **Exploit:** a technique used to compromise a system.
- **Fault:** a short-term interruption in electrical power availability.
- **Hacker:** a person who accesses systems and information without authorization and often illegally.
- **Hacktivist:** a hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.
- **Information:** data that has been organized, structured, and presented to provide additional insight into its context, worth, and usefulness.
- **Information asset:** the focus of information security; information that has value to the organization, and the systems that store, process, and transmit the information.
- **Information extortion:** the act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

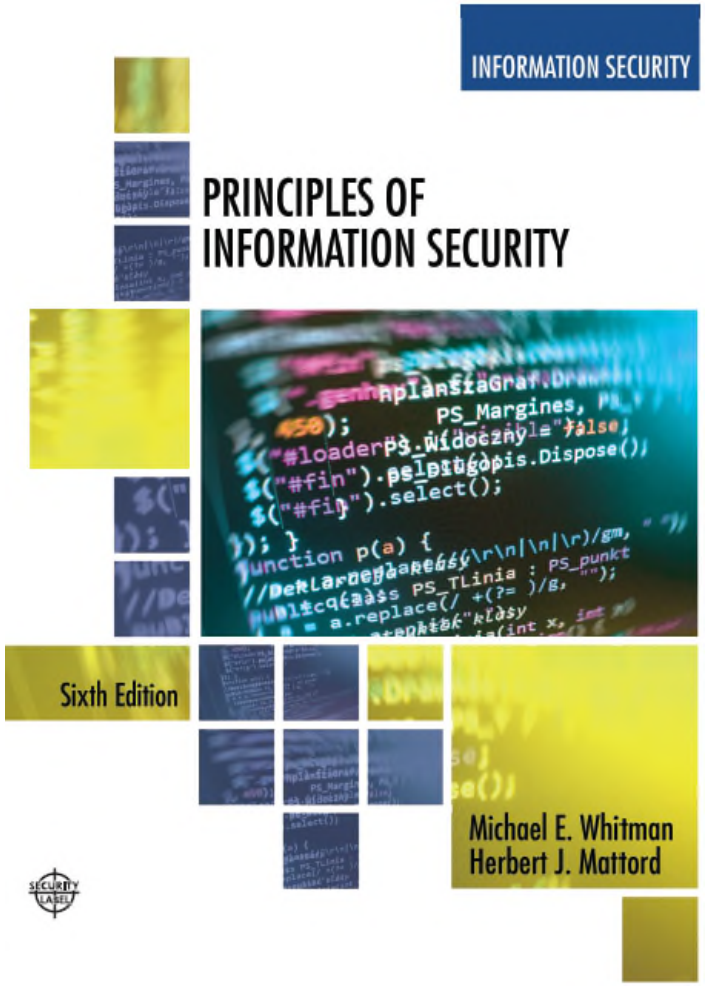
- **Industrial espionage:** the collection and analysis of information about an organization's business competitors, often through illegal or unethical means, to gain an unfair competitive advantage.
- **Integer bug:** a class of computational error caused by methods that computers use to store and manipulate integer numbers; this bug can be exploited by attackers.
- **Intellectual property(IP):** the creation, ownership, and control of original ideas as well as the representation of those ideas.
- **Jailbreaking:** escalating privileges to gain administrator-level control over a smartphone operating system (typically associated with Apple iOS smartphones). *See also Rooting.*
- **Macro virus:** a type of virus written in a specific macro language to target applications that use the language.
- **Mail bomb:** an attack designed to overwhelm the receiver with excessive quantities of email.
- **Maintenance hook:** *see Back door*
- **Malicious code:** *see Malware.*
- **Malicious software:** *see Malware.*
- **Malware:** computer software specifically designed to perform malicious or unwanted actions.
- **Man-in-the-middle:** a group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that he is the other communications partner.
- **Media:** as a subset of information assets, the systems and network that store, process, and transmit information.
- **Mean time between failure (MTBF):** the average amount of time between hardware failures, calculated as the total amount of operation time for a specified number of units divided by the total number of failures.
- **Mean time to diagnose (MTTD):** the average amount of time a computer technician needs to determine the cause of a failure.
- **Mean time to failure (MTTF):** the average amount of time until the next hardware failure.
- **Mean time to repair (MTTR):** the average amount of time a computer technician needs to resolve the cause of a failure through replacement or repair of a faulty unit.
- **Memory-resident virus:** a virus that is capable of installing itself in a computer's operating system, starting when the computer is activated, and residing in the system's memory even after the host application is terminated.
- **Noise:** the presence of additional and disruptive signals in network communications or electrical power delivery.
- **Non-memory-resident virus:** a virus that terminates after it has been activated, infected its host system, and replicated itself.
- **Novice hacker:** a relatively unskilled hacker who uses the work of expert hackers to perform attacks.
- **Packet monkey:** a script kiddie who uses automated exploits to engage in denial-of-service attacks.
- **Packet sniffer:** a software program or hardware appliance that can intercept, copy, and interpret network traffic.
- **Penetration tester:** an information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

- **Pharming**: the redirection of legitimate Web to illegitimate Web sites with the intent to collect personal information.
- **Phishing:** a form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.
- **Phreaker:** a hacker who manipulates the public telephone system to make free calls or disrupt services.
- **Polymorphic threat:** malware that over time changes the way it appears to antivirus programs, making it undetectable by techniques that look for preconfigured signatures.
- **Pretexting:** a form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information.
- **Privilege escalation**: the unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.
- **Professional hacker:** a hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government.
- **Rainbow table:** a table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.
- **Ransomware:** computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption.
- **Rooting:** escalating privileges to gain administrator-level control over a computer system (including smartphones).
- **Sag:** a short-term decrease in electrical power availability.
- **Script kiddie:** a hacker of limited skill who use expertly written software to attack a system.
- **Service Level Agreement (SLA):** a document or part of a document that specifies the expected level of service from a service provider.
- **Session hijacking:** *See TCP hijacking*.
- **Shoulder surfing:** the direct, covert observation of individual information or system use.
- **Sniffer:** *see Packet sniffer*.
- **Social engineering:** the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- **Software piracy:** the unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.
- **Spam:** undesired e-mail, typically commercial advertising transmitted in bulk.
- **Spear phishing:** a highly targeted phishing attack.
- **Spike:** a short-term increase in electrical power availability, also known as a swell.
- **Spoofing:** a technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.
- **Spyware:** any technology that aids in gathering information about a person or organization without their knowledge.
- **Surge:** a long-term increase in electrical power availability.
- **TCP hijacking:** a form of man-in-the-middle attack whereby the attacker inserts himself into TCP/IP-based communications.

- **Theft:** the illegal taking of another's property, which can be physical, electronic, or intellectual.
- **Trap door:** *see Back door*.
- **Trespass:** unauthorized entry into the real or virtual property of another party.
- **Trojan horses:** a malware program that hides its true nature and reveals its designed behavior only when activated.
- **Uptime:** the percentage of time a particular service is available; the opposite of downtime.
- **Virus:** a type of malware that is attached to other executable programs.
- **Vulnerability:** a potential weakness in an asset or its defensive control system(s).
- **Virus hoax:** a message that reports the presence of a nonexistent virus or worm and wastes valuable time as employees share the message.
- **Worm:** a type of malware that is capable of activation and replication without being attached to an existing program.
- **zero-day attack:** an attack that makes use of malware that is not yet known by the anti-malware software companies.
- **Zombie:** *see Bot.*

Principles of Information Security

Sixth Edition



Chapter 2

The Need for Security

Learning Objectives

- Upon completion of this material, you should be able to:
  - Discuss the organizational need for information security
  - Explain why a successful information security program is the shared responsibility of an organization's three communities of interest
  - List and describe the threats posed to information security and common attacks associated with those threats
  - List the common development failures and errors that result from poor software security efforts

Introduction

- The primary mission of an information security program is to ensure information assets—information and the systems that house them—remain safe and useful.
- If no threats existed, resources could be used exclusively to improve systems that contain, use, and transmit information.
- Threat of attacks on information systems is a constant concern.

