**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 2**

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

Why is information security a management problem? What can management do that technology alone cannot? (5 pts.)

**Information security is a management problem, because it deals a lot with policy and policy is a management tool. Technology alone cannot set policies or enforce policies. Management also decides what the most important assets to be protected are, not technology. Management decides how much money they want the business to dedicate to information security.**

**Problem 2**

Why do employees constitute one of the greatest threats to information security that an organization may face? (5 pts.)

**One of the twelve categories of threats is human error and failure. Attack examples include accidents and employee mistakes. Employees are also vulnerable to information extortion such as blackmail and ransomware and even to simple things such as loss of equipment or data. Employees are the ones that store, collect and maintain information and data, therefore they have a high control over what happens to that data. They also are given high security access and privileges and can abuse company policies. Also, even if an employee is given training and exposure to correct security measures that need to be taken, ignorance and human error can threaten information security. Employees can also be the victims of social engineering attacks, for example a malicious person can impersonate an IT person and get employees to give up their private credentials, endangering the company.**

**Problem 3**

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

**In dual control, each person has to complete necessary work and submit it to each other. They then examine the work to make sure no errors exist. This reduces human error as well as increases employee confidence in their submitted work. The likelihood that two different people make the same mistake is low, so human error and failure are much more unlikely.**

**Two other controls used are job rotation (or task rotation) and least privilege. In job rotation, every employee is flexible. In other words, they must be able to perform the work of another employee. This reduces threat because employee knowledge on how to handle data is broadened and universal. Least privilege, also known as need to know, makes sure that employees have access to minimum amount of information necessary for them to perform their duties. They also have restricted access. This keeps confidentiality and integrity high, and availability limited only to those who are trusted enough to have access to certain information.**

**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 pts.)

**A DoS attack is an attack that attempts to overwhelm a computer target’s ability to handle incoming communications, prohibiting legitimate users from accessing those systems. A DDoS is a form of DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies. DDoS attacks more difficult to defend against because there are currently no controls that any single organization can apply and the attack is coming from multiple 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 pts.)

**Brute force is a type of password attack that attempts to use every possible combination of characters and numbers to guess a password.**

**Dictionary attack is a type of password attack that is similar to brute force, but uses a list of common passwords to narrow the possibilities and make the attack more effective.**

**A rainbow table is an attack where the hash values for a wide range of passwords can be looked up in a database. A hash value and its corresponding plaintext value can be matched easily and quickly.**

**Social engineering password attack is a type of password attack that usually involves someone posing as a helpdesk employee and tricking an employee to give m them their credentials. This is much easier than actually hacking into a server.**

**One control a systems administrator can implement to protect them against brute force attacks is to limit the number of incorrect password attempts in a time period. Another control to protect against these attacks is to use the 10.4 password rule which means having the password be at least 10 characters long and using at least one uppercase letter, one lowercase letter, one number, and one special character. Another control to protect against these attacks is to always change the password of the manufacturer’s default administrator account. Another control is to have your own dictionary that you check against to prevent users from selecting those words as their password.**