# Week 1 Hands On

Eric Vara

The University of Arizona Global Campus

System Administration & Security (CYB - 300)

Instructor Bipin Bhatt

21, November 2022

## Part One

### Module 01: Introduction to Information Security Review Questions

1. What is the difference between a threat agent and a threat source?
   * Answer: A threat agent is a person facilitating an attack, and threats pose an ongoing threat to assets.
2. What is the difference between vulnerability and exposure?
   * Answer: System weaknesses such as B. Holes in software packages, unprotected doors, or unprotected system ports are called vulnerabilities. It exposes objects to damage and attacks. The system is only susceptible to damage during exposure. Exposure itself can be caused by vulnerability.
3. What is a loss in the context of information security?
   * Answer: In the context of information security, the impact is loss of confidentiality, integrity, or availability or all other possible losses. It`s not possible to identify nor mitigate all risks. This remaining risk is called residual risk.
4. What type of security was dominant in the early years of computing?
   * Answer: Because computing was not hyper-connected and usage required being physically present at the computing device, physical security predominated.
5. What are the three components of the C.I.A. triad? What are they used for?
   * Answer: The CIA triad, also known as confidentiality, integrity, and availability, is a concept created to direct information security policies inside a company. To avoid confusion with the Central Intelligence Agency, the approach is sometimes frequently referred to as the AIC triad (availability, integrity, and confidentiality).
6. If the C.I.A. triad is incomplete, why is it so commonly used in security?
   * Answer: Because it solves the main issues with the vulnerability of information systems, the CIA triangle is still in use.
7. Describe the critical characteristics of information. How are they used in the study of computer security?
   * Answer: Information's value is determined by its essential properties. The value of the information itself can be altered by changing any one of its qualities.
8. Identify the components of an information system. Which of the components are most directly affected by the study of computer security?
   * Answer: Networks, people, procedures, hardware, software, and data. The study of information security has a direct impact on data, software, networks, and procedure. The most prevalent concepts in the study of security are data and software.
9. What is the McCumber Cube, and what purpose does it serve?
   * Answer: The McCumber Cube, which bears the name of its inventor, John McCumber, demonstrates how the many elements of information security are interconnected. You may view availability, integrity, and confidentiality on one side. All three of these include crypto in a significant way.
10. Which paper is the foundation of all subsequent studies of computer security?
    * Answer: All future research on computer security is built on Rand Report R-609, which was funded by the Department of Defense.
11. Why is the top-down approach to information security superior to the bottom-up approach?
    * Answer: Upper management doesn't back the bottom-up strategy. The top-down strategy provides clearer planning, increased funds, and backing from upper management. 12. What are the benefits of using a methodology while implementing information security? What ways does a methodology enhance the operation?
12. Describe the need for balance between information security and access to information in information systems.
    * Answer: Since information security can never be completely guaranteed, a perfect balance between accessibility and security must be maintained. Free access to a piece of information would be detrimental, and it would be challenging to impose any accessibility restrictions.
13. How can the practice of information security be described as both an art and a science? How does the view of security as a social science influence its practice?
    * Answer: Because it requires a variety of tools and technologies that are utilized for technical objectives, information security is first and foremost a science. Because there are no set guidelines for how to implement different security methods, information security is also an art.
14. Who is ultimately responsible for the security of information in the organization?
    * Answer: The CISO of a corporation is the advocate for data security within the company. The incumbent of this position is in charge of developing the policies and strategies to protect data from threats and vulnerabilities as well as the reaction strategy in case the worst case scenario occurs.
15. What is the relationship between the MULTICS project and the early development of computer security?
    * Answer: The operating system was the first to be developed with security as its top priority. Several important engineers began working on UNIX, which did not require the same level of security, soon after MULTICS was reorganized.
16. How has computer security evolved into modern information security?
    * Answer: The physical location of a system was protected using badges, keys, and facial recognition as part of computer security. The information itself, as well as the hardware used to transmit and store it, needs to be safeguarded in order to guarantee complete security.
17. What was important about RAND Report R-609?
    * Answer: It was a paper about securing real estate that the Department of Defense sponsored. It was the first to recognize management's function in advancing the field of helicopter security. The widespread use of networking components significantly reduced the introduction of military risks.
18. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these decisions are carried out?
    * Answer: Data ownership and use are under the control of the data owners, who decide how and when the data will be used, while users interact with the data on a daily basis.
19. Who should lead a security team? Should the approach to security be more managerial or technical?
    * Answer: The team should be led by security specialists or professionals. As opposed to technology, managers are better at making and implementing choices, hence security should be approached more managerially.
20. Besides the champion and team leader, who should serve on an information security project team?
    * Answer: Because they are the ones who understand the authority culture, structures, and requirements for developing and implementing effective ways, security policy developers.