Business Needs First

- Information security performs four important functions for an organization:
  - Protecting the organization's ability to function
  - Protecting the data and information the organization collects and uses
  - Enabling the safe operation of applications running on the organization's IT systems
  - Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

- Management (general and IT) is responsible for facilitating security program.
- Implementing information security has more to do with management than technology.
- Communities of interest should address information security in terms of business impact and cost of business interruption.

Protecting Data That Organizations Collect and Use

- Without data, an organization loses its record of transactions and ability to deliver value to customers.
- Protecting data in transmission, in processing, and at rest (storage) is a critical aspect of information security.

Enabling the Safe Operation of Applications

- Organization needs environments that safeguard applications using IT systems.
- Management must continue to oversee infrastructure once in place—not relegate to IT department.

Safeguarding Technology Assets in Organizations

- Organizations must employ secure infrastructure hardware appropriate to the size and scope of the enterprise.
- Additional security services may be needed as the organization grows.
- More robust solutions should replace security programs the organization has outgrown.

Threats and Attacks

- Threat: a potential risk to an asset's loss of value.
- Attack: An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
- Exploit: A technique used to compromise a system.
- Vulnerability: A potential weakness in an asset or its defensive control system(s).
- Management must be informed about the various threats to an organization's people, applications, data, and information systems.
- Overall security is improving, but so is the number of potential hackers.

Figure 2-1 World Internet usage

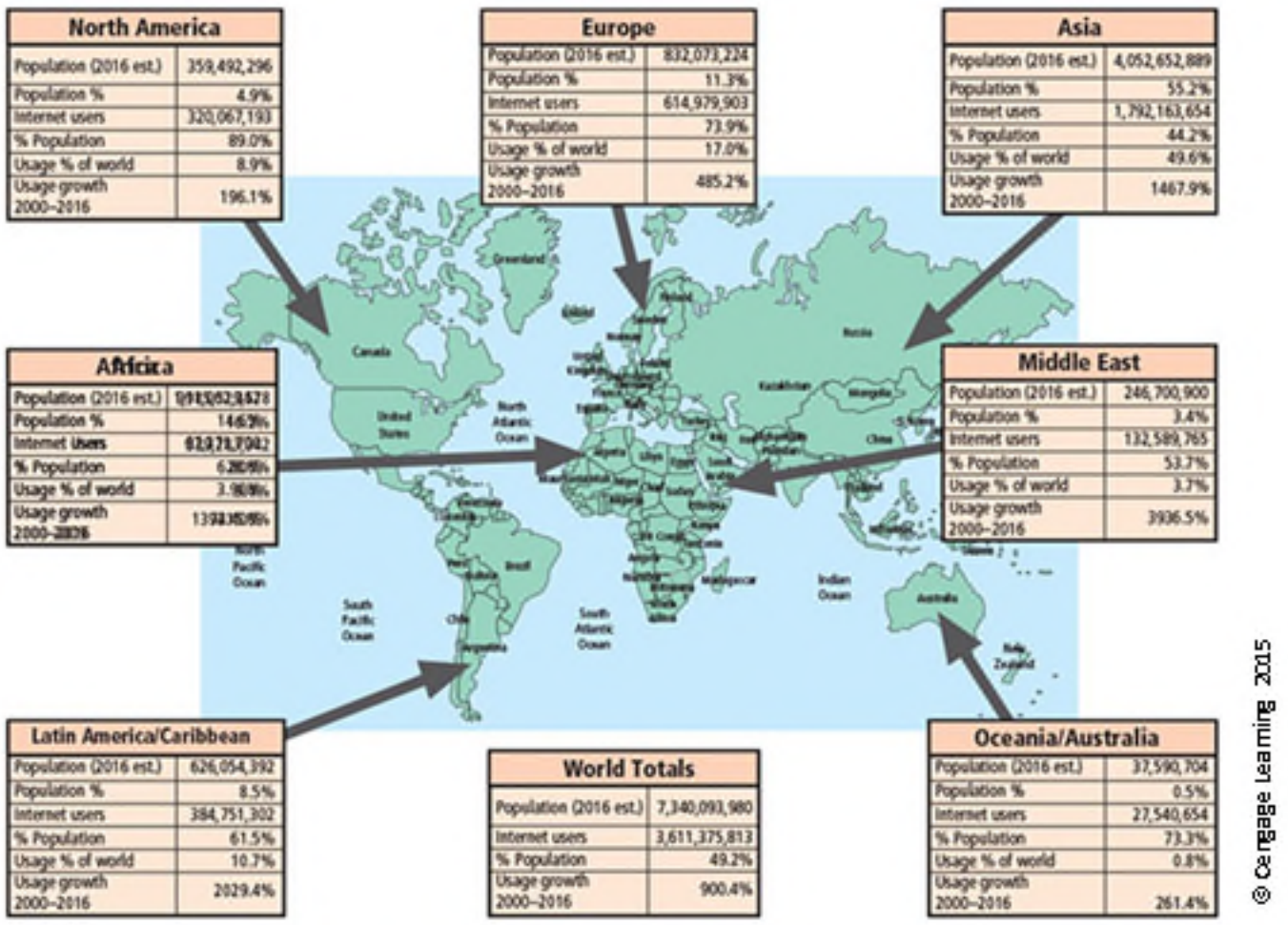


Table 2-1 Compiled Survey Results for Types of Attack or Misuse (2000-2011) (1 of 2)

Type of Attack or Misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)	(new category)		
Laptop/ mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)	(new category)		
Inside abuse of internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial of service	17%	21%	25%	39%	40%	27%

Table 2-1 Compiled Survey Results for Types of Attack or Misuse (2000-2011) (2 of 2)

Type of Attack or Misuse	2010/11	2008	2006	2004	2002	2000
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)	(revised category)		
Password sniffing	11%	9%	(new category)	(new category)		
System penetration by outsider	11%		(revised category)	(revised category)		
Exploit of client web browser	10%		(new category)	(new category)		

Source: Whitman and Mattord, 2015 SEC/CISE Threats to Information Protection Report.

Table 2-2 Rated Threats from Internal Sources in 2015 SEC/CISE Survey of Threads to Information Protection (1 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Inability/unwillingness to follow established policy	6.6%	17.2%	33.6%	26.2%	16.4%	66%
Disclosure due to insufficient training	8.1%	23.6%	29.3%	25.2%	13.8%	63%
Unauthorized access or escalation of privileges	4.8%	24.0%	31.2%	31.2%	8.8%	63%
Unauthorized information collection/data sniffing	6.4%	26.4%	40.0%	17.6%	9.6%	60%
Theft of on-site organizational information assets	10.6%	32.5%	34.1%	12.2%	10.6%	56%
Theft of mobile/laptop/tablet and related/connected information assets	15.4%	29.3%	28.5%	17.9%	8.9%	55%
Intentional damage or destruction of information assets	22.3%	43.0%	18.2%	13.2%	3.3%	46%

Table 2-2 Rated Threats from Internal Sources in 2015 SEC/CISE Survey of Threads to Information Protection (2 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Theft or misuse of organizationally leased, purchased, or developed software	29.6%	33.6%	21.6%	10.4%	4.8%	45%
Web site defacement	43.4%	33.6%	16.4%	4.9%	1.6%	38%
Blackmail of information release or sales	43.5%	37.1%	10.5%	6.5%	2.4%	37%

