**Module Eight Journal: Portfolio Reflection**

Alexander Egelston

Department of Computer Science, Southern New Hampshire University

CS-405-J7382 Secure Coding

Prof. Mike Prasad

8/20/2023

During the development of the automation presentation, several aspects of secure software development and cybersecurity were addressed. One of the critical considerations was the adoption of a secure coding standard. By prioritizing security from the outset and incorporating secure coding practices, the presentation aimed to prevent vulnerabilities and potential breaches that might arise due to negligence in security measures. Emphasizing secure coding practices ensures that security is an intrinsic part of the development process, rather than being an afterthought. This approach not only reduces the risk of vulnerabilities but also saves time and resources that would otherwise be spent on addressing security issues later in the development lifecycle.

The presentation also delved into the evaluation and assessment of risks, as well as the cost-benefit analysis of mitigation strategies. Understanding the potential risks associated with software vulnerabilities and data breaches is crucial for making informed decisions about security measures. By conducting a cost-benefit analysis, organizations can allocate resources effectively to implement mitigation strategies that provide the greatest impact in terms of risk reduction. This approach ensures that security investments are aligned with the potential consequences of security breaches, leading to a more targeted and effective security posture.

The concept of a zero-trust policy was explored in the presentation, highlighting a paradigm shift in security strategy. The zero-trust approach challenges the traditional notion of trust within a network and promotes a "never trust, always verify" mindset. This means that even within an organization's network, all users and devices are treated as potentially untrusted entities, requiring continuous verification of their identity and authorization. This approach enhances security by minimizing the potential lateral movement of attackers within the network. Incorporating a zero-trust policy emphasizes the importance of security throughout the entire network infrastructure.

The presentation concluded with the implementation and recommendations of security policies. It emphasized the significance of creating comprehensive security policies that cover aspects such as authentication, authorization, data protection, and incident response. Clear and well-defined security policies provide guidelines for employees, developers, and administrators on how to handle sensitive information, access controls, and potential security incidents. Regular reviews and updates of these policies are necessary to adapt to evolving threat landscapes and ensure that security measures remain effective over time.