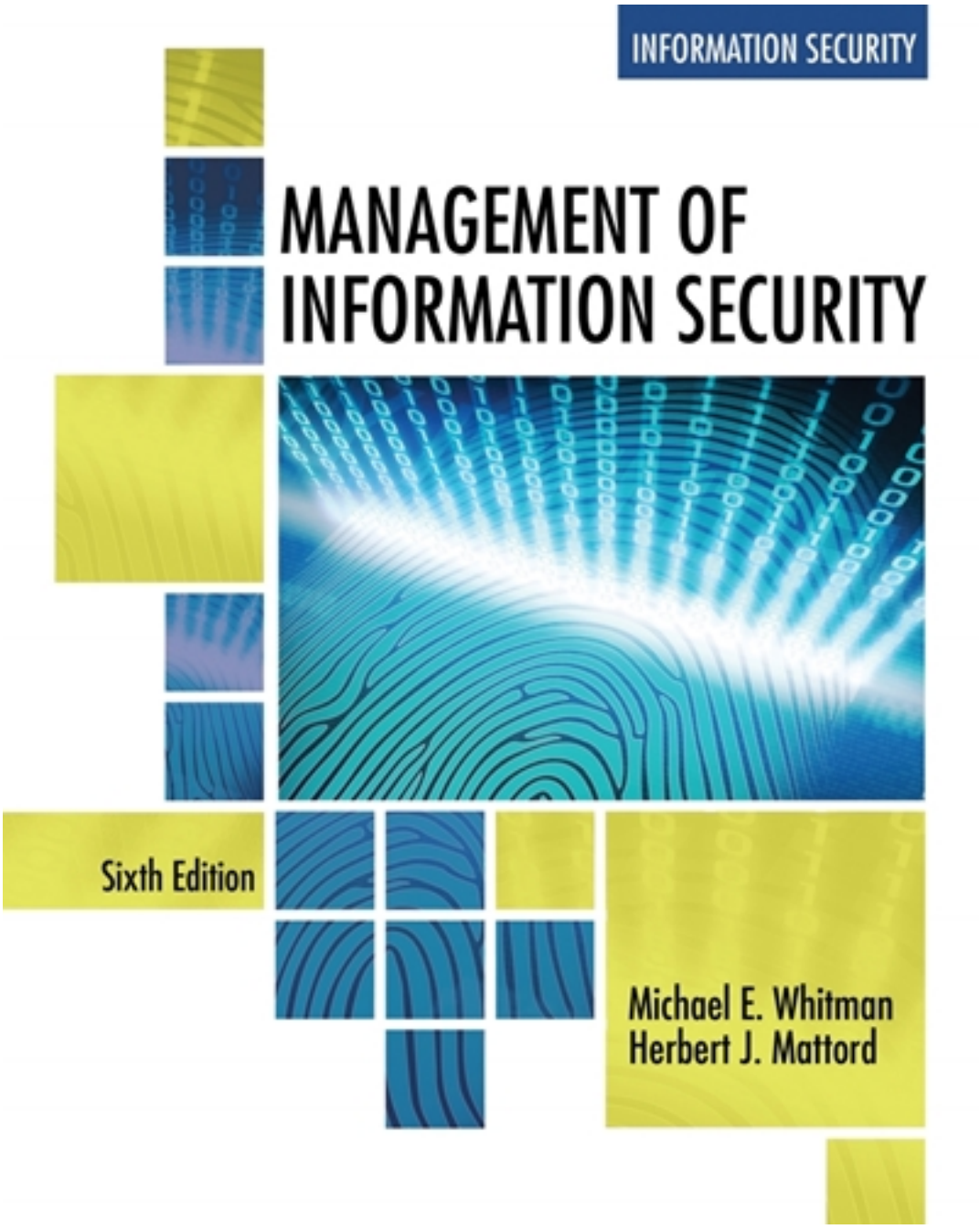
Solutions for Management of Information Security 6th Edition by Whitman

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Chapter 1 Answers to Review Questions and Exercises

