# SNHU CS-405 Journal: Portfolio Reflection

Tanner Holbrook

Southern New Hampshire University

Ensuring the integration of secure coding standards at the start of development is crucial for creating a secure and well-rounded program. In addition, emphasizing security throughout the development lifecycle instead of leaving it to the end will allow for a more proactive approach, which will inherently result in a more secure program with fewer vulnerabilities and design flaws. In addition, unlike conventional methods, this approach shows the importance of ingraining the idea of security in the code of the development process to create a safe and less vulnerable program.

The effectiveness of any cybersecurity strategies will start by evaluating the risks and a cost-benefit analysis of the mitigation efforts. By thoroughly assessing the potential and likelihood for risks to occur, organizations can efficiently allocate resources in a priority order to ensure time is well-spent. Furthermore, from an economic perspective, companies can weigh the cost-effectiveness of security against what a potential loss would cost them. This methodology will allow organizations to balance risk mitigation and resource allocation, resulting in a more secure program with fewer risks overall.

The zero-trust security model works by assuming threats can happen externally and internally, emphasizing the importance of continuously authenticating and authorizing users to minimize the risk of unauthorized access and movement within networks. In addition, security policies require an effective implementation strategy to create a robust cybersecurity framework. Security policies can serve as a guide, highlighting the importance of access controls, data protection, and an incident response plan. In addition, conducting regular audits to ensure compliance and enforcing these policies when not followed will help create a more structured, secure, and safe environment that ensures data will stay protected.