Security Awareness 6th edition Ciampa Solutions Manual

SKU: 9780357883761-SOLUTIONS

Solution and Answer Guide

CIAMPA, SECURITY AWARENESS 6E, 2024, 9780357883761; MODULE 1: INTRODUCTION TO CYBERSECURITY

TABLE OF CONTENTS

REVIEW QUESTION ANSWERS

1. Which of the following is NOT a reason why it is difficult to defend against today's attackers?
    a. Faster detection of vulnerabilities
    b. Complexity of attack tools
    c. Weak security update distribution
    d. Greater sophistication of attacks

    Answer: b

    Analysis:

    a. Incorrect. Faster detection of vulnerabilities is a valid reason for the difficulty in defending.
    b. Correct. It is the simplicity, not complexity, of attack tools that makes it difficult to defend against attackers.
    c. Incorrect. Weak security update distribution is a valid reason for the difficulty in defending.
    d. Incorrect. Greater sophistication of attacks is a valid reason for the difficulty in defending.
2. Which of the following accounts for the greatest difficulty in preventing attacks?
    a. Availability and simplicity of attack tools
    b. Delays in security updating
    c. Distributed attacks
    d. User confusion

    Answer: d

    Analysis:

    a. Incorrect. Availability and simplicity of attack tools are not considered the greatest difficulty in preventing attacks.
    b. Incorrect. Delays in security updating are not considered the greatest difficulty in preventing attacks.
    c. Incorrect. Distributed attacks are not considered the greatest difficulty in preventing attacks.
    d. Correct. The one factor that undoubtedly accounts for the greatest difficulty in preventing attacks is user confusion. For many years, users have been called upon to make often difficult security decisions and then perform complicated procedures on their devices—often with little information to guide them.
3. In a general sense, what is security?
    a. It is only available on specialized computers.
    b. It is protection from only direct actions.
    c. It is the steps necessary to protect a person or property from harm.
    d. It is both an art and a science.

    Answer: c

    Analysis:

    a. Incorrect. Security is available on all sorts of devices and not just on specialized computers.

b. Incorrect. Security is protection from both direct and indirect actions.
c. Correct. Sometimes security is defined as the state of being free from danger, which is the goal of security. It is also defined as the measures taken to ensure safety, which is the process of security. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal. In this light, security can be defined as the necessary steps to protect from harm.
d. Incorrect. Security is considered both an art as well as a process.

4. Which of the following ensures that only authorized parties can view information?
   a. Confidentiality
   b. Authorization
   c. Integrity
   d. Availability

   Answer: a

   Analysis:

   a. Correct. Confidentiality ensures that only authorized parties can view the information.
   b. Incorrect. Authorization is providing permission or approval to specific technology resources.
   c. Incorrect. Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data.
   d. Incorrect. Availability ensures that data is accessible to only authorized users and not to unapproved individuals.

5. Why can brokers command such a high price for what they sell?
   a. Brokers are licensed professionals.
   b. The attack targets are always wealthy corporations.
   c. The vulnerability they uncover was previously unknown and is unlikely to be patched quickly.
   d. Brokers work in teams and all the members must be compensated.

   Answer: c

   Analysis:

   a. Incorrect. This reason is fictitious: brokers are not licensed professionals.
   b. Incorrect. This reason is fictitious: attacks can target anyone, not just wealthy corporations.
   c. Correct. The buyers are generally willing to pay a high price because this vulnerability is unknown to the software vendor and thus is unlikely to be “patched” until after new attacks based on it are already widespread.
   d. Incorrect. This reason is fictitious: brokers do not always work in teams.

6. Which of the following is NOT a successive layer in which information security is achieved?
   a. Products
   b. People
   c. Policies and procedures
   d. Purposes

   Answer: d

Analysis:

a. Incorrect. Products is a valid layer: procedures enable people to understand how to use products to protect information.
b. Incorrect. People is a valid layer: procedures enable people to understand how to use products to protect information.
c. Incorrect. Policies and procedures is a valid layer: procedures enable people to understand how to use products to protect information.
d. Correct. A purpose is not a successive layer in which information security is achieved.

