**Chapter 2 Answers to Review Questions and Exercises**

# [A HD]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 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 (SIIA) 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.

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

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 Technological obsolescence occurs when infrastructure becomes outdated, which leads to unreliable and untrustworthy systems.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

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 Once discovered, outdated technologies must be replaced.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

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

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

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

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

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

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

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

To protect against password attacks, security administrators can:

* Implement controls that limit the number of attempts allowed.
* Use a “disallow” list of passwords from a similar dictionary.
* Require use of additional numbers and special characters in passwords.
1. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?

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

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

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

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

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

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

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

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

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

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

# [A HD]Exercises

1. Consider that an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker breaks into a network, copies a few files, defaces a Web page, and steals credit card numbers, how many different threat categories does the attack fall into?
* Deliberate acts are the main threat category for this type of attack because the hacker is deliberately trying to cause harm. This attack could fall under different subcategories, such as deliberate acts of espionage or trespass, deliberate acts of sabotage or vandalism, and deliberate acts of theft.
* Compromises to intellectual property—copying files, defacing a Web page, and stealing credit card numbers.
* Technical failures. For instance, if part of the organization’s software has an unknown trap door, this type of hacker attack could occur.
* Management failure. This type of hacker attack could happen if management used insufficient planning and foresight to anticipate the technology need for evolving business requirements.
1. Using the Web, research Mafiaboy’s exploits. When and how did he compromise sites? How was he caught?

Mafiaboy’s exploits consisted of a series of DDoS attacks on 11 corporate networks. According to investigators, the attacks caused approximately $1.7 billion in losses to the companies, although the accuracy of that figure is disputed. The attacks made some corporate Web sites and networks difficult to reach. In other cases, they crashed completely, remaining offline from hours to several days. Because the attacks were so large, authorities were prompted to investigate. They found that someone by the name of Mafiaboy was bragging about the attacks on Web sites, message boards, and even his own site. In addition, authorities were able to associate an IP address to the attacks, which in turn was linked to an Internet service provider (ISP). With the ISP’s help, authorities linked the IP address to an account whose phone numbers were linked to Mafiaboy’s father.

**Alternate Answer**

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

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

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

1. Search the Web for “The Official Phreaker’s Manual.” What information in this manual might help a security administrator to protect a communications system?

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

Security administrators could benefit from studying “The Official Phreaker’s Manual” because it could allow them to better protect their communications systems. From the system administrator’s point of view, this information could reveal many common ways of finding loopholes and alternate methods around communications system security measures. The manual could also help system administrators use different approaches in implementing a more extensive security program.

1. 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*](http://www.securityfocus.com/%20) and use a keyword search on “threats.”

Possible results are:

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

Answers will vary.