Table 2-3 Rated Threats from External Sources in 2015 SEC/CISE Survey of Threads to Information Protection (1 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Unauthorized information collection/data sniffing	6.4%	14.4%	21.6%	32.8%	24.8%	71%
Unauthorized access or escalation of privileges	7.4%	14.0%	26.4%	31.4%	20.7%	69%
Web site defacement	8.9%	23.6%	22.8%	26.8%	17.9%	64%
Intentional damage or destruction of information assets	14.0%	32.2%	18.2%	24.8%	10.7%	57%
Theft of mobile/laptop/tablet and related/connected information assets	20.5%	25.4%	26.2%	15.6%	12.3%	55%
Theft of on-site organizational informational assets	21.1%	24.4%	25.2%	17.9%	11.4%	55%
Blackmail of information release or sales	31.1%	30.3%	14.8%	14.8%	9.0%	48%
Disclosure due to insufficient training	34.5%	21.8%	22.7%	13.4%	7.6%	48%

Table 2-3 Rated Threats from External Sources in 2015 SEC/CISE Survey of Threads to Information Protection (2 of 2)

From Employees or Internal Stakeholders	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Inability/unwillingness to follow established policy	33.6%	29.4%	18.5%	6.7%	11.8%	47%
Theft or misuse of organizationally leased, purchased, or developed software	31.7%	30.1%	22.8%	9.8%	5.7%	46%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (1 of 4)

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

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (2 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
SQL injections	7.6%	17.6%	31.9%	29.4%	13.4%	65%
Social engineering of employees/insiders based on organization's Web sites	11.4%	19.5%	23.6%	31.7%	13.8%	63%
Denial of service (and distributed DoS) attacks	8.2%	23.0%	27.9%	32.8%	8.2%	62%
Software failures or errors due to known vulnerabilities in externally acquired software	8.9%	23.6%	26.8%	35.8%	4.9%	61%
Outdated organizational software	8.1%	28.2%	26.6%	26.6%	10.5%	61%
Loss of trust due to representation as source of phishing/spoofing attack	9.8%	23.8%	30.3%	23.0%	13.1%	61%
Loss of trust due to Web defacement	12.4%	30.6%	31.4%	19.8%	5.8%	55%
Outdated organizational hardware	17.2%	34.4%	32.8%	12.3%	3.3%	50%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (3 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Outdated organizational data format	18.7%	35.8%	26.8%	13.8%	4.9%	50%
Inability/unwillingness to establish effective policy by management	30.4%	26.4%	24.0%	13.6%	5.6%	48%
Hardware failures or errors due to aging equipment	19.5%	39.8%	24.4%	14.6%	1.6%	48%
Hardware failures or errors due to defective equipment	17.9%	48.0%	24.4%	8.1%	1.6%	46%
Deviations in quality of service from other provider	25.2%	38.7%	25.2%	7.6%	3.4%	45%
Deviations in quality of service from data communications provider/ISP	26.4%	39.7%	23.1%	7.4%	3.3%	44%
Deviations in quality of service from telecommunication provider/ISP (if different from data provider)	29.9%	38.5%	18.8%	9.4%	3.4%	44%

Table 2-4 Perceived Threats to Information Assets in 2015 SEC/CISE Survey of Threats to Information Protection (4 of 4)

General Threats to Information Assets	Not a Threat 1	2	3	4	A Severe Threat 5	Comp. Rank
Loss due to other natural disaster	31.0%	37.9%	23.3%	6.9%	0.9%	42%
Loss due to fire	26.2%	49.2%	21.3%	3.3%	0.0%	40%
Deviations in quality of service from power provider	36.1%	43.4%	12.3%	5.7%	2.5%	39%
Loss due to flood	33.9%	43.8%	19.8%	1.7%	0.8%	38%
Loss due to earthquake	41.7%	35.8%	15.0%	6.7%	0.8%	38%

Table 2-5 The 12 Categories of Threats to Information Security

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in equality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes. lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Compromises to Intellectual Property

- Intellectual property (IP): creation, ownership, and control of original ideas as well as the representation of those ideas.
- The most common IP breaches involve software piracy.
- Two watchdog organizations investigate software abuse:
  - Software & Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- Enforcement of copyright law has been attempted with technical security mechanisms.

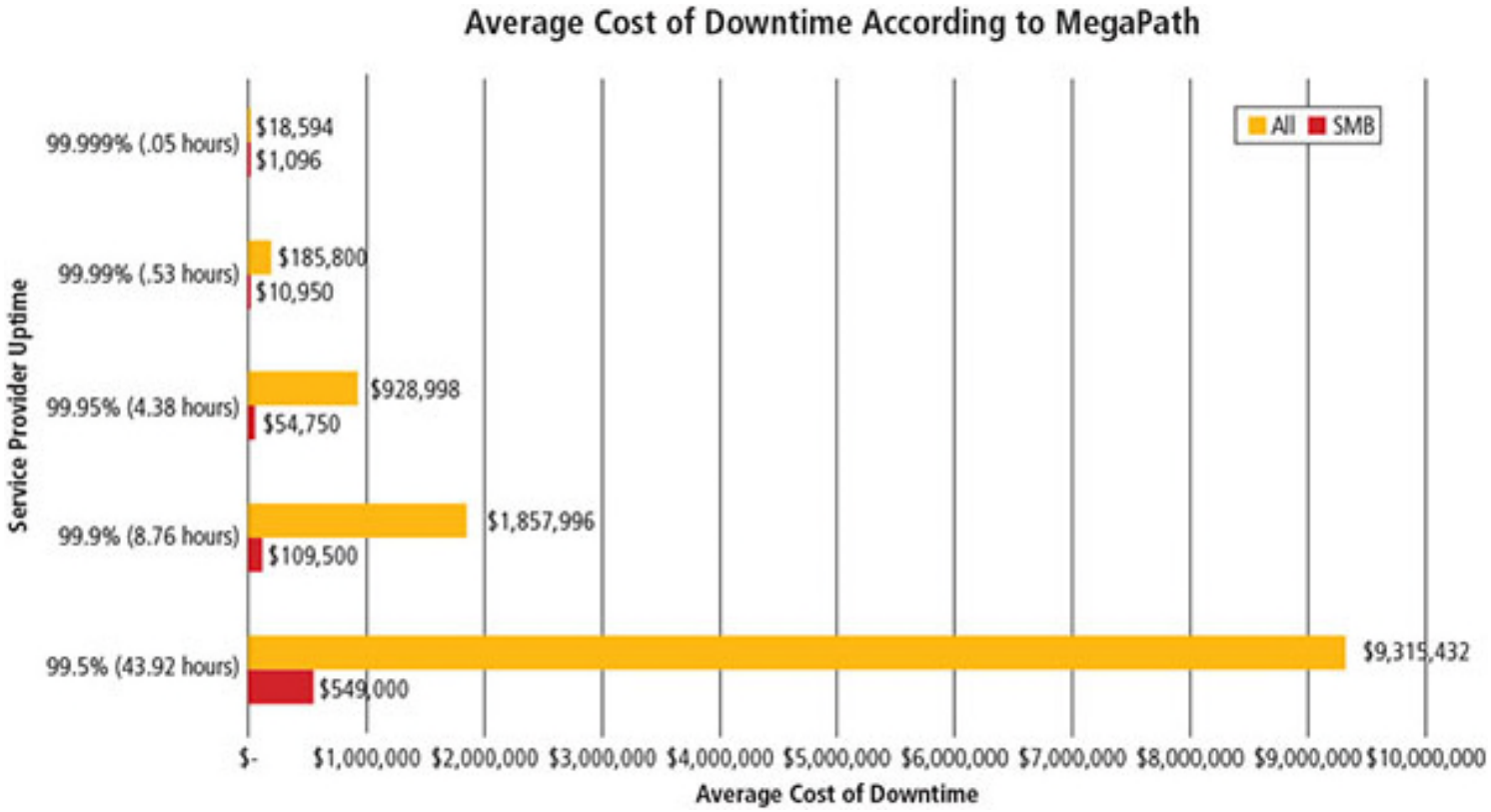
Deviations in Quality of Service (1 of 2)

- Information system depends on the successful operation of many interdependent support systems.
- Internet service, communications, and power irregularities dramatically affect the availability of information and systems.
- Internet service issues
  - Internet service provider (ISP) failures can considerably undermine the availability of information.
  - Outsourced Web hosting provider assumes responsibility for all Internet services as well as for the hardware and Web site operating system software.