[A HD]Review Questions

1. List and describe the three communities of interest that engage in an organization's efforts to solve InfoSec problems. Give two or three examples of who might be in each community. Answer: InfoSec community (InfoSec managers and professionals); information technology community (InfoSec technology managers and professionals); general business community (nontechnical managers and professionals).
2. What is information security? What essential protections must be in place to protect information systems from danger? Answer: InfoSec is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information. The elements of InfoSec that must be in place in order to have "complete" security are physical security, personal security, operations security, communications security, and network security.
3. What is the importance of the C.I.A. triad? Define each of its components. Answer: The C.I.A. triad has acted as the cornerstone of computer security since the days of the mainframe. Its component parts are confidentiality, integrity, and availability.
4. Describe the CNSS security model. What are its three dimensions? Answer: The CNSS security model is a comprehensive model of InfoSec. It has three dimensions, one of which is composed of the components of the C.I.A. triad. The other dimensions are composed of (1) policy, education, and technology and (2) storage, processing, and transmission. The CNSS model comprises 27 cells, and any security solution must address all of these cells to be considered complete.
5. What is the definition of "privacy" as it relates to InfoSec? How is this definition different from the everyday definition? Why is this difference significant? Answer: In InfoSec, "privacy" refers to information that is used only in ways known to the person providing it. This is slightly different from the traditional definition of "privacy," which is freedom from observation. The difference is significant because the privacy of information can be compromised even if it is not actually seen or observed by a third party.
6. Define the InfoSec processes of identification, authentication, authorization, and accountability. Answer: Identification is an information system's recognition of individual users. It is the first step in a user gaining access to secured information or areas. Authentication occurs when a user provides proof that he or she is who he or she really purports to be. Authorization assures that the user or the computer has been authorized to access specific information. Accountability is in place when a control provides assurance that all activities can be linked or attributed to a certain person or a process.

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

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

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

10. What is ransomware? How does an organization protect against it? Answer: Ransomware is 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. The primary defense against ransomware is a tested and frequently validated backup-and-restore program for all data. In addition, user training to avoid malware infections in general can lower exposure to more specific ransomware attacks.

11. What are the various types of force majeure? Which type might be of greatest concern to an organization in Las Vegas? Oklahoma City? Miami? Los Angeles? Answer: Force majeure refers to forces of nature or acts of God that pose a risk to people's lives and information security. Force majeure includes 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. Tornados are a concern for organizations in Oklahoma City. Miami would be most concerned with hurricanes or tsunamis. Earthquakes, mudslides, and wildfires would be of concern to organizations in Los Angeles.

12. How does technological obsolescence constitute a threat to information security? How can an organization protect against it? Answer: 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.

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

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

15. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is potentially more dangerous and devastating? Why? Answer: 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.

16. 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? Answer: 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.

17. What is management and what is a manager? What roles do managers play as they execute their responsibilities? Answer: Management is the process of achieving objectives/goals using a given set of resources. A manager works with and through other people by coordinating their work activities in order to accomplish the company's goals. As managers execute their responsibilities, they play various roles; among them are informational roles, interpersonal roles, and decisional roles.

18. How are leadership and management similar? How are they different? Answer: Leadership and management are similar in that a manager typically provides leadership as the leader of a group of people. Management and leadership are different in that some managers do not provide leadership. Managers sometimes only distribute work to employees, make budgets, and hire employees while not playing a role in motivating their employees. Motivation of employees is a job that is fulfilled by leaders.

19. What are the characteristics of management based on the method described in the text as the "popular approach" to management? Define each characteristic. Answer: Based on a popular approach to management, there are four characteristics of management: Planning: the process of setting objectives/goals and determining what should be done to accomplish them. Organizing: the process of arranging people and resources to work toward a common goal. Leading: the process of arousing enthusiasm and directing human resource efforts toward organizational goals. Controlling: the process of measuring performance and taking action to ensure desired outcome (results).

20. What are the three levels of planning? Define each. List the types of InfoSec plans and planning functions. Answer: The three levels of planning are tactical, strategic, and operational. Tactical planning focuses on resource planning by those just under "senior management" to cover a time period of no more than five years. Strategic planning is planning done at the highest level of an organization and usually covers a time period of more than five years. Operational planning is short-term, day-to-day planning of resources. InfoSec planning includes incident response planning, business continuity planning, disaster recovery planning, policy planning, personnel planning, technology rollout planning, risk management planning, and security program planning.