7. What is a class of attacks by state actors that use innovative attack tools to silently extract data over an extended period of time?
   a. RPP
   b. XLX
   c. APT
   d. GOR

   Answer: c

   Analysis:

   a. Incorrect. RPP is fictitious and does not exist.
   b. Incorrect. XLX is fictitious and does not exist.
   c. Correct. State actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. This has created a new class of attacks called Advanced Persistent Threat (APT). These attacks use innovative attack tools (advanced) and once a system is infected, they silently extract data over an extended period of time (persistent).
   d. Incorrect. GOR is fictitious and does not exist.
8. What is a person or element that has the power to carry out a threat?
   a. Threat actor
   b. Agent
   c. Risk exploiter
   d. Cyber invader

   Answer: a

   Analysis:

   a. Correct. A threat actor is a term used to describe individuals or entities who are responsible for cyber incidents against the technology equipment of enterprises and users.
   b. Incorrect. An agent is fictitious and does not exist.
   c. Incorrect. A risk exploiter is fictitious and does not exist.
   d. Incorrect. A cyber invader is fictitious and does not exist.
9. In cybersecurity, what is a flaw or weakness that allows an attacker to bypass security protections?
   a. Access
   b. Vulnerability
   c. Worm hole
   d. Access control

Answer: b

Analysis:

a. Incorrect. Access does not apply to a flaw or a weakness.
b. Correct. Vulnerability is the correct term for applying to a flaw or weakness that allows an attacker to bypass security protections.
c. Incorrect. A worm hole does not apply to a flaw or a weakness.
d. Incorrect. Access control does not apply to a flaw or a weakness.

10. Which of the following ensures that individuals are who they claim to be?
    a. Demonstration
    b. Authentication
    c. Accounting
    d. Certification

Answer: b

Analysis:

a. Incorrect. Demonstration is a fictitious method of ensuring that individuals are who they claim to be.
b. Correct. Authentication ensures that the person is who she claims to be and not an impostor.
c. Incorrect. Accounting provides tracking or an audit trail of events.
d. Incorrect. The term “certification” does not apply in the context of ensuring individuals.

11. Which of the following requires that enterprises must guard protected health information and implement policies and procedures to safeguard it?
    a. Hospital Protection and Insurance Association Agreement (HPIAA)
    b. Sarbanes-Oxley Act (Sarbox)
    c. Gramm-Leach-Bliley Act (GLBA)
    d. Health Insurance Portability and Accountability Act (HIPAA)

Answer: d

Analysis:

a. Incorrect. HPIAA is fictitious and does not exist.
b. Incorrect. The Sarbox regulation is an attempt to fight corporate corruption and covers corporate officers, auditors, and attorneys of publicly traded companies.
c. Incorrect. The GLBA requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information.
d. Correct. Under the Health Insurance Portability and Accountability Act (HIPAA), healthcare enterprises must guard protected healthcare information and implement policies and procedures to safeguard it, whether it be in paper or electronic format.

12. Which of the following is motivated for the sake of their principles or beliefs?
    a. Cyberterrorists
    b. Insiders
    c. Script kiddies
    d. Computer spies

Answer: a

Analysis:

a. Correct. Cyberterrorists' motivation is ideological, attacking for the sake of their principles or beliefs. Cyberterrorists are often the attackers that are most feared, for it is almost impossible to predict when or where an attack may occur.
b. Incorrect. Insiders do not work for principles or beliefs.
c. Incorrect. Script kiddies are typically younger individuals who want to attack computers, yet they lack the knowledge of computers and networks needed to do so. Script kiddies instead do their work by downloading automated attack software (scripts) from websites and using it to perform malicious acts.
d. Incorrect. Computer spies are not motivated for the sake of principles or beliefs.

13. What is the difference between a hactivist and a cyberterrorist?
    a. A hactivist is motivated by ideology while a cyberterrorist is not.
    b. Cyberterrorists always work in groups while hactivists work alone.
    c. The aim of a hactivist is not to incite panic like cyberterrorists.
    d. Cyberterrorists are better funded than hactivists.

Answer: c

Analysis:

a. Incorrect. Ideology is not a difference between these two groups.
b. Incorrect. The statement "Cyberterrorists always work in groups while hactivists work alone" is false.
c. Correct. The goal of a hactivist is not to incite panic but is often retaliatory in nature.
d. Incorrect. Cyberterrorists are not necessarily better funded than hactivists in all instances.