Deviations in Quality of Service (2 of 2)

- Communications and other service provider issues
  - Other utility services affect organizations: telephone, water, wastewater, trash pickup.
  - Loss of these services can affect an organization's ability to function.
- Power irregularities
  - Are commonplace
  - Lead to fluctuations such as power excesses, power shortages, and power losses
  - Sensitive electronic equipment vulnerable to and easily damaged/destroyed by fluctuations
  - Controls can be applied to manage power quality

Figure 2-5 Cost of online service provider downtime



Source: MegaPath. Used with permission.

Espionage or Trespass (1 of 3)

- Access of protected information by unauthorized individuals
- Competitive intelligence (legal) versus industrial espionage (illegal)
- Shoulder surfing can occur anywhere a person accesses confidential information
- Controls let trespassers know they are encroaching on organization's cyberspace
- Hackers use skill, guile, or fraud to bypass controls protecting others' information

Espionage or Trespass (2 of 3)

- Expert hackers
  - Develop software scripts and program exploits
  - Usually a master of many skills
  - Will often create attack software and share with others
- Unskilled hackers
  - Many more unskilled hackers than expert hackers
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack

Espionage or Trespass (3 of 3)

- Other terms for system rule breakers:
  - Cracker: “cracks” or removes software protection designed to prevent unauthorized duplication
  - Phreaker: hacks the public telephone system to make free calls or disrupt services
- Password attacks
  - Cracking
  - Brute force
  - Dictionary
  - Rainbow tables
  - Social engineering

Figure 2-6 Shoulder surfing

Figure 2-7 Contemporary hacker profile

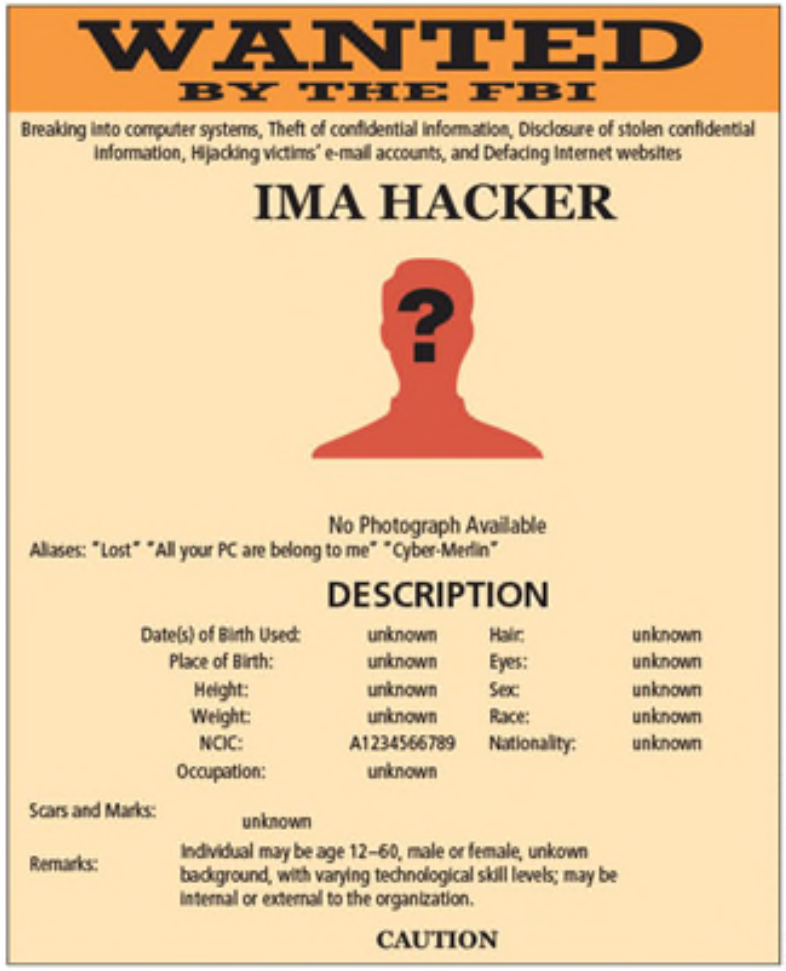


Table 2-6 Password Power (1 of 2)

Case-Insensitive Passwords Using a Standards Alphabet Set (No Numbers or Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	208,827,064,576	1.01 seconds
9	5,429,503,678,976	26.2 seconds
10	141,167,095,653,376	11.4 minutes
11	3,670,344,486,987,780	4.9 hours
12	95,428,956,661,682,200	5.3 days
13	2,481,152,873,203,740,000	138.6 days
14	64,509,974,703,297,200,000	9.9years
15	1,677,259,342,285,730,000,000	256.6 years
16	43,608,742,899,428,900,000,000	6,672.9 years

Table 2-6 Password Power (2 of 2)

Case-Sensitive Passwords Using a Standards Alphabet Set (with Numbers and Special Characters)		
Password Length	**Odd of cracking: 1 in (Based on Numbers of Characters ^ Password length):**	**Estimated Time to Crack***
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

*Estimated Time to crack is based on a 2015-era PC with an intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/ billion instructions per second) at 4.0 GHz.

Forces of Nature

- Forces of nature can present some of the most dangerous threats.
- They disrupt not only individual lives but also storage, transmission, and use of information.
- Organizations must implement controls to limit damage and prepare contingency plans for continued operations.

Human Error or Failure (1 of 2)

- Includes acts performed without malicious intent or in ignorance
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees are among the greatest threats to an organization's data

Human Error or Failure (2 of 2)

- Employee mistakes can easily lead to:
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information
- Many of these threats can be prevented with training, ongoing awareness activities, and controls
- Social engineering uses social skills to convince people to reveal access credentials or other valuable information to an attacker

Figure 2-9 The biggest threat—acts of human error or failure

Tommy Twostory,
convicted burglar

Harriett Allthumbs,
confused the copier with the shredder
when preparing the annual sales report

