CIS-481: Introduction to Information Security

Module 2 - The Need for Information Security

Exercise #2

Team: 3
Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.
B. 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 and may impact your performance on assessments, especially with respect to the essay questions.
C. 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 *(5 points)*
Why is information security a management problem? What can management do that technology alone cannot?

Information security is a management problem because management is the one who controls the technology (including new ones that are implemented) and makes the policies that they also have to reinforce. Management is the one who implements the policies that secure the information, so without management there would not be proper security implemented nor controlled, nor would there be backup/recovery plans created.

Technology is created by people and can only so what it is assigned to do. Programs have to be activated, procedures have to be implemented, and there has to be a centralized will that directs technology and the associated programs and policies. Managers are therefore exceedingly important and must be highly competent to implement the correct types of programs and procedures. Technology is essentially useless without a competent human will to direct it and managers are the individuals that must be trusted to provide that direction.

Problem 2 *(5 points)*

Why do employees constitute one of the greatest threats to information security that an organization may face?

Employees constitute the greatest threat because regardless of how seamless security architecture is, if employees are poorly trained or lack social engineering they can encourage or directly cause risks and breaches. No amount of strategic planning or risk analysis can combat poor training, awareness, and knowledge about cyber security and the necessary standards of the company.

Problem 3 *(5 points)*
How can dual controls, such as two-person confirmation (sometimes referred to as the two-man rule), reduce the threats from acts of human error and failure? [You've probably seen an example of this in a movie that shows how a nuclear weapon requires two keys, held by two different people, to be launched.] Describe two other common controls that can also reduce this threat.

It reduces threats from acts of human error and failure because it requires two-step verification (which is now used in protecting accounts online). It allows for a safety net in case one account is compromised, then the other account is used as "backup" to prevent further. Two other common controls that can also reduce this threat are backup drives and input validation. Backup drives save all the information on another drive in case the first is compromised, so there's no risk of loss of information. Input validation makes sure that the correct types of data are being utilized and sent within a system's organization.

Problem 4 *(5 points)*
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?

The difference between a DoS and a DDoS attack is that DDoS attacks are from multiple locations using multiple systems and a DoS attack is mainly from one single user/location that sends a massive amount of traffic or requests that shuts down a system. DDoS attacks tend to be harder to combat since the attack is faster than DoS attacks, they are harder to trace, and have multiple devices sending packets and attacking from multiple locations, compared to DoS attacks where a single system is used.

Problem 5 *(5 points)*

Briefly describe the types of password attacks addressed in Module 2 of the text. Describe three controls a systems administrator can implement to protect against one or more of these types of password attacks.

Cracking, brute force, social engineering, dictionary, and rainbow tables are the various types of password attacks that users and businesses can be vulnerable to.These all either interfere with software security of said systems or exploit weak password habits. One control to protect against password attacks is a complex password structure composed of numbers, case sensitive letters, and symbols. Another control is multi-factor authentication as the increased security steps decrease the ability for hackers to use generic or known cracks to compromise the system. The last control would be the consistent use of an anti-virus software scanner that allows for malware and other risks to be monitored and acted on promptly.