Chapter 1 Answers to Review Questions and Exercises

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 the most common violation of intellectual property? How does an organization protect against it? What agencies fight it? Answer: 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).

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 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 towards a common goal. Leading: the process of arousing enthusiasm and directing human resource efforts towards 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.

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 2016. 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.