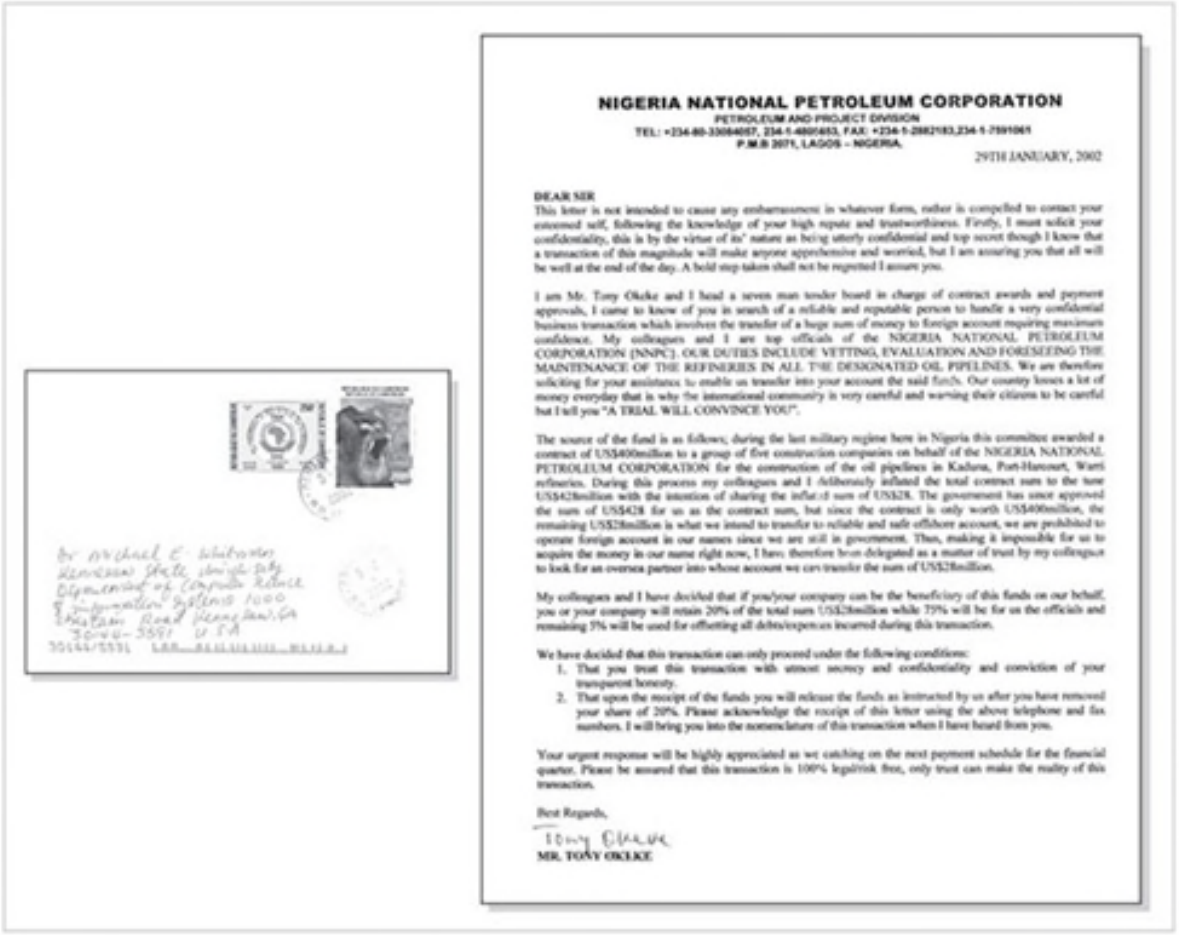
Elite Skillz,
wannabe hacker

Source: © iStockphoto/BartCo, © iStockphoto/sdominick, © iStockphoto/mikkelwilliam.

Social Engineering

- “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”—Kevin Mitnick
- Advance-fee fraud: indicates recipient is due money and small advance fee/personal banking information required to facilitate transfer
- Phishing: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site

Figure 2-10 Example of a Nigerian 4-1-9 fraud letter



NIGERIA NATIONAL PETROLEUM CORPORATION
PETROLEUM AND PROJECT DIVISION
TEL: +234-80-33084057, 234-1-4805453, FAX: +234-1-2682183,234-1-7591061
P.M.B 2071, LAGOS – NIGERIA.

29TH JANUARY, 2002

DEAR SIR
This letter is not intended to cause any embarrassment in whatever form, rather is compelled to contact your esteemed self, following the knowledge of your high repute and trustworthiness. Firstly, I must solicit your confidentiality, this is by the virtue of its' nature as being utterly confidential and top secret though I know that a transaction of this magnitude will make anyone apprehensive and worried, but I am assuring you that all will be well at the end of the day. A bold step taken shall not be regretted I assure you.

I am Mr. Tony Okeke and I head a seven man tender board in charge of contract awards and payment approvals, I came to know of you in search of a reliable and reputable person to handle a very confidential business transaction which involves the transfer of a huge sum of money to foreign account requiring maximum confidence. My colleagues and I are top officials of the NIGERIA NATIONAL PETROLEUM CORPORATION (NNPC). OUR DUTIES INCLUDE VETTING, EVALUATION AND FORESEEING THE MAINTENANCE OF THE REFINERIES IN ALL THE DESIGNATED OIL PIPELINES. We are therefore soliciting for your assistance to enable us transfer into your account the said funds. Our country looses a lot of money everyday that is why the international community is very careful and warning their citizens to be careful but I tell you "A TRIAL WILL CONVINCE YOU".

The source of the fund is as follows; during the last military regime here in Nigeria this committee awarded a contract of US$400million to a group of five construction companies on behalf of the NIGERIA NATIONAL PETROLEUM CORPORATION for the construction of the oil pipelines in Kaduna, Port-Harcourt, Warri refineries. During this process my colleagues and I deliberately inflated the total contract sum to the tune US$428million with the intention of sharing the inflated sum of US$28. The government has since approved the sum of US$428 for us as the contract sum, but since the contract is only worth US$400million, the remaining US$28million is what we intend to transfer to reliable and safe offshore account, we are prohibited to operate foreign account in our names since we are still in government. Thus, making it impossible for us to acquire the money in our name right now, I have therefore been delegated as a matter of trust by my colleagues to look for an oversea partner into whose account we can transfer the sum of US$28million.

My colleagues and I have decided that if you/your company can be the beneficiary of this funds on our behalf, you or your company will retain 20% of the total sum US$28million while 75% will be for us the officials and remaining 5% will be used for offsetting all debts/expenses incurred during this transaction.

We have decided that this transaction can only proceed under the following conditions:
1. That you treat this transaction with utmost secrecy and confidentiality and conviction of your transparent honesty.
2. That upon the receipt of the funds you will release the funds as instructed by us after you have removed your share of 20%. Please acknowledge the receipt of this letter using the above telephone and fax numbers. I will bring you into the nomenclature of this transaction when I have heard from you.

Your urgent response will be highly appreciated as we catching on the next payment schedule for the financial quarter. Please be assured that this transaction is 100% legal/risk free, only trust can make the reality of this transaction.

Best Regards,

MR. TONY OKEKE

Source: © iStockphoto/BartCo, © iStockphoto/sdominick, © iStockphoto/mikkelwilliam.