14. Lorenzo has decided to make regular backup copies of information from his laptop and store it in a safe place. Which of the following principles is Lorenzo following?
    a. Minimizing losses
    b. Blocking attacks
    c. Updating defenses
    d. Using layers

Answer: a

Analysis:

a. Correct. It is important that action be taken in advance in order to minimize losses. This may involve keeping backup copies of important data stored in a safe place.
b. Incorrect. Blocking attacks is not a principle that involves regular data backups.
c. Incorrect. Updating defenses is not a principle that involves regular data backups.
d. Incorrect. Using layers is not a principle that involves regular data backups.

15. Which of the following is NOT classified as an insider?
    a. Business partners
    b. Contractors
    c. Cybercriminals
    d. Employees

Answer: c

Analysis:

a. Incorrect. “Business partners” is a classification of an insider.
b. Incorrect. “Contractors” is a classification of an insider.
c. Correct. Cybercriminals are not insiders.
d. Incorrect. “Employees” is a classification of an insider.

16. What is an objective of state actor?
    a. To right a perceived wrong
    b. To spy on citizens
    c. To sell vulnerabilities to the highest bidder
    d. To earn fortune over fame

Answer: b

Analysis:

a. Incorrect. State actors do not attempt to right any perceived wrongs.
b. Correct. The foes of a government may be foreign governments or even citizens of their own nation that the government considers hostile or threatening, and state actors are often employed to attack these perceived foes.
c. Incorrect. Brokers sell vulnerabilities to the highest bidder.
d. Incorrect. Earning fortune over fame is an objective of cybercriminals.

17. Which of the following requires banks and financial institutions to protect all electronic and paper containing personally identifiable financial information?
    a. California Savings and Loan Security Act (CS&LSA)
    b. Sarbanes-Oxley Act (Sarbox)
    c. Gramm-Leach-Bliley Act (GLBA)
    d. USA Patriot Act

Answer: c

Analysis:

a. Incorrect. The CS&LSA is fictitious and does not exist.
b. Incorrect. Sarbox covers the corporate officers, auditors, and attorneys of publicly traded companies. Stringent reporting requirements and internal controls on electronic financial reporting systems are required.
c. Correct. The Gramm-Leach-Bliley Act (GLBA) passed in 1999 protects private data. GLBA requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information. All electronic and paper data containing personally identifiable financial information must be protected.
d. Incorrect. The USA Patriot Act does not apply to banks and financial institutions protecting information.

18. Which of the following ensures that the information is correct and no unauthorized person or malicious software has altered that data?
    a. Integrity
    b. Obscurity
    c. Layering
    d. Confidentiality

Answer: a

Analysis:

a. Correct. Integrity ensures that the information is correct and that no unauthorized person or malicious software has altered the data.
b. Incorrect. Obscurity does not ensure that information is correct.
c. Incorrect. Layering does not ensure that information is correct.
d. Incorrect. Confidentiality ensures that only authorized parties can view the information.

19. Which of the following is a type of action that has the potential to cause harm?
    a. Hazard
    b. Risk
    c. Threat
    d. Peril

Answer: c

Analysis:

a. Incorrect. “Hazard” is not the correct term used to describe an action that has the potential to cause harm.
b. Incorrect. “Risk” is not the correct term used to describe an action that has the potential to cause harm.
c. Correct. A threat is a type of action that has the potential to cause harm.
d. Incorrect. “Peril” is not the correct term used to describe an action that has the potential to cause harm.

20. Bella is explaining to her friend that her new role at work requires her to block the pathways for an attack. Which of the following terms would Bella use to explain what this pathway is?
    a. Interception
    b. Attack vector
    c. Cybersecurity intrusion
    d. Asset roadway

Answer: b

Analysis:

a. Incorrect. “Interception” is not the correct term used to describe a pathway for blocking attacks.
b. Correct. An attack vector is a pathway used by a threat actor to penetrate a system.
c. Incorrect. “Cybersecurity intrusion” is not the correct term used to describe a pathway for blocking attacks.
d. Incorrect. “Asset roadway” is not the correct term used to describe a pathway for blocking attacks.

Hands-On Project Solutions

Project 1-1: Examine Data Breaches – Visual

The purpose of this project is to assist students in grasping the enormity of recent cybersecurity attacks.

In Step 14, students are asked to "Create your own filters to view different types of breaches." There are a variety of filters that students may apply. Students are also asked, "Does this graphic convey a compelling story of data breaches?" Most students will respond affirmatively since a picture is worth a thousand words.

