**Portfolio Reflection**

Trenton Mendiola

Southern New Hampshire University

CS 405

Dr. Mimi Tam

June 29, 2025

**Adoption of a secure coding standard, and not leaving security to the end**

Adopting secure coding standards is essential when creating a system that adheres to current best practices and security standards. Adopting and implementing those standards is something that must be done first. As explained by The Federal Trade Commission in the article “Start with Security: A Guide for Business” starting with security is how you create a standard for security and apply it throughout the entire project (The Federal Trade Commission, 2024). In the case of system security, adopting secure coding standards and applying them into a security policy that will guide the implementation of security in the system is how you ensure that the system is built inherently with security in mind. If done properly, this will result in a system that adheres to all current coding standards and follows the best industry practices to prevent attacks throughout the entire system.

**Evaluation and assessment of risk and cost benefit of mitigation**

When evaluating risks, it is important to assess what would be lost or compromised during an attack. As stated by Adam Murray in the article “What You Need to Know About Code Risk Management” when explaining proper risk management they say “ The first step to good risk management of code is to think about the exposure to risk, the likelihood of occurrence, and the impact” (Murray, 2021). What Adam Murray is explaining is that when evaluating risk in a system you would prioritize different vulnerabilities based on the likelihood of it being exploited, the value of what can be affected, and what would happen if it was exploited (Murray, 2021). The end goal of risk assessment is to determine where priority should lie, mitigating as many different risks as possible to make the most secure system possible (Murray, 2021). The cost of mitigation would be what it would cost to make right or make repairs to a system after an attack has already taken place (Murray, 2021). This could include the cost to rescue a system, compensate affected individuals, and many other costs involved. This cost would be assessed in risk evaluation assuming the vulnerability exploited was known (Murray, 2021).

**Zero trust**

The zero-trust concept is based on the sentiment that nothing accessing the system can be inherently trusted. This concept enforces authentication every time anything attempts to make access to the system. This concept helps to prevent attacks from compromised users or programs and ensures that anything accessing the system is authorized to do so. This is an efficient concept that should be implemented throughout every system to enforce the principles of authorization and authentication. If this concept is implemented into a system this can help prevent many attacks, an example being as stated by Francis Dinha in the article “How Zero Trust Could Have Changed The Outcome” the “...Colonial Pipeline Hack” (Dinha, 2022). In this attack, the system was compromised as a result of one compromised password (Dinha, 2022). With the zero-trust concept, a password would not be enough to access the system (Dinha, 2022). The individual would still have to prove their identity through another form of authentication, thus likely preventing this attack entirely (Dinha, 2022).

**Implementation and recommendations of security policies**

Security policies serve as set guidelines that dictate how security is implemented into a system. They are a set of instructions that explain what security principles and standards need to be implemented into the system and how to do so. This would often include aspects like how to implement automation. This would include where in the system's lifecycle it should be implemented and what tools should be used to perform this. This is one example of many different rules in the security policy that all dictate how security is implemented into the system. When making recommendations for a security policy there are many different factors that dictate what security policy would work for a specific system. Different systems will benefit more from different security policies. As stated by Michael Buckbee in the article “How to Create a Good Security Policy” when explaining security policies, they state “Policies should also support and be driven by business needs” (Buckbee, 2023). Appropriate security policies for a system should be based on the system and business need to create a set of system security that provides industry standard security specific to the system that is being created (Buckbee, 2023). As an example, if the business wants a cloud-based system, the security policy would need to address cloud-based system specific vulnerabilities that need to be addressed (Buckee, 2023).

References

Buckbee, M. (2023, June 2). *How to create a good security policy*. Varonis: We Protect Data. Retrieved June 29, 2025, from <https://www.varonis.com/blog/how-to-create-a-good-security-policy>

Dinha, F. (2022, April 4). *Google search*. Forbes. Retrieved June 29, 2025, from <https://www.forbes.com/councils/forbestechcouncil/2022/04/04/how-zero-trust-could-have-changed-the-outcome/>

FEDERAL TRADE COMMISSION. (2024, February 14). *Start with security: A guide for business*. Federal Trade Commission. Retrieved June 29, 2025, from <https://www.ftc.gov/business-guidance/resources/start-security-guide-business#start>

Grammarly.Retrieved June 29, 2025, from <https://app.grammarly.com/>

Murray, A. (2021, October 28). *Code risk management - What you need to know*. Mend.io. Retrieved June 29, 2025, from <https://www.mend.io/blog/risk-management-of-code/>