Figure 2-11 Phishing example: lure

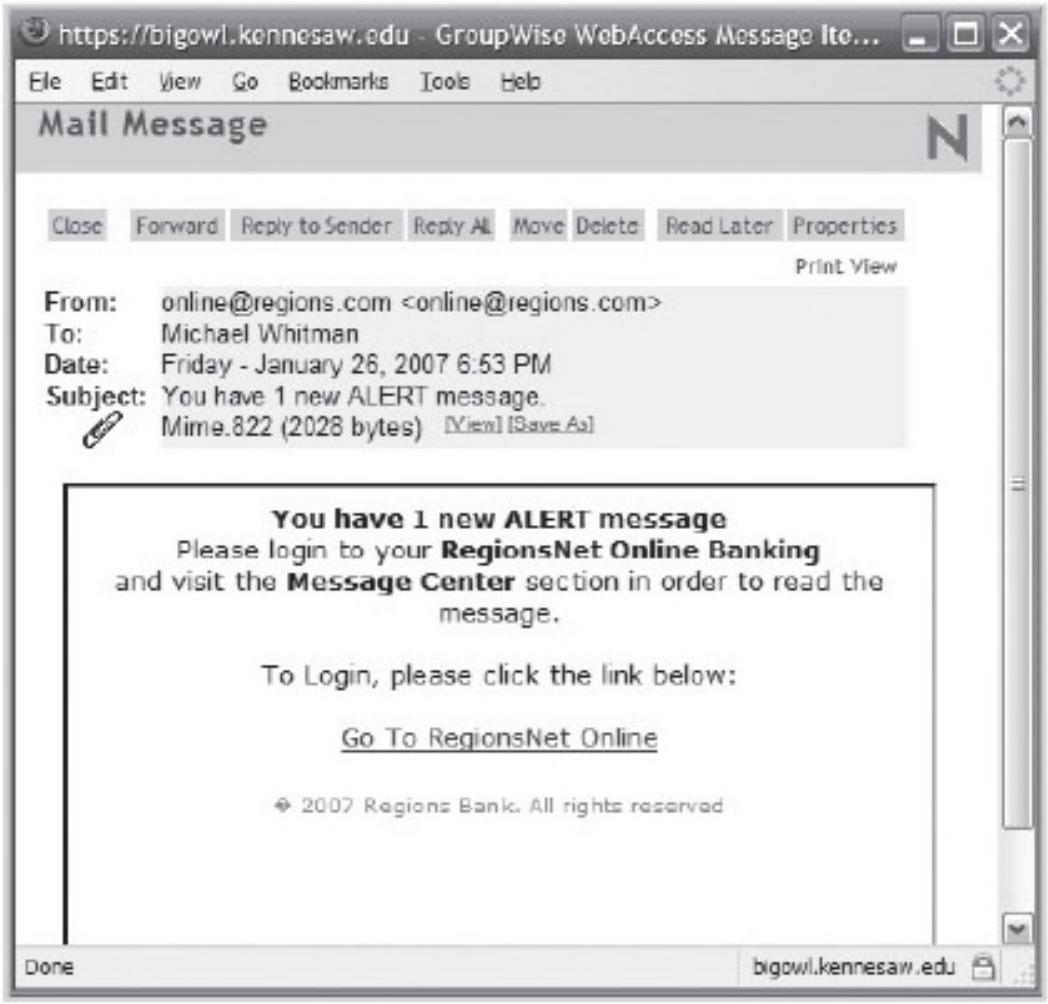
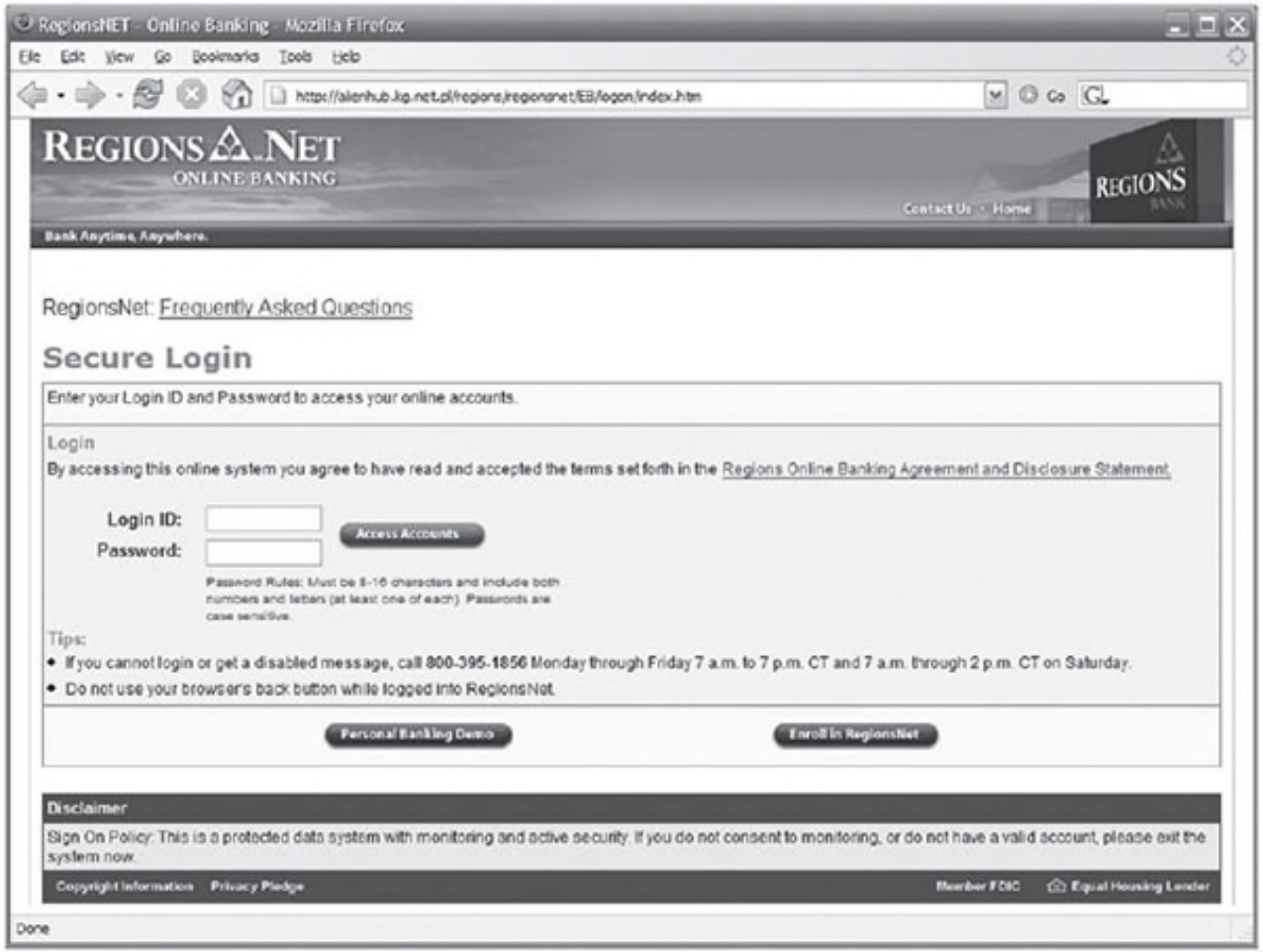


Figure 2-12 Phishing example: fake Website



Information Extortion

- Attacker steals information from a computer system and demands compensation for its return or nondisclosure. Also known as cyberextortion.
- Commonly done in credit card number theft

Sabotage or Vandalism

- Threats can range from petty vandalism to organized sabotage.
- Web site defacing can erode consumer confidence, diminishing organization's sales, net worth, and reputation.
- Threat of hacktivist or cyberactivist operations is rising.
- Cyberterrorism/Cyberwarfare: a much more sinister form of hacking.

Software Attacks (1 of 5)

- Malicious software (malware) is used to overwhelm the processing capabilities of online systems or to gain access to protected systems via hidden means.
- Software attacks occur when an individual or a group designs and deploys software to attack a system.

Software Attacks (2 of 5)

- Types of attacks include:
  - Malware (malicious code): It includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
    - Virus: It consists of code segments that attach to existing program and take control of access to the targeted computer.
    - Worms: They replicate themselves until they completely fill available resources such as memory and hard drive space.
    - Trojan horses: malware disguised as helpful, interesting, or necessary pieces of software.

Software Attacks (3 of 5)

- Polymorphic threat: actually evolves to elude detection
- Virus and worm hoaxes: nonexistent malware that employees waste time spreading awareness about

– Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism

– Denial-of-service (DoS): An attacker sends a large number of connection or information requests to a target.

- The target system becomes overloaded and cannot respond to legitimate requests for service.
- It may result in system crash or inability to perform ordinary functions.

Software Attacks (4 of 5)

- Distributed denial-of-service (DDoS): A coordinated stream of requests is launched against a target from many locations simultaneously.
- Mail bombing (also a DoS): An attacker routes large quantities of e-mail to target to overwhelm the receiver.
- Spam (unsolicited commercial e-mail): It is considered more a nuisance than an attack, though is emerging as a vector for some attacks.
- Packet sniffer: It monitors data traveling over network; it can be used both for legitimate management purposes and for stealing information from a network.

Software Attacks (5 of 5)

- Spoofing: A technique used to gain unauthorized access; intruder assumes a trusted IP address.
- Pharming: It attacks a browser's address bar to redirect users to an illegitimate site for the purpose of obtaining private information.
- Man-in-the-middle: An attacker monitors the network packets, modifies them, and inserts them back into the network.