[A HD] Exercises

1. Assume that a security model is needed to protect information used in the class you are taking—say, the information in your course's learning management system. Use the CNSS model to identify each of the 27 cells needed for complete information protection. Write a brief statement that explains how you would address the components represented in each of the 27 cells. Answer: In general, C.I.A. is confidentiality, integrity, and availability.

   Confidentiality: Only allow students access to class if they have registered and paid for the ISA 3100 course at KSU for the fall semester of 2018. Controls to prevent unauthorized access to class would include taking roll call, learning each student's name and face, and verifying them against the computerized printout of each registered student.

   Integrity: Require students to carry their photo ID cards and present them on demand. Provide each student with a syllabus that contains the course description, course objectives, and instructor's contact information, including office hours and phone number. The syllabus must also include information about the withdrawal policy, grading, and an integrity statement that must be read and signed before the student can receive a final grade for the semester.

   Availability: Ensure that the classroom is accessible and provides a secure environment to promote well-organized learning. The controls include requiring the professor to be present at the beginning of class and have operational equipment so students can use their laptops for note taking.

Confidentiality—Policy—Storage: An example of protecting the confidentiality of class information in storage by means of policy would be issuing rules to keep access restricted to unauthorized viewers. One such rule could be to lock file cabinets that contain the information.

Confidentiality—Policy—Processing: An example of protecting the confidentiality of class information in processing by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being processed. For instance, only registered students in the class should be allowed to attend and listen to lectures.

Confidentiality—Policy—Transmission: An example of protecting the confidentiality of class information in transmission by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being transmitted. For instance, a policy may require that all transmission of confidential data over public networks must be encrypted.

Confidentiality—Education—Storage: An example of protecting the confidentiality of class information in storage by means of education would be to train students and faculty about which people have authorized access to the information in storage.

Confidentiality—Education—Processing: An example of protecting the confidentiality of class information being processed by means of education would be to train students and faculty to verify whether people are authorized to get the information before class starts by using a student ID or schedule.

Confidentiality—Education—Transmission: An example of protecting the confidentiality of class information being transmitted by means of education would be to train students and faculty to close classroom doors during a lecture so that others outside could not hear it.

Confidentiality—Technology—Storage: An example of protecting the confidentiality of class information being stored by means of technology would be using locks on file cabinets that contain the information while not in use.

Confidentiality—Technology—Processing: An example of protecting the confidentiality of class information being processed by means of technology would be forcing the use of electronic IDs during classes.

Confidentiality—Technology—Transmission: An example of protecting the confidentiality of class information being transmitted by means of technology would be having a password on a class Web site.

Integrity—Policy—Storage: An example of protecting the integrity of class information being stored by means of policy would be a simple rule that only certified people may alter the information.

Integrity—Policy—Processing: An example of protecting the integrity of class information being processed by means of policy would be a rule that forces students to study in quiet areas without the help of people who are not in the class.

Integrity—Policy—Transmission: An example of protecting the integrity of class information being transmitted by means of policy would be a rule that the teacher is not allowed to drink alcohol before class.

Integrity—Education—Storage: An example of protecting the integrity of class information being stored by means of education would be teaching people who store the information the names and roles of others who are authorized to change it.

Integrity—Education—Processing: An example of protecting the integrity of class information being processed by means of education would be informing students not to risk receiving incorrect information by studying with people who are not in the class.

Integrity—Education—Transmission: An example of protecting the integrity of class information being transmitted by means of education would be providing instructors with effective ways to teach.

Integrity—Technology—Storage: An example of protecting the integrity of class information being stored by means of technology would be electronically storing all data on a device that requires authorization to modify.

Integrity—Technology—Processing: An example of protecting the integrity of class information being processed by means of technology would be creating PowerPoint presentations to verify what the teacher says.

Integrity—Technology—Transmission: An example of protecting the integrity of class information being transmitted by means of technology would be printing the PowerPoint presentations and giving a copy to each student.

Availability—Policy—Storage: An example of protecting the availability of class information being stored by means of policy would be a policy that only authorized students are allowed access to certain stored information.

Availability—Policy—Processing: An example of protecting the availability of class information being processed by means of policy would be a rule that only authorized people are allowed to enter the classroom.

Availability—Policy—Transmission: An example of protecting the availability of class information being transmitted by means of policy would be a rule that only students are allowed into the classroom.

Availability—Education—Storage: An example of protecting the availability of class information being stored by means of education would be teaching correct storage processes so information doesn't get lost.