### Module 02: The Need for Security Review Questions

1. Why is information security a management problem? What can management do that technology cannot?
   * Answer: To safeguard the organization's ability to function, information security must be implemented by both general management and IT management. Making wise policy judgments and enforcing decisions that have an impact on applications and the IT infrastructures that support them are the responsibility of management.
2. Why is data the most important asset an organization possesses? What other assets in the organization require protection?
   * Answer: Data is crucial to a company because without it, it would be unable to keep track of transactions and/or provide value to its clients. Protecting data in motion and data at rest are equally important because every company, academic institution, or governmental organization that operates within the contemporary social environment of connected and responsive services depends on information systems to support these services.
3. Which management groups are responsible for implementing information security to protect the organization’s ability to function?
   * Answer: Information security management, general management, and IT management.
4. Has the implementation of networking technology, such as the cloud, created more or less risk for businesses that use information technology? Why?
   * Answer: Networking is typically thought to entail increased risk for information technology-using enterprises. This is because networked information systems, particularly those connected to the Internet, give potential attackers more and easier access to these systems.
5. What is information extortion? Describe how such an attack can cause losses, using an example not found in the te411xt.
   * Answer: When an attacker has access to an asset, they can force it to comply with their demands. For instance, if an attacker is able to access a collection of data in a database and encrypt that data, they may demand money or another valuable resource from the owner in exchange for disclosing the encryption key, allowing the owner to use the data.
6. Why are employees among the greatest threats to information security?
   * Answer: Since they are closest to the organizational data and will have access as a result of their duties, employees pose the most threats. Employee errors seriously jeopardize the security, integrity, and accessibility of data because they are the ones who use it in daily activities.
7. How can you protect against shoulder surfing?
   * Answer: The easiest strategy for someone to prevent shoulder surfing is to steer clear of accessing private information while another person is around, if at all possible.
8. How has the perception of the hacker changed over recent years? What is the profile of a hacker today?
   * Answer: The traditional idea of a hacker is commonly romanticized in fictional works as someone who cunningly works their way through a labyrinth of computer networks, systems, and data to discover the knowledge that solves the problem presented in the plot and saves the day.
9. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?
   * Answer: A skilled hacker is one who creates software scripts and routines to take advantage of undiscovered weaknesses. A master of numerous programming languages, networking protocols, and operating systems characterizes the skilled hacker. One who employs scripts and code created by skilled hackers is considered an unskilled hacker.
10. What are the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?
    * Answer: Viruses, worms, Trojan horses, logic bombs, and back doors are typical forms of malware. Code fragments known as computer viruses cause other programs to act in a certain way. Worms are harmful programs that continuously duplicate themselves without the aid of another program to create a secure environment. When a Trojan horse program is run by a trusted user, it spreads viruses or worms over the entire network as well as the local workstation.
11. Why does polymorphism cause greater concern than traditional malware? How does it affect detection?
    * Answer: Because polymorphism makes harmful code more evasive, it raises more concerns.
12. What is the most common violation of intellectual property? How does an organization protect against it? What agencies fight it?
    * Answer: The most frequent infractions are software piracy, which is the illegal use or replication of intellectual property based on software. Some businesses have employed copyright codes, digital watermarks, embedded code, faulty sectors purposefully placed on software media, and other security methods. Most businesses also register their patents, trademarks, or copyrights, which enables them to take legal action against anyone who violates them.
13. 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?
    * Answer: Fire, flood, earthquake, lightning, mudslides, tornadoes, strong winds, hurricanes, typhoons, tsunamis, electrostatic discharge (ESD), and/or dust contamination are all examples of force majeure. Dust pollution can be a top worry for a Las Vegas company. Oklahoma City, OK, is concerned about tornadoes. Hurricanes or tsunamis would cause the most anxiety in Miami, Florida. Los Angeles would be concerned about riots, wildfires, mudslides, and earthquakes.
14. How is technological obsolescence a threat to information security? How can an organization protect against it?
    * Answer: Management's probable lack of foresight and failure to foresee the technology needed for changing company requirements can result in technological obsolescence, which poses a security risk. When infrastructure ages, it becomes technologically obsolete, which results in unreliable and untrustworthy systems. As a result, assaults run the risk of compromising data integrity.
15. Does the intellectual property owned by an organization usually have value? If so, how can attackers threaten that value?
    * Answer: Yes, a company's intellectual property (IP) could be its most valuable asset. By deleting or restricting the asset's availability to the owner or by stealing and then selling copies of the asset, attackers can jeopardize its economic worth.
16. What are the types of password attacks? What can a systems administrator do to protect against them?
    * Answer: There are three different kinds of password attacks: dictionary, brute force, and password crack. Security managers can implement restrictions that restrict the number of attempts permitted, employ a "disallow" list of passwords from a related dictionary, and mandate the usage of additional numbers and special characters in passwords to safeguard against password attacks.
17. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?
    * Answer: When an attacker floods a target with connection or information requests, a denial-of-service attack occurs. When multiple locations simultaneously launch a coordinated stream of requests against a target, this is known as a distributed denial-of-service attack.
18. 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?
    * Answer: In order to install the sniffer, the attacker must first acquire access to a network. The most effective method for an attacker to enter a network and set up a physical sniffer device is through social engineering.
19. What methods would a social engineering hacker use to gain information about a user’s login ID and password? How would these methods differ depending on the user’s position in the company?
    * Answer: The practice of using social skills to acquire credentials for access or other useful information is known as social engineering. As an illustration, attackers may pretend to be in positions of power and ask for information through role playing. Other strategies include putting malicious malware on user computers to obtain access information and employing deceit to manipulate users' consciences.
20. What is a buffer overflow, and how is it used against a Web server?
    * Answer: When a buffer receives more data than it can hold, a buffer overflow occurs. When the two entities involved in the communication process have different processing rates, it can happen over a network.4

