CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #2 - Option A

Team: 5
Participants: Ethan Grimes, Holli Grubbs, James Hoagland, Gregory Ellis

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)*

Both general and IT management are responsible for facilitating and advancing security programs. Information security can be a management problem because if you are looking at it from the perspective of a top-down approach, it starts with management. Management is always the one mainly implementing information security for protection because they know the company the best. Information security is also a management problem because as a manager of information security, and like other management positions in different industries, you are mainly dealing with enforcing policy and bringing awareness to different risks that can occur. As managers enforce policy to protect information it becomes clear that without management the technology would be less secure.

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

Employees are one of the greatest threats to information security because they may have access to intellectual property, and therefore have the potential to damage, harm, or steal it. They are also the closest to the information. Human error with information security involves acts performed either without malicious intent, or ignorance. A few causes of human error with employees include inexperience, poor training, and incorrect assumptions. Employee mistakes can lead to revelation of classified data, entry of erroneous data, accidental data deletion/modification, data storage in areas unprotected, and failure to protect information. Employee failure to follow procedure and policy also leave information security vulnerable.

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)*

Since employees present one of the largest threats to information security, dual controls can be a powerful tool to help reduce the threats from acts of human error and failure because it adds an extra layer of security. For example, with two-factor or multi-factor authentication, the user must verify themselves in two or more ways to be granted access. Another example that was used in the chapter was how the military use dual approval controls built into their systems. Another way is to have a second party verify commands.

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)*

In a regular denial of service (DoS) attack, the attacker sends a large amount of connection or information requests to a single target. Whereas in a distributed denial of service (DDoS) attack, a coordinated stream of requests is launched against a target from many locations at the same time, resulting in the target system being overloaded and not being able to answer to legitimate requests for service. Distributed denial of service attacks is much harder to combat because of the distributed attacks coming from many different locations.

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)*

- Cracking: attempting to guess or reverse-calculate a password
- Brute force: an attempt to guess a password by attempting every possible combination of character and numbers in it.
- Dictionary attack: a variation of the brute force attack and narrows the field by using a dictionary of common passwords and includes information related to the target user.
- Rainbow table: a table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.
- Social engineering: attackers posing as an organization's IT professionals in an attempt to gain access to system information by contacting low-level employees and offering help for their computer issues.

A systems administrator can protect the system by using multi-factored authorization for all employees. This keeps hackers from discovering a single password and gaining access to critical data. An administrator can also implement the use of fingerprint identification to make it difficult for hackers to impersonate as an employee. A final control is teaching employees how to distinguish social engineering tactics from legitimate sources.