Availability—Education—Processing: An example of protecting the availability of class information being processed by means of education would be instructing those who teach the information to speak up so everyone in the classroom can hear.

Availability—Education—Transmission: An example of protecting the availability of class information being transmitted by means of education would be teaching students to remain quiet in the classroom so everyone can hear.

Availability—Technology—Storage: An example of protecting the availability of class information being stored by means of technology would be making the information available on the Internet via a password-protected Web site.

Availability—Technology—Processing: An example of protecting the availability of class information being processed by means of technology would be a teacher making PowerPoint files available to students via the Internet.

Availability—Technology—Transmission: An example of protecting the availability of class information being transmitted by means of technology would be a teacher using a microphone so lectures are loud enough for all students to hear.

2. Consider the information stored in your personal computer. Do you currently have information stored in your computer that is critical to your personal life? If that information became compromised or lost, what effect would it have on you? Answer: This will be unique to each student.

3. Using the Web, research Stuxnet. When was it discovered? What kind of systems does it target? Who created it and what is it used for? Answer: See Wikipedia at *https://en.wikipedia.org/wiki/Stuxnet*.

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

5. 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." Answer: Each student will prepare a unique response to this question.

6. 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. Answer: Each student will prepare a unique response to this question.

Chapter 1

Introduction to the Management of Information Security

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources

Lecture Notes

Overview

This chapter serves as an introduction to information security and project management. Students will learn about basic security concepts and organizational roles in relation to the protection of information. Different aspects of project management and its relationship with information security are discussed.

Chapter Objectives

After reading this chapter and completing the exercises, the student will be able to:

- List and discuss the key characteristics of information security
- List and describe the dominant categories of threats to information security
- Discuss the key characteristics of leadership and management
- Describe the importance of the manager's role in securing an organization's information assets
- Differentiate information security management from general business management

Teaching Tips

Introduction to Security

1. Discuss how the need for information security has increased over time, and explain its necessity within a business environment.

2. Point out that "information security" can sometimes be referred to as "InfoSec".

3. Explain that information security funding and planning decisions should involve three distinct groups of managers and professionals (communities of interest):
    a. Those in the field of information security
    b. Those in the field of IT
    c. Those from the rest of the organization

4. Provide information on the following communities of interest, and elaborate on how they work together to ensure information security:
    a. Information security community
    b. Information technology community
    c. General business community

5. Elaborate on the meaning of security and how being secure involves the use of risk assessment and management.

6. Explain the specialized areas of security, and discuss the role of management in ensuring that security is adequate:
    a. Physical security
    b. Operations security
    c. Communications security
    d. Cyber (or computer) security
    e. Network security

7. Introduce the Committee on National Security Systems (CNSS), which was formerly known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC), and discuss their role in creating security standards.

8. Explain that Information security (InfoSec) is the safeguarding of information and the means by which information is secured. Discuss the protection mechanisms mentioned in the text: policy, training and awareness programs, and technology.

9. Use Figure 1-1 to discuss how confidentiality, integrity, and availability are protected by proper information security.

CNSS Security Model

1. Discuss the CNSS NSTISSI No. 4011, "National Training Standard for Information Systems Security (InfoSec) Professionals" document.

2. Explain the McCumber Cube as a model showing the relationship between information characteristics, information location, and security control categories, and note its intended use in identifying issues with information security policies. Use Figure 1-2 in your discussion.

3. Elaborate on the use of a host intrusion detection and prevention system (HIDPS) for monitoring file access and deletion of data.

4. Discuss some of the drawbacks and weaknesses of the CNSS security model.

Teaching Tip	In contrast to intrusion detection systems, intrusion prevention systems are more proactive. Many network and host monitoring systems are combinations of intrusion prevention and intrusion detection systems.

The Value of Information and the C.I.A. Triad

1. Provide students with information on the use of the C.I.A. triangle, which is used to provide a basic model for information security.

2. Define confidentiality as the restriction of information to only authorized individuals with proper permissions, and discuss some of the different ways confidentiality is accomplished:
    a. Information classification
    b. Secure document and data storage
    c. Application of general security policies
    d. Education of information custodians and end users
    e. Cryptography

3. Point out some examples of disclosure that can occur either deliberately or by mistake. Discuss the possible repercussions of these examples of disclosure.

