2-2 Project One Milestone: Security Control Implementation

Joshua Merren

Southern New Hampshire University

CYB-420-13227-M01 Enterprise Security

Professor Aaron Tyler

15 January 2025

I. Threat Assessment

A. Vulnerabilities in the Risk Domain of People

A key vulnerability in the people domain is employees' lack of security training. Without regular education on cybersecurity best practices, employees are more likely to fall victim to threats like phishing scams or social engineering tactics. These mistakes can lead to unauthorized access to sensitive systems and data breaches. Additionally, remote employees who use unsecured networks to access organizational systems are at greater risk of exposing the company to external threats. Security awareness training and tools, such as Virtual Private Networks (VPNs), can reduce these risks. According to NIST Special Publication 800-53, implementing security awareness and training programs is critical in ensuring employees are equipped to protect organizational systems and data (JOINT TASK FORCE, Ross, and Copan 2020).

B. Vulnerabilities in the Risk Domain of Process

In the process domain, the absence of formalized security policies creates inconsistencies in how employees handle sensitive information. Without clear procedures, there is a greater chance of errors or negligence that could lead to security breaches. Another critical issue is the lack of a structured incident response plan. A breach hinders the organization’s ability to respond effectively without a predefined strategy, potentially causing prolonged downtime and data loss. NIST Special Publication 800-122 highlights the importance of creating detailed processes to protect sensitive information and effectively respond to incidents. It emphasizes that strong process controls are necessary for organizations to minimize risks to sensitive data (McCallister et al., 2010).

C. Vulnerabilities in the Risk Domain of Technology

The technology domain is vulnerable due to terrible network segmentation. The current infrastructure does not effectively isolate departments, making it easier for threats to move laterally across systems. Segmentation would help limit the spread of malicious activities by restricting access between network segments. Additionally, outdated hardware, such as routers and switches, poses a security risk as these devices may not include the latest security updates or advanced protective features. NIST Special Publication 800-53 outlines the importance of implementing robust technological safeguards, such as network segmentation and regular updates to hardware, to protect against evolving threats and maintain data integrity (JOINT TASK FORCE, Ross, and Copan 2020).

II. Implementation Approach

A. Implementing Security Controls in the People Domain

Organizations should implement security awareness training programs to address vulnerabilities in the people domain. These programs would educate employees on recognizing and mitigating risks like phishing attempts and social engineering attacks. Train employees to protect sensitive data actively, especially when working remotely. Providing tools like Virtual Private Networks (VPNs) and enforcing multi-factor authentication (MFA) can enhance the security of remote connections. NIST Special Publication 800-53 emphasizes security awareness and training programs to equip personnel with the skills to mitigate risks and protect organizational data, aligning with these measures (JOINT TASK FORCE, Ross, and Copan 2020).

B. Implementing Security Controls in the Process Domain

In the process domain, establishing formalized security policies and procedures is critical. These policies should clearly outline best practices for handling sensitive data, creating secure passwords, and reporting suspicious activities. Additionally, teams must develop an incident response plan that clearly outlines the steps for identifying, containing, and recovering from security incidents. Such a plan should include designated roles, communication protocols, and recovery timelines to minimize the impact of a breach. NIST Special Publication 800-122 emphasizes creating detailed processes to protect personally identifiable information (PII) and implementing structured incident response plans to safeguard organizational operations (McCallister et al., 2010).

C. Implementing Security Controls in the Technology Domain

In the technology domain, network segmentation is a key measure to prevent lateral movement of threats across systems. By isolating departments and critical data, segmentation helps limit the impact of potential breaches. It is equally important to regularly update hardware, such as routers and switches, to equip devices with the latest security patches and features. Replacing outdated equipment with more advanced models can provide additional protection against emerging threats. NIST Special Publication 800-53 recommends enforcing strong technological safeguards, such as network segmentation and hardware updates, to secure information systems and protect against evolving cyber threats (JOINT TASK FORCE, Ross, and Copan 2020).

References:

JOINT TASK FORCE, Wilbur L. Ross Jr., and Walter Copan. 2020. "NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations." U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

McCallister, Erika, Tim Grance, Karen Scarfone, and National Institute of Standards and Technology. 2010. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." *National Institute of Standards and Technology Special Publication 800-122*. https://leocontent.umgc.edu/content/dam/course-content/tus/sdev/sdev-360/document/sp800-122.pdf?ou=1029097.