CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #2 - Option A

Team: Seven
Participants: Jackson Dillingham, Matt Jackson, Hilton Siaffa, Tabor Payne, and Emily Wantland

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the two options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
Why is information security a management problem? What can management do that technology alone cannot? *(5 points)*

- Information security is a management problem because they are the ones responsible for the authorization of new policies. They implement new technology and security that protects the organization. The policies must be enforced, or they will not work. Management makes the decisions that impact the organization, so they must comply with technology standards. They must view security needs from a business standpoint, and factor in human error and failure. This is the risk management aspect; technology alone cannot account for it. They must look at the infrastructure and make informed decisions that support security.

Problem 2
Why do employees constitute one of the greatest threats to information security that an organization may face? *(5 points)*

- Employees constitute one of the greatest threats to information security because they are hands-on users that interact with data. Due to the nature of their positions, they are active within the system, this can lead to deleting data they did not mean to, entering incorrect values, or using unsafe practices. Building on that, they are targets for hackers since they have access. An employee can be the target of social engineering which can compromise a system. Employees endanger the confidentiality of data, even when trained.

Problem 3
How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? Describe two other common controls that can also reduce this threat? *(5 points)*

- Dual controls essentially entail a security measure requiring two confirmation steps. In other words, two-factor authentication. This is when credentials are entered and the user has previously chosen to receive a phone call, a text, or an email that they will respond to which confirms their identity. This can help keep systems secured because if an external individual tries to log in, they might not be able to complete the second step. A common

control includes validation, when a user inputs a value that is not supported, they will be warned. Another would be backing up user data, saving a copy can prevent future loss.

Problem 4

What is the difference between a regular denial of service (DoS) attack and a distributed denial of service (DDoS) attack? Which is harder to combat? Why? *(5 points)*

- A regular denial-of-service (DoS) attack is when an attacker attempts to overwhelm a computer's ability to handle incoming communications. They do this by sending a large number of connection or information requests to a target. This prohibits users from accessing the system. This type of attack is launched from a single location. A distributed denial-of-service (DDoS) attack is a coordinated event that is launched against a targeted system. In contrast, these attacks come from many locations at the same time. They employ bots or zombies to carry it out.
- We believe a DDoS attack is harder to combat. It's difficult to determine where the attack originated from as it appears to be from several locations at once. Numerous bots or zombies are used, and there are no simple strategies to defend against these attacks.

Problem 5

Briefly describe the types of password attacks addressed in Chapter 2 of your text? Describe three controls a systems administrator can implement to protect against them? *(5 points)*

- Password attacks come in many forms. These forms include the brute-force attack, which is trying every possible combination until it succeeds. The dictionary attack uses common dictionary words that are used as passwords and trying them one at a time. The rainbow table attack uses a table that shows the hash values of pre-matched plaintext words, which essentially allows "reverse hashing." Lastly, hackers use social engineering which involves taking advantage of the human element. Basically, the hacker will trick the unsuspecting victim into giving up information without them realizing it.
- In order to combat these attacks, admins can set password requirements when users are setting up their accounts. Moreover, they can implement multi-factor authentication and they can train employees to be more cautious with sensitive information, such as passwords. Training can be informing users not to give out passwords over email or over the phone, covering their screens, etc.