Table 2-7 The Most Dangerous Malware Attacks to Date (1 of 2)

Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
MyDoom	Worm	2004	2 million	$ 38 billion
Klez (and variants)	Virus	2001	7.2% of Internet	$19.8 billion
ILOVEYOU	Virus	2000	10% of Internet	$ 5.5 billion
Sobig F	Worm	2003	1 million	$ 3 billion
Code Red (and CR II)	Worm	2001	400,000 servers	$ 2.6 billion
SQL slammer, a.k.a. Sapphire	Worm	2003	75,000	$ 950 million to $ 1.2 billion
Melissa	Macro virus	1999	Unknown	$ 300 million to $ 600 million
CIH, a.k.a. Chernobyl	Memory-resident virus	1998	Unknown	$ 250 million
Storm Worm	Trojan horse virus	2006	10 million	Unknown

Table 2-7 The Most Dangerous Malware Attacks to Date (2 of 2)

Malware	Type	Year	Estimated Number of Systems Infected	Estimated Financial Damage
Conficker	Worm	2009	15 million	Unknown
Nimda	Multivector worm	2001	Unknown	Unknown
Sasser	Worm	2004	500,000 to 700,000	Unknown
Nesky	Virus	2004	Under 100,000	Unknown
Leap-A/Oompa-A	Virus	2006	Unknown (Apple)	Unknown

Table 2-8 Attack Replication Vectors

Vector	Description
IP scan and attack	The infected system scans a range of IP addresses and service ports and targets several vulnerabilities known to hackers or left over from previous exploits, such as Code Red, Back Orifice, or PoizonBox.
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files infectious, including .html, .asp, .cgi, and other files. Users who browse to those pages infect their machines.
Virus	Each affected machine infects common executable or script files on all computers to which it can write, which spreads the virus code to cause further infection.
Unprotected shares	Using vulnerabilities in file systems and in the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to addresses found in the address book, the affected machine infects many other users, whose mail-reading programs automatically run the virus program and infect even more systems.

Figure 2-18 Denial-of-service attack

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of service attack, dozens or even hundreds of computers (known as zombies or bots) are compromised, loaded with Dos attack software, and then remotely activated by the hacker to conduct a coordinated attack.

