**CIS-481: Introduction to Information Security**

**Module 2 - The Need for Information Security**

**Exercise #2**

**Team: 3**

**Participants: Dustin Thompson, Bryce Watson, Goerge Flarsheim, Bradley Lawton, Destinee Matsoumou**

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or virtually.
2. 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.
3. 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, “... managing information security has more to do with risk management, policy, and its enforcement than the technology of its implementation.” (p.29) It is important to remember business needs come first so it is up to management to evaluate business impacts and control through policy, procedure, and governance.

Management makes policies for information technology. Something technology alone cannot do. Good security programs begin and end with policy.  These policies direct how issues should be addressed and how technology is to be used. According to the text, "policy is a management tool that obliges personnel to function in a manner to preserve the security of the information asset” security policies are particularly important for the maintenance of an organization, so it needs to be well established and implemented.

Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*. Cengage, 2022.

**Problem 2** *(5 points)*

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

Employees are closest to business data and information. An attacker can exploit employee mistakes, representing a threat to confidentiality, integrity and availability. It is much easier for an attacker to phish an employee to gain access to internal systems than it is to try to exploit a vulnerability. Most vulnerabilities are patched within a few days, if not weeks, of their discovery by organizations. However, employees are easily susceptible to phishing attacks where their account information can be obtained and used to gain access to a system.

**Problem 3** *(5 points)*

How can dual controls, such as two-person confirmation (sometimes referred to as the [two-man rule](https://en.wikipedia.org/wiki/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.

Dual controls provide an added benefit by reducing the chance of human error. It is much more unlikely for both users to make an error as opposed to one user. This method ensures that both users check each other and make sure that they are following correct procedures and policies.

One control that can reduce threats from acts of human error is multifactor authentication. If a user is tricked into giving their password to a hacker, they could be protected against the error they have made since the hacker would still need the MFA key to sign into their account. This adds an extra layer of protection to safeguard system access, even from shoulder surfing, as the MFA solution can be invoked by the users’ phone, e.g., Google Authenticator.

A second control is to require critical commands to be entered twice, or with additional steps. Take for example when one deletes a critical file from the system. The system can require that the user enter the command twice to lessen the factor of human error, deleting a file or resource by mistake. The system could also ask that the user type out the command, ‘Delete’, to further guard against unknowingly deleting content.

**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?

A DoS or denial-of-service attack attempts to swamp a server with connection or information requests to overload it so it cannot respond to legitimate requests for service. With the goal of crashing the system. A DDoS or distributed denial-of-service attack is a DoS attack, but uses streams of requests from many locations. The attack is often preceded by an attack on many machines, perhaps thousands that were compromised to allow the attacker to run remote code. These bots or zombies are difficult to stop as they can overwhelm the system from different machines, any of which could be rejected from a system, but with hundreds or thousands of compromised machines it makes that effort extremely difficult. There is no central control system that can curtail a DDoS attack.

**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.

Password attacks come in the form of social engineering, brute force attack, dictionary attack and using rainbow tables. Social engineering attacks are simply gathering information that attacker through various one-to-one means with the victim. The attacker may present themselves as a helpdesk employee to gather information that will help them guess or outright learn of the users’ password. A brute force attack uses computing and networking resources to try every conceivable password combination. This type of attack is often not attempted due to the resources required and more complex passwords when the 10.4 password rule is utilized. Dictionary password attacks are much like brute force attacks, but they also employ the use of common password dictionaries to help speed up the password cracking. Rainbow tables are a set of hash values that correspond to their plaintext password values. An encrypted password manager file would need to be accessed to gain this information. An attacker with the likes of the Security Account Manager file, could find password or password strings by locating the corresponding hash value.

Three controls a systems administrator can take to protect against password attacks are the enforcement of a limit on the number of attempts on a unsuccessful access; enforcing that passwords use the 10.4 password rule which requires lower case, upper case, special character and numbers; and utilizing a password dictionary to prevent users from using common password words and combinations.