4. Integrity should be described as the preservation of data in its original, uncorrupted state. Educate students on some of the risks to data integrity, such as viruses or faulty transmission. Students should be aware of different methods to protect data integrity.

5. Explain to students how availability affects information security, and note that availability is applicable to users with proper permissions.

6. Point out that in the context of management of information systems, privacy does not mean freedom from observation but means that the information collected will be used only in ways approved by the person who provided it.

7. Define the term information aggregation as the collecting and combining of personal information from several different sources. Discuss how the trend of data collection can have negative effects on privacy.

8. Identification should be discussed as the way individual users are recognized in a system. Make students aware of how this is accomplished.

9. Detail how authentication is used in conjunction with a user's identification to establish a user's identity.

10. Authorization should be explained as the means by which a user is granted access to resources, and the extent of their allowed access.

11. Describe accountability as the ability to track each action on a system to a specific user identity or process running on the system.

Teaching Tip	More information about the CIA triangle, or triad, can be found below: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Key Concepts of Information Security: Threats and Attacks

1. Use Figure 1-4 to introduce students to the following key concepts in information security:
    a. Threat
    b. Attack
    c. Threat event
    d. Threat agent
    e. Exploit
    f. Vulnerability
    g. Information asset

2. Point out the agreement that the threat from external sources increases when an organization connects to the Internet.

The 12 Categories of Threats

1. Introduce students to the 12 general categories of threats that represent danger to an organization's people, information, and systems. Use Table 1-1 to discuss examples of each threat category.

2. Explain that intellectual property can be trade secrets, copyrights, trademarks, and patents. Discuss the efforts put in place to combat piracy of intellectual property.

3. Discuss the following two primary areas:
    a. Software piracy
    b. Copyright protection and user registration

4. Discuss the importance of providing quality of service by an organization. Point out that a degradation of service is a form of availability disruption and discuss the following subcategories of availability disruption:
    a. Internet service issues
    b. Communications and other service provider issues
    c. Power irregularities

5. Describe industrial espionage as the act of gathering information while employing techniques that cross a legal or ethical threshold. Compare this to competitive intelligence, which employ legal methods of accessing information stored in an information system.

6. Mention that the classic perpetrator of espionage or trespass is known as a hacker. Discuss the following classifications of hackers today:
    a. Expert hacker
    b. Professional hacker
    c. Novice hacker (script kiddie)

7. Explain that once an attacker gains access to a system, the next step is to increase his or her privileges, which is known as privilege escalation.

8. Discuss the act of jailbreaking, which is a common example of privilege escalation.

9. Point out that attempting to guess of reverse-calculate a password is often called cracking. Discuss the following types of password attacks:
    a. Brute Force
    b. Dictionary Attacks
    c. Rainbow Tables
    d. Social Engineering Password Attacks

10. Point out that forces of nature can sometimes disrupt the storage, transmission, and use of information. Describe some of the force of nature attacks many organizations face:
    a. Fire
    b. Flood
    c. Earthquake
    d. Lightning
    e. Landslide or mudslide
    f. Tornados or severe storms
    g. Hurricanes, typhoons, and tropical depressions
    h. Tsunami
    i. Electrostatic discharge (ESD)
    j. Dust contamination

11. Mention that the category of human error or failure includes acts performed without intent or malicious purpose or in ignorance by an authorized user. Describe the following examples of human error:
    a. Social Engineering
    b. Advance-fee Fraud
    c. Phishing (spear phishing and pretexting)

12. Discuss the concept of information extortion, which is also known as cyberextortion. Introduce students to a specialized form of malware known as ransomware.

13. Go over the recommendations on how to react when becoming a victim of ransomware.
    a. Do not pay the ransom
    b. Turn all devices off and disconnect from the network
    c. Find the source of the infection
    d. Alert all users
    e. Restore from a backup to a new device
    f. Reimage the infected systems

14. Explain to students that the category of sabotage involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy an asset or damage the image of an organization.

15. Discuss the following types of sabotage:
    a. Online Activism
    b. Cyberterrorism and Cyberwarfare
    c. Positive Online Activism

16. Point out that malware is also referred to as malicious code or malicious software. Discuss the following attack vectors used to exploit vulnerabilities:
    a. Virus
    b. Worms
    c. Trojan horses
    d. Polymorphic threats
    e. Virus and worm hoaxes

17. Explain that an attacker may attempt to gain access to a system or network resource through a back door. Discuss how this is possible.