In Step 17, students are asked, "How does this visualization help you with the understanding of threats?" Students will likely respond that that were unaware of the enormity of the problem and seeing it in a graphical form can be beneficial.

Project 1-2: Configure Microsoft Windows Sandbox

This project allows students to use the Microsoft Windows Sandbox feature. This feature was first added in Windows 10 and has proven to be very popular, since it allows users to download and test software without affecting the underlying computer. All Hands-On Projects in this course can take advantage of the Sandbox by performing the activities within the Sandbox, thus eliminating any impact on the computer itself. Once the Sandbox is closed, then all work is erased. Note that it may be necessary to first launch the computer's BIOS or UEFI and turn on virtualization.

In Step 13, students are asked, "What happened to Google Chrome? Why?" Students should respond that the Sandbox is a nonpersistent environment, and any software installed or used in the Sandbox will disappear when the Sandbox is shut down.

Project 1-3: Comparing Data Breach Notification Letters

Because there are no national data breach notification laws in place, each state has its own requirements. This activity compares several California data breach notifications as examples of what a state may require of a business that experienced a data breach.

In Step 2, students are asked if the number of recent California data breaches is surprising. Most students will respond that it is surprising, illustrating again that breaches have become so commonplace, they often do not make the news.

In Step 13, students are asked, "Which elements are most useful if you were the victim of this breach? What additional information would be helpful?" Although the answers will vary, most students may respond that just the notification itself is helpful. They may also indicate that the date and scope of the breach is good information.

In Step 14, students are asked to create their own sample notification letter. Students will likely include multiple elements from the Sample of Notice entry. They may also want to include new elements that are more direct to helping the user, such as including a telephone number for those impacted by the breach may use for further information.

Project 1-4: Are You a Victim?

This project asks students to enter their email address to determine if it is on a list of known breaches.

In Step 6, students are asked if they remember being alerted to a data breach that compromised their email address. Because data breaches have become so commonplace, most victims cannot remember when the breach occurred or what was stolen.

In Step 9, students are asked if this activity would inspire them to take even greater security protections. Hopefully most students will answer that this type of real-life activity will inspire them to be more secure once they see that they could be a victim.

Case Project Solutions

Case Project 1-1: Personal Attack Experiences

Students are asked to describe an attack that they or a friend has experienced and provide specific details. At this point, most students may be confused on the details and how the attack was mitigated. This is not unusual, since most students lack the background to understand the attack and how it impacted them. As a teaching moment, instructors may want to reassure students that this confusion is normal, but the goal of this course is to help students understand more about attacks and defenses.

Case Project 1-2: Security Podcasts or Video Series

Students will locate two podcasts and two video series about computer security. There are an enormous number of podcasts and videos on cybersecurity. As a branch off this project, instructors may ask students to swap lists or compile a master listing for the entire class to which students may refer back to during the course.

Case Project 1-3: Sources of Security Information

A partial listing of sources for cybersecurity information is provided, and students are asked to create a table listing the Advantages, Disadvantages, Example, and Rating of each of the seven listings. This is an opportunity for a class-wide discussion on each of the sources, since no two students will reach the same conclusions. It is interesting to note that research has shown that “Friends and family” is actually a source that many users rank very high. Even though these individuals may not be well informed on cybersecurity topics, they may be trusted sources. This illustrates the problem users face of filtering through conflicting information found on the Internet or even where to turn for that information.

Instructor Manual

MARK CIAMPA, SECURITY AWARENESS: APPLYING PRACTICAL CYBERSECURITY IN YOUR WORLD, 2024, 9780357883761; MODULE 1: INTRODUCTION TO CYBERSECURITY

Table of Contents

Purpose and Perspective of the Module

This module introduces the student to cybersecurity. It begins by examining why it is so difficult to protect devices. The module then describes cybersecurity in more detail and explores its importance. Finally, the module looks at who is responsible for these attacks, and what the steps are in building a comprehensive security strategy.

Module Objectives

By the end of this module, your students should be able to:

1. Explain the difficulties in preventing attacks.
2. Define cybersecurity and describe why it is important.
3. Identify threat actors and their attributes.
4. Explain how to build a comprehensive cybersecurity strategy.