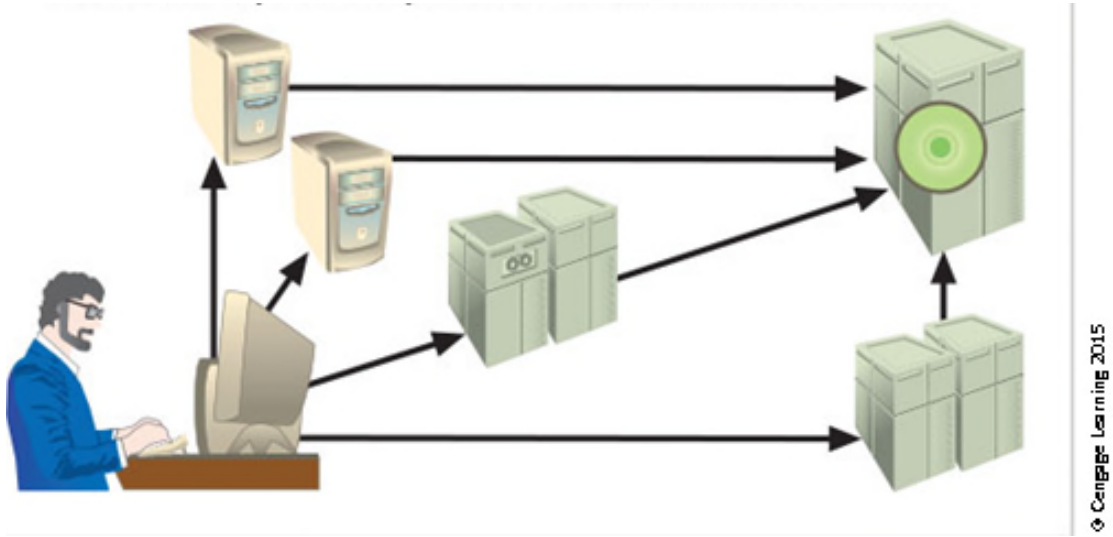


Figure 2-19 IP Spoofing attack

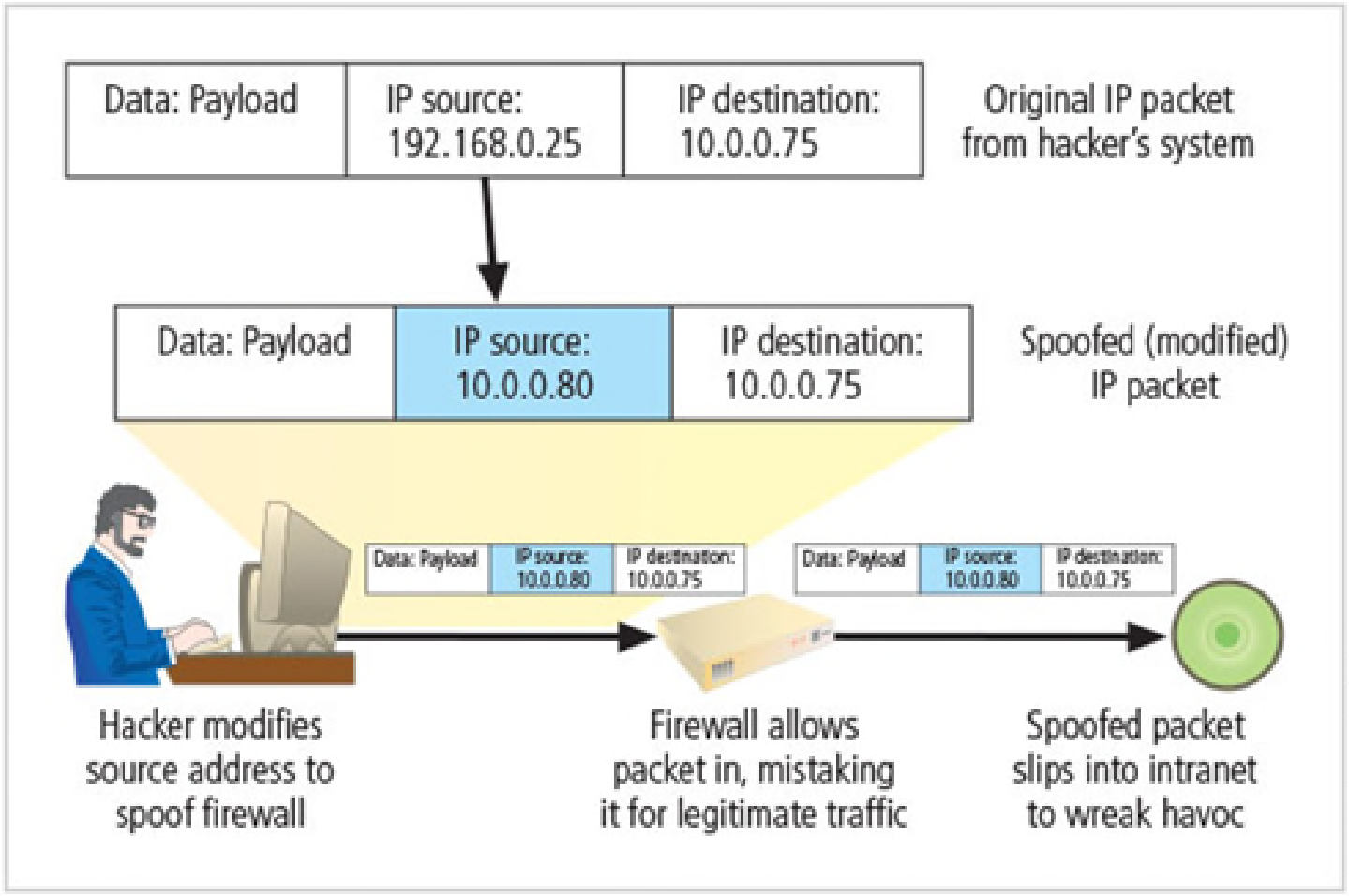
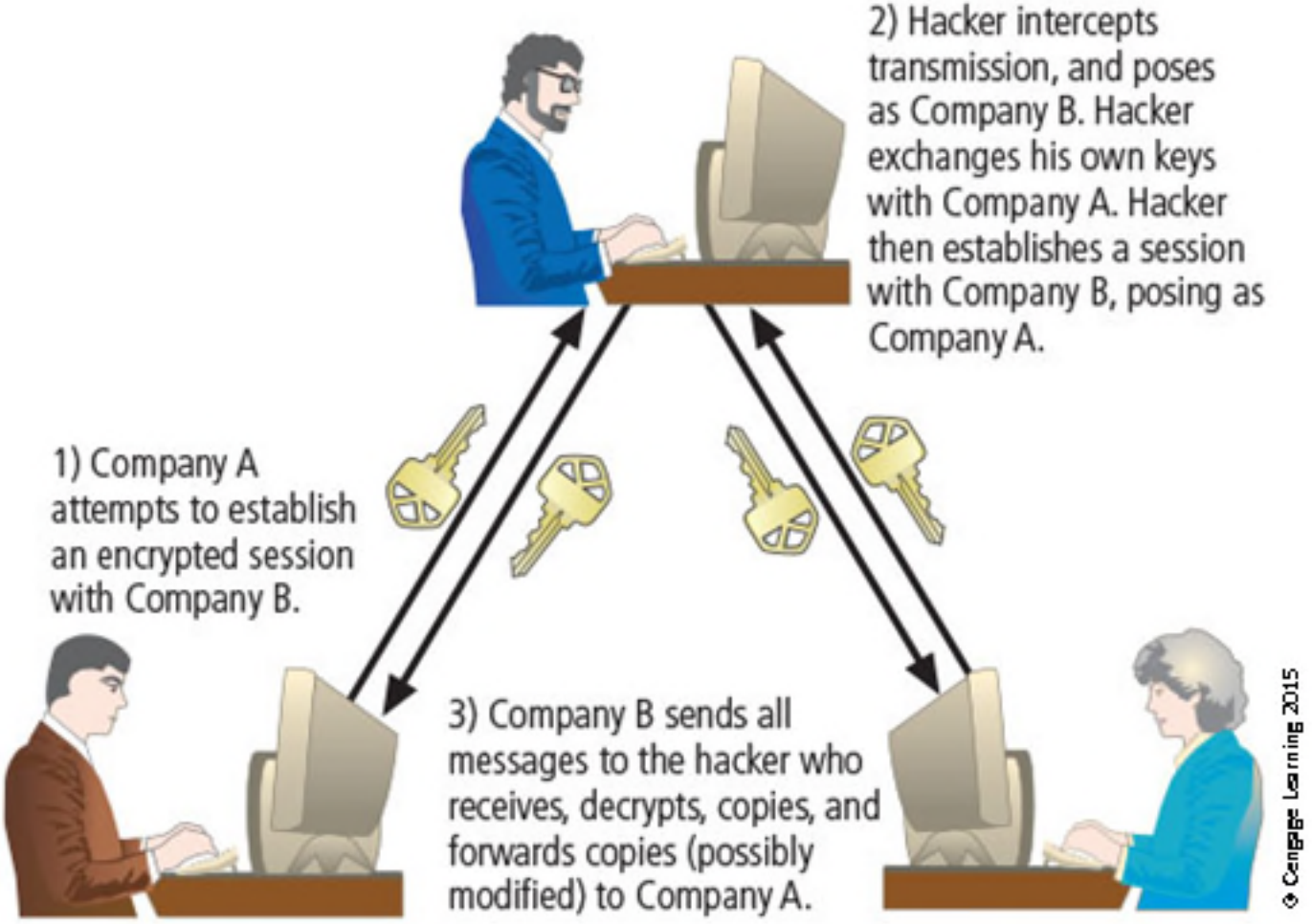


Figure 2-20 Man-in-the-middle attack



Technical Hardware Failures or Errors (1 of 2)

- They occur when a manufacturer distributes equipment containing a known or unknown flaw.
- They can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.
- Some errors are terminal and some are intermittent.
  - Intel Pentium CPU failure.
  - Mean time between failure measures the amount of time between hardware failures.

Technical Software Failures or Errors (2 of 2)

- Large quantities of computer code are written, debugged, published, and sold before all bugs are detected and resolved.
- Combinations of certain software and hardware can reveal new software bugs.
- Entire Web sites are dedicated to documenting bugs.
- Open Web Application Security Project (OWASP) is dedicated to helping organizations create/operate trustworthy software and publishes a list of top security risks.

The Deadly Sins in Software Security (1 of 3)

- Common failures in software development:
  - Buffer overruns
  - Catching exceptions
  - Command injection
  - Cross-site scripting (XSS)
  - Failure to handle errors
  - Failure to protect network traffic
  - Failure to store and protect data securely
  - Failure to use cryptographically strong random numbers
  - Format string problems
  - Neglecting change control

The Deadly Sins in Software Security (2 of 3)

- Improper file access
- Improper use of Secure Sockets Layer (SSL)
- Information leakage
- Integer bugs (overflows/underflows)
- Race conditions
- SQL injection

The Deadly Sins in Software Security (3 of 3)

- Problem areas in software development:
  - Trusting network address resolution
  - Unauthenticated key exchange
  - Use of magic URLs and hidden forms
  - Use of weak password-based systems
  - Poor usability

Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems.
- Proper managerial planning should prevent technology obsolescence.
- IT plays a large role.

Theft

- Illegal taking of another's physical, electronic, or intellectual property.
- Physical theft is controlled relatively easily.
- Electronic theft is a more complex problem; the evidence of crime is not readily apparent.

Summary (1 of 4)

- Information security performs four important functions:
  - Protecting organization's ability to function
  - Enabling safe operation of applications implemented on organization's IT systems
  - Protecting data an organization collects and uses
  - Safeguarding the technology assets in use at the organization
- Threats or dangers facing an organization's people, information, and systems fall into the following categories:
  - Compromises to intellectual property: Intellectual property, such as trade secrets, copyrights, trademarks, or patents, are intangible assets that may be attacked via software piracy or the exploitation of asset protection controls.

Summary (2 of 4)

- Deviations in quality of service: Organizations rely on services provided by others.
- Losses can come from interruptions to those services.
- Espionage or trespass: Asset losses may result when electronic and human activities breach the confidentiality of information.
- Forces of nature: A wide range of natural events can overwhelm control systems and preparations to cause losses to data and availability.
- Human error or failure: Losses to assets may come from intentional or accidental actions by people inside and outside the organization.
- Information extortion: Stolen or inactivated assets may be held hostage to extract payment of ransom.

Summary (3 of 4)

- Sabotage or vandalism: Losses may result from the deliberate sabotage of a computer system or business, or from acts of vandalism. These acts can either destroy an asset or damage the image of an organization.
- Software attacks: Losses may result when attackers use software to gain unauthorized access to systems or cause disruptions in systems availability.
- Technical hardware failures or errors: Technical defects in hardware systems can cause unexpected results, including unreliable service or lack of availability.
- Technical software failures or errors: Software used by systems may have purposeful or unintentional errors that result in failures, which can lead to loss of availability or unauthorized access to information.

Summary (4 of 4)

- Technological obsolescence: Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems that may result in loss of availability or unauthorized access to information.
- Theft: Theft of information can result from a wide variety of attacks.