CIS-481: Introduction to Information Security

Module 3 - Information Security Management

Exercise #3

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 *(10 points)*
This module introduced the NIST Cybersecurity Framework (p. 111). NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. In order to reflect the ever-changing cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is planning a significant update to the Framework in the coming months to CSF 2.0.

Review the current CSF 1.1 Quick Start Guide, linked below:

https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

and choose one of the five key Functions (**Identify**, **Protect**, **Detect**, **Respond**, **Recover**). For your selected key function, briefly describe the main activities associated with this (one) function.

The key function “respond" is a concept that explains the ability for information security teams to design, create, and deploy appropriate action in the instance of a cyber security breach. One characteristic of this function is the need for systems to test and practice deploying the responses they predict themselves using in the instance of a cyber attack.This ensures everyone is educated and prepared on the role they would take if this ever became a reality and decreases the chance for human error to exacerbate already compromised circumstances. Another important component of this function is to ensure that all plans are accurate and up to date with the software and hardware of the current system. Lastly, communicating with all stakeholders the state of security as well as future plans and anything they can do to aid the protection of the organization.

Problem 2 *(15 points)*
The University of Louisville's Information Security Office maintains the University's information security policies, standards, and procedures. Click on the following URL for an overview:

http://louisville.edu/security/policies/overview-of-policies-and-standards

The current list of UofL Information Security Office Policies & Standards can be reviewed here:

http://louisville.edu/security/policies/policies-standards-list

1. From the above list, look for which policy is serving as the Enterprise Information Security Policy (EISP) as discussed in your text. What is its policy number (ISO PSxxx) and name? When did it take effect? How often is it supposed to be reviewed? When was it last reviewed? Is this consistent with the policy's stated timeline for review? *(5 points)*

The policy serving as the Enterprise Information Security Policy (EISP) is Business Continuity and Disaster, its policy number is ISO PS002. It took effect on July 23, 2007. It can be reviewed one time a year or at most once a year. It was last reviewed on June 23, 2022. The date is consistent with the policy's stated timeline for review.

2. From the above list, look for a policy that would be an example of a Systems-Specific Policy (SysSP). What is the policy number (ISO PSxxx) and name? Is this of the Managerial Guidance, Technical Specifications, or Combination SysSP type? *(5 points)*

An example of a Systems-Specific Policy is regarding Firewalls, policy number ISO PS017. The policy contains both managerial guidance and technical specifications, making it a combination SysSP type. For example, the managerial guidance of the policy is to have individual computer firewalls installed or enabled on all computers and servers controlled by the department, including personal computing devices used to store or process university data, and to specify their uses, which guides the implementation and configuration of technology and addresses the behavior of those using the system in ways that support information security. Then there are the network devices having unique passwords or other access control mechanisms, which fit into the access control lists in the technical specifications part.

3. From the above list, look for a policy that would be an example of an Issue-Specific Policy (ISSP). What is the policy number (ISO PSxxx) and name? Is this of the independent, comprehensive, or modular ISSP type? *(5 points)"*

The Email Archive Policy is an example of an issue-specific policy (ISSP). The policy is policy # ISO PS019 Email Archiving. The policy directs employees that anything past the 120 day period that havent been deleted will automatically be archived. Archived email, calendar entries, tasks and notes will be retained for a period of 2 years and there will be designated folders for emails that need to be retained for specific purposes such as grants. The folders will be created for 5, 7, 10 , and 15 years for the previously mentioned emails related to those specific purposes. This policy is considered to be modular because it appears to have different directions for different data types; this is customized therefore falls into the customized area.