Key Terms

accounting: provides tracking (“audit trail”) of events

Advanced Persistent Threat (APT): a new class of attacks that use innovative attack tools and once a system is infected, they silently extract data over an extended period of time

asset: an item that has value

attack vector: a pathway used by a threat actor to penetrate a system

authentication: ensures that the individual is who she claims to be (the authentic or genuine person)

authorization: providing permission or approval to specific technology resources

availability: ensures that data is accessible to only authorized users and not to unapproved individuals

brokers: attackers who sell their knowledge of a vulnerability to other attackers or even governments

confidentiality: ensures that only authorized parties can view the information

cybercriminal: those that attack for financial gain

cybersecurity: that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit information through products, people, and procedures

cyberterrorism: attacks that are intended to cause panic or provoke violence among citizens

cyberterrorist: attackers whose motivation is ideological, attacking for the sake of their principles or beliefs

General Data Protection Regulation (GDPR): holds companies legally obligated to inform the European Union if they suffer a breach involving the personal information of customers or employees

Gramm-Leach-Bliley Act (GLBA): requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information

hacker: a person who uses advanced computer skills to attack computers

hactivists: attackers who break into a website and change its contents as a means of making a political statement

Health Insurance Portability and Accountability Act (HIPAA): requires healthcare enterprises to guard protected healthcare information and implement policies and procedures to safeguard it, whether it be in paper or electronic format

identity theft: stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, often for financial gain

insider: an organization's employees, contractors, and business partners

integrity: ensures that the information is correct and no unauthorized person or malicious software has altered the data

Payment Card Industry Data Security Standard (PCI DSS): a set of security standards that all companies that process, store, or transmit credit card information must follow

risk: a situation that involves exposure to some type of danger

Sarbanes-Oxley Act (Sarbox): an attempt to fight corporate corruption

script kiddie: typically, younger individuals who want to attack computers, yet they lack the knowledge of computers and networks needed to do so state actors: state-

sponsored attackers, employed by their government, who launch cyberattacks against their foes

threat: a type of action that has the potential to cause harm

threat actor: describes individuals or entities who are responsible for cyber incidents against the technology equipment of enterprises and users

threat agent: a person or element that has the power to carry out a threat

threat likelihood: the probability that the threat will come to fruition

vulnerability: a weakness that can be exploited

[return to top]

What's New in This Module

The following elements are improvements in this module from the previous edition:

- New focus on cybersecurity rather than information security.
- New attention to current terminology for hackers and attacks.
- Identification of threat actors and their attributes
- New attention to the importance of building a cybersecurity strategy

[return to top]

Module Outline

The following outline organizes activities (including any existing discussion questions in PowerPoints or other supplements) and assessments by module (and therefore by topic), so that you can see how all the content relates to the topics covered in the text.

I. Today's Attacks (PPT Slides 5–7)
   a. In the past, the news of just one cyber attack would have gone viral across the Internet. Today, a cyber attack barely registers a blip on the radar screen. The AV-TEST Institute receives instances of over 450,000 new malicious programs (malware) and potentially unwanted applications (PUA) each day.
   b. Anyone who uses a computing device (such as a laptop, a tablet, or a smartphone) is at risk of being attacked and compromised. Anyone who has a device connected to the Internet (such as a security camera, a

doorbell, or a thermostat) is also at risk of being attacked and compromised.

c. Polling Activity: 2–5 minutes total. Poll the class. If time allows, initiate a discussion.
    i. Question: If you were warned that a vicious new attack was to begin within the next 15 minutes, would you know the steps to take to check the security on your devices and quickly fix anything deficient? Yes or No

II. Difficulties in Preventing Attacks (PPT Slides 8–10)
    a. Universally connected devices. Not just computers and mobile devices but IP connected devices such as doorbells and monitors.
    b. Attackers from anywhere in the world can send attacks. They can launch attacks against millions of computers within minutes with unprecedented speed without human intervention. Today's attack tools vary their behavior so the same attack appears differently each time.
    c. Greater sophistication as attacks are more complex and harder to defend. Common Internet communications are used so attacks are varied each time complicating detection.
    d. Attack tools require little knowledge of tool development by the attacker as tools are readily available and free to download.
    e. Attackers are finding security weaknesses in hardware and software and exploited.
    f. Vendors are overwhelmed with updating software and hardware, and updates do not keep up with new attacks.
    g. Vendors update on regular basis combining multiple fixes, delaying implementation of security.
    h. Single devices can attack multiple devices, known as a distributed attack
    i. End users are required to do preventive measures with little information, sometimes contradictory yet critical.
    j. Knowledge Check Activity: 2–5 minutes total. Ask students to determine which two statements are correct.
        i. Some attacks can vary their behavior so that the same attack appears differently. **[Correct]**
        ii. Attack tools still require a degree of skill and knowledge to use them. **[Incorrect]**
        iii. The single difficulty that accounts for the greatest difficulty in preventing attacks is user confusion. **[Correct]**

