Andree Salvo

Southern New Hampshire University

CYB 400

4-3 Activity: Enterprise Assessment Approach

Instructor: Robert Chubbuck

9/3/2025

When assessing an enterprise, I would take a structured and layered approach. The first thing I would do is to understand how the organization's overall security posture is evaluated by its existing policies and compliance requirements, and identify strengths and weaknesses, as well as risk mitigation strategies. Additionally, I would assess the current state of its network infrastructure. From there, I would need to plan an audit that focuses on both technical controls and human factors. In essence, we are not only testing our systems but also examining how employees and new employees can handle whether the processes are being followed as required.

To account for people, process, and technology, I would have to break it down into three parts. First, people, I would have to adopt **security awareness training and alerting for insider risks**. According to TechTarget, “Security awareness training is a strategic approach IT and security professionals take to educate employees and stakeholders on the importance of cybersecurity and data privacy.” (TechTarget, 2023) The primary objective of implementing security awareness training is to enhance security measures among employees and reduce the risks associated with cyberattacks. An insider threat is a type of cyberattack originating from an individual who works for an organization or has authorized access to its networks or systems. An insider threat could be a current or former employee, consultant, board member, or business partner and could be intentional, unintentional, or malicious.” (Fortinet, n.d.) For the process, I would have to review

how the policies are written, enforced, and how they align with compliance standards. As for technology, I would review everything, from its network architecture and access controls to vulnerability management and monitoring systems that are in place. Adding IDS and IPS is essential because it helps strengthen detection and prevention. Another thing I would also like to add is the principle of defense in depth, so that if one layer fails, another layer will still be in place to protect the enterprise.

To really understand enterprise security, I need to gather both technical documents and insights from real-world experiences. For the technical side, I'm looking for network diagrams, system and asset inventories, access control lists, policy documents, and logs from security tools. It's also essential for me to review any incident reports and past risk assessments to identify any issues. On the human side, I need to conduct staff interviews and do physical security checks, as not everything is captured in documents. I also need to make sure that employees are adhering to their security awareness training, including recognizing phishing scams, resisting social engineering, and maintaining good password practices. By collecting this type of data, I can gain a clear understanding of both the technical vulnerabilities and human behaviors that impact security, providing a comprehensive view of how the enterprise is protected.

One of the biggest challenges in this effort is putting everything together to get a complete view. It's tempting to zero in on just the technical aspects or just compliance, but the real challenge lies in blending people, processes, and technology into a single assessment. Another challenge is ensuring that both leadership and employees are aligned and cooperating, as any resistance or lack of transparency can significantly slow down operations within the enterprise.

References

Yasar, K., & Pratt, M. K. (2023, October 12). *What is security awareness training?* SearchSecurity. TechTarget. https://www.techtarget.com/searchsecurity/definition/security-awareness-training

Fortinet. (n.d.). *What is an insider threat? Definition, types, and prevention*. Fortinet CyberGlossary. https://www.fortinet.com/resources/cyberglossary/insider-threats