Topic 2 Discussion 1

Hackers have been upping their game recently. Not a single week goes by without an organization somewhere in the world in the news for being a recent victim of a cyberattack. Discuss how adopting the National Institute of Standards and Technology (NIST) cybersecurity framework could help contribute to an organization's security posture and help improve protection against those attacks.

Hello Class,

The increasing frequency of cyberattacks underscores the urgent need for organizations to adopt robust cybersecurity measures, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a comprehensive approach to enhancing security posture(Federal Trade Commission, 2025). By implementing this framework, organizations can systematically identify, assess, and mitigate cyber risks, thereby improving their overall resilience against attacks. The framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover, which together create a holistic lifecycle for managing cybersecurity threats(Bresnahan, 2022).

For instance, the Identify function helps organizations understand their assets and vulnerabilities, allowing them to prioritize security efforts effectively. The Protect function focuses on implementing safeguards, such as access controls and employee training, which are crucial for preventing breaches(NIST 2018). Meanwhile, the Detect function emphasizes the importance of establishing monitoring systems to quickly identify potential threats, enabling organizations to respond swiftly to incidents. The Respond function outlines procedures for managing and containing attacks, ensuring that organizations can minimize damage and recover efficiently(NIST, 2024). Finally, the Recover function aids in restoring services and improving processes post-incident, which is vital for maintaining business continuity.

Adopting the NIST Cybersecurity Framework not only enhances an organization’s ability to defend against cyber threats but also fosters a culture of continuous improvement in cybersecurity practices(Ugalde, 2022). By regularly reviewing and updating their security measures in line with the framework, organizations can adapt to the evolving threat landscape, thereby reinforcing their defenses against increasingly sophisticated cyberattacks. This proactive approach is essential for building trust with stakeholders and ensuring compliance with regulatory requirements, ultimately contributing to a more secure digital environment.

References:

Bresnahan, E. (2022). *What Are the Benefits of the NIST Cybersecurity Framework*. Www.cybersaint.io. https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework

Federal Trade Commission. (2025). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

NIST. (2018). CSF 1.1 Uses and Benefits of the Framework. *NIST*. https://www.nist.gov/cyberframework/uses-and-benefits-framework

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *2.0*(29). https://doi.org/10.6028/nist.cswp.29

Ugalde, J. (2022, September 3). *5 Benefits of the NIST Cybersecurity Framework*. Www.systems-X.com. https://www.systems-x.com/blog/nist-cybersecurity-framework-benefits