CIS-481: Introduction to Information Security

Module 3 - Information Security Management

Exercise #3

Team: 4
Participants: Aneesa Bell, Paige Hensley, Patrick Nguyen, Logan Whaley, Emily Wyland

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.

We have chosen recovery as our key function. Caution and communication adequately convey the activities associated with recovery. When a cyber-security event takes place, you must restore anything that has been impaired as well as maintain resilience.
In recovery, it is essential to communicate with the stakeholders. Stakeholders need to receive the appropriate amount of information. Nothing more and nothing less.
The relevant recovery plans should be updated with what has been learned from the cyber-security event.
Lastly, a huge part of the recovery function is managing the company reputation. Information given must be accurate, timely, and whole.
These activities must be handled with both caution and communication to maintain trust amongst all involved parties.

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 EISP is ISO PS001 - Information Security Responsibility. It took effect on July 23, 2007. It is supposed to be reviewed annually. It was last reviewed on June 23, 2022. This is consistent with the 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)*

The SysSP we have chosen is ISO-017 v2.1 Firewalls – IT Division Policy. This policy took effect on July 23rd, 2007. The last revision data was on June 14th, 2017, and is supposed to be reviewed annually. However, the revision updates seem to have not been updated or updates have not occurred. This policy is a combination of the two SysSps. Looking over the policy, we see administrative authority (managerial) and configuration rules (technical).

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 ISSP we chose from the list was ISO PS019 - Email Archive. This policy took effect on February 14, 2011, and was last reviewed on March 8, 2016. The policy is supposed to be reviewed annually, so the most recent review date is not consistent with this policy. This ISSP is independent because it only covers one specific issue. It does not provide a comprehensive list of every issue or a modular breakdown of a general category.