## Part Two

### Hands-On Project: Web Browser Security

Complete the Hands-On Project: Web Browser Security

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Which browser(s) did you improve the security and privacy for? (Check all that you performed.)

* Google Chrome
* Mozilla Firefox
* Microsoft Edge
* Apple Safari

Were you able to access all the security and privacy features of the browsers you used?

* Yes
* No (explain what you could not revise)

Do you feel more equipped to make your browser experience more secure?

* Yes
* No

Please explain: Chrome is quick and simple to use, but it's not secure because Google collects all user data and makes recommendations based on past behavior in the background. Sometimes recommending the preference is helpful. Additionally, Chrome uses a lot of RAM because each tab operates in its own thread, which uses a lot of memory. The other applications can hang if your device doesn't have a lot of memory. The alternative is the best you can come up with.

### Hands-On Project: Ethics in IT and Detecting Phishing E-mails

Complete the Hands-On Project: Ethics in IT and Detecting Phishing E-mails

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

In the space below, write a brief statement indicating your intention to abide by the ethics codes spelled out in this lab.

|  |
| --- |
| I learned and implemeneted steps to configure the secuirty and privaicy settings in Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari to optimize personal broswer safety settings. I went with enchanced safe mode to secure web browsering to beteter secure my broswer and other broswer tools like extentions. |