**8-2 Journal: Portfolio Reflection**

Levi Bajuscik

Southern New Hampshire University

CS-405: Secure Coding

Mimi Tam

June 29, 2025

I believe that every organization that creates software should adopt a secure coding standard. They provide rules and guidelines to help development teams write code that is maintainable, efficient, and most importantly secure. As a positive side effect of this, it also facilitates the approach called secure by design, which integrates security across the entire development process instead of just at the end (Fitzgerald, 2024).

Evaluating and assessing the risk of a cybersecurity threat is through both quantitive and qualitive analysis to determine the best course of action. This process identifies potential vulnerabilities, their likelihood of being exploited as well as their severity. Then it’s decided, typically based on a mathematical model, whether or not the benefit of mitigating this vulnerability outweighs the cost of doing so as well as the cost of the attack. In some cases, the remediation can be quite high to fix while the severity of the vulnerability is quite low and would probably be considered an acceptable level of risk by the organization. However, there are other vulnerabilities that if they were to happen, the cost of it (i.e. loss of private user data and reputational damage) would be astronomical and it would be in the organization's best interest to invest heavily in cybersecurity to mitigate this possible vulnerability.

Zero Trust is an example of a security policy that shows when the technology landscape changes, so too must security strategies lest an organization leaves itself vulnerable to all sorts of new attacks. The traditional “trust-by-default as long as it’s within the network perimeter” is no longer the case for many organizations. With the increased adoption of cloud services and normalization of remote work, a new strategy like Zero Trust needed to be put in place. So instead of trusting-by-default, we need to always verify a person is who they say they are and know what they are allowed to do within the system. It’s important to note this isn't just done once at the point of entry but, continuously.

A good security policy is the backbone of an organization's cybersecurity framework. They are essential in order to assess the risks that the development project is likely to face and plans for mitigation of those risks as well as the determination of coding best practices and standards.

**References**

Fitzgerald, A. (2024, April 23). *Secure by design: What does it mean & how to reasonably implement it*. Secureframe. https://secureframe.com/blog/secure-by-design