Contents

[1. Chapter 1 1](#_Toc158652735)

[1.1. Review Questions 1](#_Toc158652736)

[2. Chapter 2 6](#_Toc158652737)

[2.1. Review Questions 6](#_Toc158652738)

# Chapter 1

## Review Questions

1. **What is the difference between a threat agent and a threat?**

A threat agent is the facilitator of an attack, whereas a threat is a category of objects, persons, or other entities that represents a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences and others are purposeful. Fire is a threat; however, a fire that has begun in a building is an attack. If an arsonist set the fire, then the arsonist is the threat agent. If an accidental electrical short started the fire, the short is the that agent.

1. **What is the difference between vulnerability and exposure?**

Vulnerability is a weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Exposure is a condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

1. **How is infrastructure protection (assuring the security of utility services) related to information security?**

The availability of information assets is dependent on having information systems that are reliable and that remain highly available.

1. **What type of security was dominant in the early years of computing?**

In the early years of computing when security was addressed at all, it dealt only with the physical security of the computers themselves and not the data or connections between the computers. This led to circumstances where most information being stored on computers was vulnerable since information security was often left out of the design phase of most systems.

1. **What are the three components of the CIA triangle? What are they used for?**

The three components of the C.I.A are:

* confidentiality (assurance that the information is shared only among authorized persons or organizations);
* integrity (assurance that the information is complete and uncorrupted); and
* availability (assurance that the information systems and the necessary data are available for use when they are needed).

These three components are frequently used to conveniently articulate the objectives of a security program that must be used in harmony to assure an information system is secure and usable.

1. **If the C.I.A. triangle is incomplete, why is it so commonly used in security?**

The CIA triangle is commonly used in security because it addresses the fundamental concerns of information: confidentiality, integrity, and availability. It is still used when not complete because it addresses all of the major concerns with the vulnerability of information systems.

1. **Describe the critical characteristics of information. How are they used in the study of computer security?**

The critical characteristics of information define the value of information. Changing any one of its characteristics changes the value of the information itself. There are seven characteristics of information:

* Availability enables authorized users either persons or computer systems-to access information without interference or obstruction, and to receive it in the required format.
* Accuracy occurs when information is free from mistakes or errors and it has the value that the end user expects.
* Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred
* Confidentiality is achieved when disclosure or exposure of information to unauthorized individuals or systems is prevented. Confidentiality ensures that only those with the rights and privileges to access information are able to do so.
* Integrity of information is maintained when it is whole, complete, and uncorrupted.
* Utility of information is the quality or state of that information having value for some purpose or end. Information has value when it serves a particular purpose. Possession of information is the quality or state of ownership or control of seme object or item. Information is said to be in one's possession if one obtains it, independent of format or other characteristics.

1. **Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?**

The six components are software, hardware, data, people, procedures, and networks. People would be impacted most by the study of computer security. People can be the weakest link in an organization's information security program. And unless policy. education and training, awareness, and technology are properly employed so prevent people from accidentally or intentionally damaging er losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system

Procedures, written instructions for accomplishing a specific task, could be another component, which will be impacted. The information system will be effectively secured by teaching employees to both follow and safeguard the procedures. Following procedure reduces the likelihood of employees erroneously creating information insecurities. Proper education about the protection of procedures can avoid unauthorized access gained using social engineering Hardware and software are the components that are historically associated with the study of computer security. However, the IS component that created much of the need for increased computer and information security is networking.

1. **What system is the predecessor of almost all modern multiuser systems?**

MULTICS

1. **Which paper is the foundation of all subsequent studies of computer security?**

Rand Report R-609, sponsored by the Department of Defense.

1. **Why is the top-down approach to information security superior to the bottom-up approach?**

The top-down approach, in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action, has a higher probability of success. This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

1. **Why is a methodology important in the implementation of information security? How does a methodology improve the process?**

A methodology is a formal technique that has a structured sequence of procedures that is used to solve a problem. Methodology is important in the implementation of information security because it ensures that development is structured in an orderly, comprehensive fashion. The methodology unifies the process of identifying specific threats and the creation of specific controls to counter these threats into a coherent program. Thus, a methodology is important in the implementation of information security for two main reasons.

* First, it entails all the rigorous steps for the organizations' employees to follow, therefore avoiding any unnecessary mistakes that may compromise the end goal (ie, to have a comprehensive security posture). An example of this is that a methodology guides an organization to solve the root cause of the information security problem, not just in symptoms.
* Second, methodology increases the probability of success. Once a methodology is adopted, the personnel selected will be responsible for establishing key milestones and made accountable for achieving the project goals.

The methodology can greatly improve the process. For example, following the six steps of the SDLC (Systems Development Life Cycle) (investigation, analysis, logical design. physical design, implementation, and maintenance and change) allows developments to proceed in an orderly, comprehensive fashion. Individuals or groups assigned to do the analysis step do not have to initiate their work until the investigation step is completely finished. Moreover, each step of the methodology may determine whether the project should be continued, discontinued, outsourced, or postponed. For example, the physical design step may need to be postponed or outsourced if the organization does not possess the technology needed.

