Topic 2 Discussion 1

When building an information security policy, it is important to note how the required security controls impact the organization and affect the business application processes. Discuss how an organizational security policy is developed and implemented in an organization. What are some of the formal roles and responsibilities required by the organization's security policy and the reporting structure?

Hello Class,

The development of an organizational security policy is an iterative process that begins with a thorough risk assessment. This involves identifying potential threats and vulnerabilities to the organization's assets, including hardware, software, data, and personnel(NSF, 2024). The assessment should consider various factors such as the organization's size, industry, and regulatory environment. Once the risks are identified, the organization must determine the appropriate security controls to mitigate those risks. These controls can range from technical measures like firewalls and intrusion detection systems to administrative controls like access control policies and employee training programs. Crucially, the selection of security controls must consider their impact on business operations. Overly restrictive controls can hinder productivity and efficiency, while inadequate controls can leave the organization vulnerable to attacks. Therefore, a balance must be struck between security and usability. The policy should clearly define the roles and responsibilities of various stakeholders, including the Chief Information Security Officer (CISO), security administrators, and end-users. The CISO typically oversees the development and implementation of the security policy and reports to senior management(NCES, 2019). Security administrators are responsible for implementing and maintaining the technical security controls, while end-users are responsible for adhering to the policy's guidelines. A clear reporting structure is essential for effective communication and accountability. Regular security audits and reviews should be conducted to ensure the policy remains effective and up-to-date. The policy should be regularly reviewed and updated to reflect changes in the threat landscape and the organization's business needs(Flowerday & Tuyikeze, 2016). Finally, the policy should be communicated effectively to all employees through training programs and awareness campaigns. Effective communication is crucial to ensure that employees understand their roles and responsibilities and can adhere to the policy's guidelines(NIST, 2024). This comprehensive approach ensures a security policy that is both effective and practical, minimizing disruption to business processes while maximizing protection against threats.

References:

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

National Center for Education Statistics (NCES). (2019). *Chapter 3-Security Policy: Development and Implementation, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics)*. Ed.gov. https://nces.ed.gov/pubs98/safetech/chapter3.asp

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

NSF. (2024, February 23). *Building Information Security Policies With Ease*. Www.nsf.org. https://www.nsf.org/knowledge-library/building-information-security-policies-with-ease