III. What Is Cybersecurity? (PPT Slides 13–17)
    a. It is important to know the definition of security and how it relates to cybersecurity. It is also important to know the terminology used in this area in order to understand the importance of cybersecurity.
    b. Security is necessary to protect a person or property from harm. For example, security for a home can include protection from burglary and

protection from natural forces, such as storms. The relationship between security and convenience is **not** directly proportional. If two events are directly proportional, then as one increases, the other increases. The relationship between security and convenience is indirectly proportional. As security increases, convenience decreases.

c. Cybersecurity is an art of protecting networks and devices. It systematically applies the correct knowledge and skills and is never a "one and done" event. Cybersecurity ensures protective measures are properly implemented.
d. Cybersecurity as a practice of continual action to ensure:
    i. Confidentiality ensures authorized access.
    ii. Integrity ensures correct information.
    iii. Availability ensures access to information.
e. Protections required
    i. Authentication of users
    ii. Authorization or permissions
    iii. Accounting or audit trails
f. Knowledge Check Activity: 2–5 Minutes total
    i. Match
        1. Audit trail of events—Accounting
        2. Password utilization—Authentication
        3. Permission to access—Authorization

IV. Importance of Cybersecurity (PPT Slides 27–32)
a. Data theft—personal or corporate data—give examples
b. Identity theft—personal information—give examples
c. Cyberterrorism—attack on information, computers via violence—examples
d. Legal consequences—laws to protect privacy and data
    i. HIPPA—examples and why
    ii. Sarbanes Oxley—examples and why
    iii. Gramm Leach Bliley Act—examples and why
    iv. Payment Card Industry Data Security Standard—examples and why
e. Knowledge Check Activity—ask students to explain how they relate to HIPPA
    i. HIPPA protects their individual health data.
    ii. HIPPA keeps their health data private.
    iii. HIPPA requires personal authorization to release data.
    iv. Everyone signs a HIPPA form at a new doctor to share information.

V. Review definitions of different types of attackers (PPT Slides 35–47)
a. Cybercriminals—hackers for financial gain
b. Script kiddies—utilize predeveloped hack software, are inexperienced to do malicious attacks

c. Brokers—paid hackers to find vulnerabilities for vendors
d. Insiders—disgruntled employees or business partners
e. Cyberterrorist—attack for disruption or panic
f. Hactivist—make political statements
g. State actors—government employed cyberattackers
h. Knowledge check—match
    i. Hackers from countries not friendly to the United States—State actors
    ii. Disgruntled employee—Insider
    iii. Young inexperienced hacker—Script Kiddie

VI. Security Strategy (PPT Slides 48–53)
a. Block attack—strong security perimeter
b. Update defenses—keep security up to date
c. Minimize losses—keep backups just in case
d. Layer—Use multiple defenses
e. Be on defensive—always

[return to top]

TEACHING TIPS

Challenges of Securing Information

1. Introduce the concept of cybersecurity, noting that it is more complicated than many might think.

Today's Attacks

1. Demonstrate the number and variety of attack types by discussing the information regarding recent computer security attacks listed on pages 4–6.
2. Review the statistics related to personal information breaches provided in Table 1-1.

Teaching Tip	Ask students whether they have been the victim of any computer attacks. Invite them to describe their experiences.

Difficulties in Defending against Attacks

1. Explain why it is so difficult to defend against attacks by discussing the following challenges:
    a. Universally connected devices
    b. Increased speed of attacks
    c. Greater sophistication of attacks
    d. Availability and simplicity of attack tools
    e. Faster detection of vulnerabilities
    f. Delays in security updating

g. Weak security update distribution
h. Distributed attacks
i. User confusion

Note: These issues are summarized in Table 1-2 in the textbook.

What Is Information Security?

Note that the following sections will introduce the concept of security, review common terminology, and explain the importance of information security.