1. **Which members of an organization are involved in the security system development life cycle? Who leads the process?**

Initiation and control of the SecSDLC is the responsibility of upper management Responsible managers, contractors and employees are then utilized to execute the SecSDLC. The process is usually led by a senior executive, sometimes called the champion, that promotes the project and secures financial, administrative, and companywide backing of the project, then a project manager is assigned the task of managing the project.

1. **How can the practice of information security be described as both an art and a science? How does security as a social science influence its practice?**

The practice of information security is a never-ending process. An effective information security practice must be considered as a tripod that relates to three important aspects (science, art, and social science):

* First, information security is a science because it requires various kinds of tools and technologies used for technical purposes. It can also include sound information security plans and policies that may dictate the needs of particular technologies
* Second, information security is also an art because there are no clear-cut rules on how to install various security mechanisms. Different factors such as budgets, time, threats, risks, vulnerabilities, and asset values can significantly affect the numbers and types of passive and active controls an organization needs. The overall goal is for the organization to have a sound information security posture that can reduce the risks of being attacked as much as possible.
* Third, and most importantly, information security must be looked at as a social science mainly because social science deals with people, and information security is primarily a people issue, not a technology issue. Though the eye of a social scientist, an organization can greatly benefit from the Security Education Training, and Awareness program (SETA), which can help employees (1) understand how to perform their jobs more securely, (2) be fully aware of the security issues within the organization, and (3) be accountable for their actions.

Therefore, information security must be viewed as having all three natures, with the most emphasis on the social science perspective. After all people are the ones who make the other five components of information assets (software, hardware, data, procedures and networks) possible.

1. **Who is ultimately responsible for the security of information in the organization?**

The Chief Information Security Officer (CISO) is primarily responsible for the assessment, management, and implementation of information security in the organization. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two. However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals.

1. **What is the relationship between the MULTICS project and early development of computer security?**

MULTICS, Multiplexed Information and Computing Service, was the first operating system created with security as its primary goal. It was a mainframe, time-sharing operating system developed through a partnership between GE, Bell Labs and MIT. Much of the early focus for research on computer security was centered on this system.

1. **How has computer security evolved into modern information security?**

Before the creation and use of networking technologies computer security consisted of securing the physical location of the system by the use of badges, keys and facial recognition. With the creation of ARPANET and the increasing popularity of networked systems, it was no longer adequate to merely physically secure a system. In order to insure total security, the information itself, as well as the hardware used to transmit and store that information, needed to be addressed. Information security developed from this need. Eventually, computer security became just another component of information security.

1. **What was important about Rand Report R-609?**

The movement toward security that went beyond protecting physical locations began with the Rand Report R-609, a paper sponsored by the Department of Defense. This report attempted to address the multiple controls and mechanisms necessary for the protection of a multilevel computer system. In addition, the Rand Report was the first to identify the role of management and policy issues in the expanding area of computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper signaled a pivotal moment in computer security history ---- when the scope of computer security expanded significantly from the safety of physical locations and hardware to include securing the data, limiting random and unauthorized access to that data, and involving personnel from multiple levels of the organization in matters pertaining to information security.

1. **Who decides how and when data in an organization will be used and or controlled? Who is responsible for seeing these wishes are carried out?**

The three types of data ownership and their respective responsibilities are

Data owners: Those responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOS. The data owners usually determine the level of data classification (discussed later) associated with the data, as well as the changes to that classification required by organizational change. The data owners work with subordinate managers to oversee the day-to-day administration of the data.

Data custodians: Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups. implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the owner

Data users: End users who work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

1. **Who should lead a security team? Should the approach to security be more managerial or technical**

A project manager, who may be a departmental line manager or staff unit manager would lead a security team. Typically, that person would understand project management personnel management, and information security technical requirements. The approach to security should be more managerial than technical, although, the technical ability of the resources actually performing the day-to-day activities is critical. The top-down approach to security implementation is by far the best. It has strong upper management support, a dedicated champion, dedicated funding, clear planning and the opportunity to influence organizational culture.

# Chapter 2

## Review Questions

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

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

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

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

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

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

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

General management, IT management, and information security management are each responsible for implementing information security that protects the organization's ability to function. Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, implementing information security actually has more to do with management than technology. Just as managing payroll involves management more than mathematical wage computations, managing information security has more to do with policy and its enforcement than the technology of its implementation.

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

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

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

When an attacker can control access to an asset, it can be held hostage to the attacker's demands. For example, if attackers gain access to a database and then encrypt its data, they may extort money or other value from the owner by threatening to share the encryption key and the data with others.

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

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

1. **How can you protect against shoulder surfing?**

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

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

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

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

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

An expert hacker develops software scripts and codes to exploit relatively unknown vulnerabilities. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems. Unskilled hackers use scripts and code developed by skilled hackers. They rarely create or write their own hacks, and are often relatively unskilled in programming languages, networking protocols, and operating systems.

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

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

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

Computer viruses are segments of code that induce other programs to perform actions. Worms are malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication. Once a trusting user executes a Trojan horse program, it unleashes viruses or worms to the local workstation and the network as a whole.

1. **Why does polymorphism cause greater concern than traditional malware? How does it a it affect detection?**

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

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

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

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

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

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

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

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