**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 2**

Grading ID: A7386

**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 they are primarily in charge of determining the policies, practices and programs that are used to facilitate the security of the company’s assets. They are also in charge of training the employees and enforcing these security practices. In the end, the responsibility for a company’s assets typically falls on the management, so in order to ensure effective security, they must maintain that all employees adhere to the policies that have been set, which technology alone cannot do.

**Problem 2**

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

Employees are such a great threat to information security for many reasons, but two stick out: they have access, in some form, to the company’s assets, and unlike machines, they are unpredictable. A reliable security system will always ask you for your password before allowing you to access a system, but it cannot prevent you from sharing your password with another employee, or even worse, an external user that can then enter the system with malicious intent. Improper training, entry of erroneous data, accidental data manipulation, and many other use cases make people dangerous to the integrity of a system.

**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.)

Dual controls reduce threats by decreasing the likelihood of mistakes and by not allowing one person to have immediate access to a system. If two people have to enter a password before executing a function within a system, it becomes the case that both of these people are aware of what they are doing, otherwise one person would ideally prevent the other from performing this task by not entering their portion of the password. There are several other controls that can reduce the threat of human error, or at least the frequency, such as training and ongoing awareness activities, that help employees stay up-to-date on how to properly and safely interact with a system

.

**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 uses one machine to conduct the attack, while a DDoS attack uses multiple machines simultaneously. DDoS attacks are much harder to combat because it is very difficult to trace which machine is the “root” of the attack. Meanwhile, a large number of machines send service requests into a system, flooding it to the point where it becomes very hard to extract useful data. If these machines are blocked, the attack will continue from those that are still able to access the system.

**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.)

There are several different types of password attacks, including social engineering, brute force, and dictionary attacks, among others. Some, like dictionary and brute force attacks, are primate, relying on repeated guessing attempts until a correct value is found. Others are more complex, such as social engineering, which involves manipulating a user into handing you their password directly through a variety of methods. There are a lot of ways that these methods can be countered by a systems administrator, including, but not limited to: forced password changes on regular intervals, password recovery questions, challenge tests such as CAPTCHA, multi-factor authentication, or even password requirements such as length and the use of special characters and numbers.