Understanding Security

1. Provide a general definition of security. Note: Refer Pages 5–6 of textbook.
2. Explain the two sources of harm: a direct action or an indirect action.
3. Refer to Figure 1-2 and explain the relationship between security and convenience.

Defining Information Security

1. Define **information security** and explain how this concept applies to digital information.
2. Describe the following facets of protecting information and review the components of information security presented in Figure 1-3 and Table 1-3.
   a. Properly implementing protective measures
   b. CIA (Confidentiality, Integrity, Availability)
   c. AAA (Authentication, Authorization, and Accounting)
   d. Properly protecting the devices on which information is found

Note: Refer Pages 6–7 of textbook.

Teaching Tip	Discuss the importance of all the three aspects of CIA and how securing any one of the three without the others is insufficient.

3. Provide a more comprehensive definition of information security, noting that information security is achieved through combining products, people, and procedures.

Information Security Terminology

1. Refer to Table 1-4 and define the following terms as they relate to information security. Note: Refer Pages 8–9 of textbook.
   a. Asset
   b. Threat
   c. Threat agent
   d. Vulnerability
   e. Threat vector
   f. Threat likelihood
   g. Risk

Understanding the Importance of Information Security

Note that the next section outlines the main goals of information security.

Teaching Tip	Invite students to visit a U.S. Government website devoted to identity theft: **http://www.ftc.gov/bcp/edu/microsites/idtheft**

Preventing Data Theft

1. Explain how information security protects against the theft of data and how this type of theft affects businesses and individuals.

Thwarting Identity Theft

1. Define identity theft and emphasize that the cost to individuals who have been victims of identity theft as a result of data breaches is significant.

Avoiding Legal Consequences

1. Describe the laws listed on pages 17–18 to emphasize how businesses must ensure the security and confidentiality of data.

Maintaining Productivity

1. Discuss the productivity loss that occurs due to attack clean up and attack prevention. Table 1-5 summarizes these costs.

Foiling Cyberterrorism

1. Define cyberterrorism and explain why this is a growing area of concern.

Teaching Tip	Students can read more about how governments are using "lawful interception" methods to spy on citizens at the following site: http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance

Who Are the Attackers?

1. Note that the following section examines the profiles and motivations of different types of attackers.
2. Mention that the term hacker is no longer commonly used by the security community.

Cybercriminals

1. Define the term cybercriminal. Explain that this type of attacker is often located in Eastern Europe, Asia, and Third World regions (some underground forums are listed in Table 1-6).

2. Explain that the motivation of cybercriminals is to make money.

Script Kiddies

1. Define the term script kiddie and describe how they do their work. Note: Younger individuals who want to attack computers, yet they lack the knowledge of computers and networks needed to do so. Script kiddies instead do their work by downloading automated attack software (scripts) from websites and using it to perform malicious acts.
2. Explain the skills needed for creating attacks. These are summarized in Figure 1-5. Note: Skills required depend on the attack victim's security systems. High skills are required for very secure installations and low skills are required for computers with little or no security.

Brokers

1. Describe the motivation and operation methods of a broker. Note: Brokers assist and are paid by corporations to find vulnerabilities and are paid either piecework or salary.

Insiders

1. Discuss the threat provided to an organization by its employees and the different factors that might motivate an attack by an employee. Note: Employees that are fired or let go are primary motivators.

Cyberterrorists

1. Define the term cyberterrorist and discuss the goals of a cyberterrorist attack. Note: Cyberterrorist is a hacker whose motivation is ideological, attacking for the sake of principles or beliefs. Goal is to cause disruption or panic.
2. Explain why a cyberterrorist may be the most feared type of attacker. Note: Cyberterrorist is set to disrupt an infrastructure such as financial, utility, or government to spread panic in the general population.

Hacktivist

1. Describe a hacktivist and distinguish one from a cyberterrorist. Note: A hacktivist does damage for personal reasons, such as to a bank, etc., or to make a statement as to how good they are.

State-Sponsored Attackers

1. Review the examples on page 23 to explain why government agencies appear to have been behind attacks on foreign governments and even attacks against their own citizens when considered hostile or threatening. Note: Have students name some probable state-sponsored attackers.
2. Use Table 1-7 to summarize the characteristics of different types of attackers.