18. Point out that in a denial-of-service (DOS) attack, the attacker sends a large number of connection or information requests to a target in order to cause the system to crash or be unable to perform ordinary functions.

19. Explain that a distributed denial-of-service (DDoS) attack is a coordinated stream of requests launched against a target from many locations at the same time.

20. Discuss the following types of email attacks:
    a. spam
    b. wire fraud solicitations
    c. malware attachments
    d. clickbait
    e. mailbomb

21. Examine the following forms of communication interception attacks:
    a. Packet sniffer
    b. Spoofing
    c. Pharming
    d. Man-in-the-middle

22. Explain to students that technical hardware failures occur when a manufacturer distributes equipment containing a known or unknown flaw.

23. Be sure to point out the difference between the terms mean time between failures (MTBF) and mean time to failure (MTTF). Discuss the acronyms related to the repair of failures: mean time to diagnose (MTTD) and mean time to repair (MTTR).

24. Discuss technical software failures with your students. Be sure to mention that software bugs are so commonplace that entire Web sites are dedicated to documenting them.

25. Introduce and explain the four categories of the "deadly sins of software security":
    a. Web application sins
    b. implementation sins
    c. cryptographic sins
    d. networking sins

26. Explain to students that antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Point out that management's strategic planning should always include an analysis of technology currently in use.

27. Mention to students that theft is an ever-present threat to an organization. Explain that theft is often an overlapping category with software attacks, espionage or trespass, information extortion, and compromises to intellectual property.

Quick Quiz 1

1. True or False: Data integrity can be affected by virus infections and data communications errors.
   Answer: True

2. What is the name of the process that is used to establish whether or not a user's identity is legitimate?
   A. Availability
   B. Accountability
   C. Authorization
   D. Authentication
   Answer: D

3. Which of the following terms can be used to describe trade secrets, copyrights, trademarks, and patents?
   A. Quality of service
   B. Availability
   C. Intellectual property
   D. Competitive intelligence
   Answer: C

4. A person who has authorization from an organization to test its information systems and network defense is known as which of the following?
   A. script kiddie
   B. penetration tester
   C. professional hacker
   D. packet monkey
   Answer: B

5. What type of malware actually evolves, changing its size and other external file characteristics to elude detection by antivirus programs?
   A. Trojan horse
   B. trap door
   C. polymorphic threat
   D. macro virus

   Answer: C

Management and Leadership

1. Inform students on the proper management of information security, and discuss the following management roles:
   a. Informational role
   b. Interpersonal role
   c. Decisional role

2. Compare leadership to management, and discuss the roles of a leader in accomplishing information security goals.

Behavioral Types of Leaders

1. Compare the three different types of leaders, and familiarize students with the advantages and disadvantages of each type:
   a. Autocratic
   b. Democratic
   c. Laissez-faire

Teaching Tip	Many more personality types for leadership exist than are mentioned in this chapter. For a list of additional personality types, see: https://www.psychologyjunkie.com/2017/06/28/leadership-skills-every-myers-briggs-personality-type/

Management Characteristics

1. Elaborate on the traditional management theory, which uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC)

2. Compare the popular management theory to the traditional management theory, and note that it uses the core principles of planning, organizing, leading, and controlling (POLC).

3. Explain the planning process, and note the three different levels of planning:
    a. Strategic planning
    b. Tactical planning
    c. Operational planning

4. Define a goal as the result of a planning process, and explain objectives as a means to measure progress towards a goal.

5. Explain the organizing process of management involves the structuring of resources to support accomplishing objectives.

6. Re-iterate the importance of the leadership role in the planning and organization functions.

7. Discuss the control function of management as involving the monitoring of a task by management personnel. Students should understand how cybernetic control, or negative feedback loops are used. Use Figure 1-8 in your discussion.

Governance

1. Define the governance as the level of uppermost management. Further explain that governance emphasizes escalating the importance of InfoSec to the uppermost levels of the organization.

2. Note that regulatory compliance is the set of actions an organization undertakes to assure government and other evaluators that is in compliance with governmental or industry laws, regulations, or standards.

