**8-2 Journal: Portfolio Reflection**

Jacqueline G. Darwish

Southern New Hampshire University

CS-405-11671-M01 Secure Coding 2025 C-1 (Jan – Mar)

Mimi Tam

February 24, 2025

**Adoption of a Secure Coding Standard**

Secure coding practices should never be an afterthought in the software development lifecycle. By adopting a secure coding standard from the start, organizations can mitigate security risks before they manifest as vulnerabilities in production systems. Implementing best practices, such as input validation, proper authentication mechanisms, and secure memory management, reduces the likelihood of exploitable flaws (National Institute of Standards and Technology [NIST], 2024). Historically, many cyber incidents, such as the Equifax data breach, resulted from poor coding practices that could have been avoided with early security integration (IBM, 2024). Following a structured secure software development framework, such as NIST's Secure Software Development Framework (SSDF), ensures that security measures are embedded throughout the development process rather than applied as reactive patches (Souppaya et al., 2022). A proactive approach to secure coding significantly enhances an organization’s resilience against cyber threats.

**Evaluation and Assessment of Risk and Cost Benefit of Mitigation**

Every security decision involves an evaluation of risk versus the cost of mitigation. Organizations must assess the severity and likelihood of potential threats to prioritize resources effectively. For example, an advanced persistent threat (APT) targeting financial data warrants a different level of investment compared to a minor phishing attempt. Implementing continuous threat intelligence monitoring, such as IBM’s X-Force Threat Intelligence framework, enables businesses to stay ahead of emerging risks (IBM, 2024). The cost-benefit analysis of mitigation strategies must also consider regulatory fines, reputational damage, and operational downtime, which can far exceed the initial cost of security investments (CrowdStrike, 2024). By integrating risk assessment into decision-making, organizations can allocate resources efficiently while maintaining a robust security posture.

**Zero Trust as a Fundamental Security Approach**

Zero trust has revolutionized the traditional perimeter-based security model by enforcing a "never trust, always verify" policy (Kueh, 2020). Unlike legacy security frameworks that assume implicit trust for internal users, zero trust requires continuous authentication, authorization, and monitoring for all access requests. This model reduces the attack surface by ensuring that users and devices must prove their identity and meet security requirements before accessing sensitive resources (NIST, 2024). Additionally, zero trust minimizes insider threats, as lateral movement within a network is strictly controlled. Implementing zero trust principles, such as multi-factor authentication (MFA), least-privilege access, and network segmentation, strengthens an organization’s defense against both external and internal attacks. As cyber adversaries become more sophisticated, zero trust serves as a necessary evolution in modern cybersecurity.

**Implementation and Recommendations for Security Policies**

Security policies must be both comprehensive and enforceable to remain effective. Organizations should develop policies based on industry-recognized frameworks, such as the NIST Cybersecurity Framework and SSDF, to ensure alignment with best practices (Souppaya et al., 2022). Effective security policies should include clearly defined authentication mechanisms, encryption standards, and access control measures to protect sensitive data. Additionally, continuous compliance monitoring tools, such as AWS Config, can automate policy enforcement and detect security drift in real-time (AWS, 2019). As cybersecurity threats continue to evolve, security policies must be regularly reviewed and updated to address new attack vectors and regulatory requirements. Organizations that prioritize adaptive and well-implemented security policies will be better equipped to defend against emerging cyber threats.

**Conclusion**

The adoption of secure coding standards, thorough risk assessment, and zero trust implementation are essential for modern cybersecurity. Organizations that proactively integrate security at every stage of development minimize vulnerabilities and reduce the risk of costly data breaches. By continuously refining security policies and leveraging automation, companies can enhance their overall security posture and maintain compliance with evolving industry regulations. Cyber threats will only continue to grow in sophistication, making it critical for businesses to stay ahead through robust security frameworks and proactive mitigation strategies.

**References**

AWS. (2019). *AWS Config*. Amazon Web Services, Inc. <https://aws.amazon.com/config/>‌

*CrowdStrike 2024 Global Threat Report | CrowdStrike*. (2024). Crowdstrike.com. https://www.crowdstrike.com/en-us/global-threat-report/

‌IBM. (2024). *IBM Security X-Force Threat Intelligence Index 2024*. Www.ibm.com. https://www.ibm.com/reports/threat-intelligence

‌Kueh, T. (2020, January 15). *A Practical Guide to Zero-Trust Security*. Threatpost.com. https://threatpost.com/practical-guide-zero-trust-security/151912/

‌National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

‌Souppaya, M., Scarfone, K., & Dodson, D. (2022, February 3). *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/218/final

‌