Building a Comprehensive Security Strategy

1. Introduce the five key elements of a security strategy"
    a. Block attacks
    b. Update defenses
    c. Minimize losses
    d. Use layers
    e. Stay alert

Block Attacks

1. Describe how a practical security strategy should block attacks. Note: Have multiple levels of security, from network to server to data.

Update Defenses

1. Describe how a practical security strategy should protect information. Note: Develop and implement security update methodology for all security systems.

Minimize Losses

1. Describe how a practical security strategy should block attacks. Note: Security methodology should include minimizing losses by backing up critical information.

Stay Alert

Describe how a practical security strategy requires constant vigilance as new attacks exploiting previously unknown vulnerabilities occur on a daily basis. Note: Ensure that security is a standard component of any newly developed processes.

Teaching Tip	Learn more about cyber threat source descriptions in the following article: **http://www.us-cert.gov/control_systems/csthreats.html**

Teaching Tip	Students can learn more about perimeter security from the following Redpaper: **http://www.redbooks.ibm.com/abstracts/redp4397.html**

QUICK QUIZ 1

1. What is the definition of a Risk?
    A. Exposure to danger
    B. Pathway to penetrate a system
    C. Threat to security
    D. Weakness

Answer: A

2. True or False: One of the main targets of attackers today is the healthcare industry.

   Answer: True

3. Which of the following protections ensures that only authorized parties can view the information?
   A. Availability
   B. Confidentiality
   C. Accounting
   D. Integrity

   Answer: B

4. What term is frequently used to describe the tasks of securing information that is in a digital format?
   Answer: Information security

5. Which of the following is an example of a vulnerability?
   A. Likelihood of virus infection
   B. Hurricane
   C. Software defect
   D. Stolen passwords through a software flaw

   Answer: C

6. Which of the following laws was created as an attempt to fight corporate corruption?
   A. Payment Card Industry Data Security Standard
   B. California's Database Security Breach Notification Act
   C. The Health Insurance Portability and Accountability Act of 1996
   D. The Sarbanes-Oxley Act of 2002

   Answer: D

[return to top]

QUICK QUIZ 2

1. What term is used as a generic term used to describe individuals who launch attacks against other users and their computers (another generic word is simply attackers)?

   Answer: Cybercriminals

2. Which term is used to describe individuals who want to attack computers yet they lack the knowledge of computers and networks needed to do so?
   A. Script kiddies
   B. Cybercriminals
   C. Brokers
   D. Insiders

   Answer: A

3. Which type of attacker might break into a website and change the contents on the site as a means of making a political statement against those who oppose their beliefs?
   A. State-sponsored attacker
   B. Broker
   C. Insider
   D. Hacktivist

   Answer: D

4. What are the five key elements to creating a practical security strategy?

   Answer: There are five key elements to creating a practical security strategy: block attacks, update defenses, minimize losses, use layers, and stay alert

5. What type of hacker is known as an ethical hacker, assisting in uncovering vulnerabilities for organizations or vendors?
   A. Gray Hat Hacker
   B. White Hat Hacker
   C. Black Hat Hacker
   D. Hactivist

   Answer: B

6. True or False: Keeping backup copies of important data stored in a safe place is an example of implementing update defenses within a practical security strategy.

   Answer: False

Class Discussion Topics

1. Why is it important to distinguish between different types of attackers? Note: Different hackers use various techniques to breach security, and different security measures are required to protect against each.
2. Which of the five key security strategy elements discussed in the chapter do you think is the most important? Why? Note: Security strategies are (1) block

attacks, (2) update defenses (3), minimize loss, (4) use layers, and (5) stay alert.

[return to top]

Additional Projects

1. Research recent information security attacks. Find one that is not covered in the chapter and provide a summary of the incident.
2. Using the Internet, research one of the types of attackers covered in this chapter. Write a short profile of this type documenting their motivation, common methods of attack, and the prevalence of this type of attacker.
3. Use the Internet to research a well-known hacker, outlining their motivations, type of hacker, target or targets, what was stolen, result of hack, and if and when they were caught.

Additional Resources

1. Security Week Cyber Crime News: http://www.securityweek.com/cybercrime
2. FBI Cyber Crime Site http://www.fbi.gov/about-us/investigate/cyber/cyber
3. 2015 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2015/
4. Cybersecurity and Homeland Security: dhs.gov/topics/cybersecurity

[return to top]