4-2 Journal: Risk Management

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

22 July 2024

Cybersecurity risk management is crucial for protecting the assets and operations of any organization. Every organization faces unique challenges, making it vital to identify what specific risks pose the greatest threat to its operations and data. This process involves understanding the potential threats, identifying vulnerabilities within our systems, and then taking measures to reduce the associated risks. Reflecting on the material from the course, it is clear that managing these risks is about implementing technology solutions and understanding and aligning these strategies with the organization's broader objectives. For instance, different industries face different levels of risk and consequences from data breaches, as highlighted in the readings. This insight helps us see why a one-size-fits-all approach does not work in cybersecurity, and it emphasizes the need for a tailored strategy that considers the specific needs and threats facing an organization.

From the readings, I learned that effective cyber risk management involves continuous assessment, mitigation, and monitoring. The NIST Cybersecurity Framework provides a valuable guideline for this process, helping organizations systematically manage their cybersecurity risks. The framework suggests identifying and prioritizing assets, which is crucial because it allows an organization to focus its resources where they are most needed. Then, assessing the risks to these assets helps understand the potential impacts of different cybersecurity threats. Based on this assessment, the organization can develop strategies to mitigate these risks, implementing security controls and measures tailored to their needs. Regularly monitoring these controls ensures they are practical and allows the organization to adjust them as new threats emerge. This ongoing assessment, mitigation, and monitoring cycle is essential for maintaining robust cybersecurity defenses and ensuring the organization can respond effectively to cyber threats.