Adoption of secure coding standards is important because they have been written based on known attacks and vulnerabilities that were exploited in many attacks. The coding standards also include tools for analyzing and identifying many similar vulnerabilities. Furthermore, the likelihood and remediation cost are important factors to consider when under time constraints and given limited resources for testing. For these reasons, it is important to incorporate security into the system design from the beginning. Leaving security to the end will only increase the risk of not properly handling vulnerabilities. In addition, leaving security to the end will result in code that may not be written to standard and could result in significant refactoring.

In order to properly evaluate and assess the risks to a system, it is important that security plays a large role in the design and planning stage. Any risk to the system could lead to a catastrophic loss of service, customer confidence, and legal liability for not being in compliance with regulatory requirements. The benefit for such mitigation is that the code is written from the ground up with security in mind. This way, testing can be done in an iterative fashion, ensuring that the code is secure throughout development. Mitigation is important because these types of techniques are swift to implement and are more resource-friendly (Demi Ben-Ari, 2023). However, mitigation alone is not enough to secure your system and should be in support of remediation. Mitigation is best suited for threats that require an immediate response. But relying on this too much will leave many vulnerabilities lingering in the system which could someday be exploited to devastating results.

Zero trust is a modern concept for security in which you assume that all users and devices require verification of their identity and should be considered untrustworthy (Terry, 2025). This is partly due to the widespread adoption of mobile devices and IoT devices. These devices introduce many new vectors of attack since they are often overlooked when it comes to ensuring that the connection is secure. For example, mobile devices are much more likely to connect to public networks, where it is easier for malicious actors to intercept data transmissions. Social engineering has also become a problem with companies placing more emphasis on the elaborate phishing strategies that are now actively in use to steal user credentials to gain access to sensitive data. By adopting a zero-trust model of security, systems are better prepared for intruders from all forms of attack. Not only are these systems better prepared, but by following the code of “never trust, always verify,” they are also better able to respond to data breaches and to minimize the damage done to the organization and its customers. This is due to principles such as the principle of Least Privilege, micro-segmentation, and multi-factor authentication.

References:

Demi Ben-Ari. “Remediation vs. Mitigation: What’s the Difference?” *Panorays*, 22 June 2023, panorays.com/blog/remediation-vs-mitigation/.

Terry, Ryan. “What Is Zero Trust Security? Principles of the Zero Trust Model | CrowdStrike.” *Crowdstrike.com*, 13 Mar. 2025, www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/.