CIS-481: Introduction to Information Security

Module 3 - Information Security Management

Exercise #3

Team: 5
Participants: Abril Beascoechea, Ricardo Portillo, Charles Degboe, Nicholas Zhang, Sam Martin

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.
Detect:
For this function in CSF 1.1 the main activities are to test and update detection, maintain and monitor logs, analyze the data provided from the logs and know the data that is used for the company and finally understand the impact of cybersecurity. Then with all the data collected analyze it and check for any possible cybersecurity events.
Through detection we need to develop and implement detection processes that can help in checking cybersecurity issues like unauthorized access from infrastructure, networks and applications.
Maintaining logs from anything related to the enterprise is something very important for many different reasons. One of these is to know any possible issues with the company resources. Another thing that is very useful is to know if infrastructure has been altered and by who. All of this is not only useful to know threats to the company, but it is also useful to achieve compliance with industry standards and regulatory frameworks. If the company accomplishes

industry standards, possible clients see the company as a better option compared to competitors with worse security standards.

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 ISO PS001 Information Security Responsibility. This policy, effective since July 23, 2007, requires an annual review to ensure it continues to address the University's risk exposure and is in compliance with the applicable security regulations and university direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed per the Policy Management process.

  The policy was last reviewed on June 23, 2022 where a minor edit was made. This aligns with the policy's stated timeline for review, although it's been almost 2 years from the last review, there were significant changes made in 2021 so it will be reviewed and updated as needed per the Policy Management Process.

2. From the above list, look for a policy that would be a good 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)*

   From the policy above a good example of a Systems-Specific Policy(SysSp) is ISO PS012 Workstation and Computing Devices. This is a combination SysSp of both managerial guidance and technical specifications. The managerial guidance touched on the dean or department heads responsibilities for each department and there will be consequences if not followed. A technical specification was HIPAA and its privacy put in place to protect ePHI.

3. From the above list, look for a policy that would be a good 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)*

One ISSP is ISO PS021 Voice Mail. This policy is a comprehensive ISSP type as it applies to all university workforce, faculty, and students, and all components are present on a single document.