Solving Problems

1. Provide students with an overview of the 5-step process for solving problems, and give examples of basic use.

2. Step 1 should be explained as involving the identification of a specific issue or problem.

3. Step 2 should be shown as the step where information about an issue is gathered, and where assumptions are made in regards to the issue.

4. Step 3 involves the development of possible solutions to an issue. Provide students with information on how managers may attempt to gather and generate ideas.

5. Step 4 should be discussed as the step when solutions are evaluated for their potential in solving a specific problem. List some of the different feasibility metrics that may be used to determine potential success of a solution:
    a. Economic feasibility

b. Technological feasibility
c. Behavioral feasibility
d. Operational feasibility

6. Step 5 is the step at which a solution is selected, implemented, and then evaluated for effectiveness in solving a problem.

Principles of Information Security Management

1. Elaborate on the goals of the information security management team, and discuss how these goals may conflict with the goals of an IT management team.

2. Discuss the "six Ps" of information security management: planning, policy, programs, protection, people, and project management.

Planning

1. Describe how a business strategy dictates the development of an IT strategy, which is then used to develop an information security strategy. Provide students with a general understanding of how this is typically accomplished in an organization.

2. List some of the different types of information security plans and planning functions that exist:
   a. Incident response
   b. Business continuity
   c. Disaster recovery
   d. Policy
   e. Personnel
   f. Technology rollout
   g. Risk management
   h. Security program

Policy

1. Discuss the three different general policy categories, and explain how each is used:
   a. Enterprise information security policy (EISP)
   b. Issue-specific security policies (ISSPs)
   c. System-specific policies (SysSPs)

Programs

1. Explain the existence of information security programs, and specifically mention the security education training and awareness (SETA) program, and how it provides training to employees in order to increase security awareness.

Protection

1. Describe how the protection function is accomplished through risk management activities.

People

1. Emphasize the importance of people in an information security program, and note how this includes security personnel and security of personnel.

Projects

1. The project function should be explained as involving project management, which involves the application of resources to a specific project and the monitoring of its progress.

Quick Quiz 2

1. Which is NOT one of the core principles in traditional management theory?
   A. Staffing
   B. Leading
   C. Directing
   D. Controlling

   Answer: B

2. What is the name for an intermediate point in a planning process, at which progress towards a goal can be measured?
   A. Break point
   B. Stop point
   C. Objective
   D. Directive

   Answer: C

3. Which management function is dedicated to the structuring of resources to support the accomplishment of objectives?
   A. Organizing
   B. Controlling
   C. Planning
   D. Leading

   Answer: A

4. Which of the following involves assessing the likelihood that subordinates will adopt and support a particular solution rather than resist it?
   A. Economic Feasibility
   B. Technological Feasibility
   C. Behavioral Feasibility
   D. Operational Feasibility

   Answer: C

5. In which of the following policies would you find sets of rules that define acceptable behavior within a specific organizational resource, such as Internet usage?
   A. System-Specific Policies
   B. Issue-Specific Security Policies
   C. Enterprise Information Security Policy
   D. Security Awareness Policy

   Answer: B

Class Discussion Topics

1. Start a class discussion about which leadership role students believe would be most effective in assisting with project completion, and require that students justify their opinion.

2. Give students time to discuss what types of security should be considered when dealing with information security as a whole. Which areas of security might be more critical than others?

Additional Projects

1. Have students research at least 3 of the leading anti-malware programs available today. Students should compare features offered by each of the 3 programs and write a recommendation on which anti-malware program they feel an organization should use to protect information technology resources.

2. Task students with researching the different types of management approaches. Students should write down the defining features of several different types of management, then share them with the class.

Additional Resources

1. Information Security Threats: http://searchsecurity.techtarget.com/resources/Information-Security-Threats

2. Review article on the McCumber Cube: https://www.revolvy.com/main/index.php?s=McCumber%20cube

3. C.I.A. Triad: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

4. Best Malware Protection Software of 2018: https://www.pcmag.com/roundup/354226/the-best-malware-removal-and-protection-tools

5. 5 Tips to Improve Your Defenses Against Social Engineering Attacks: https://www.tripwire.com/state-of-security/security-awareness/5-tips-against-social-engineering/

Key Terms

For definitions of key terms, see the Glossary near the end of the book.