**8-2 Journal**

Adopting a secure coding standard can help with enhancing security by providing a strong foundation for how to properly implement specific coding patterns or system architectures in a way that avoids vulnerabilities. Implementing security measures, including a secure coding standard, while a piece of software or larger system is still being developed instead of saving security for the end carries the benefits of higher confidence in the amount of coverage provided by security layers, easier implementation as it can be done incrementally, and the software or system being able to be adjusted to better fit security measures.

When considering when to implement security layers and what types of security are needed in a system, the risk of delaying security implementation and the cost benefit of threat mitigation are two important factors. First, delaying security implementation carries the risk of falling victim to preventable system attacks or data breaches. In addition to the benefits listed above, implementing security layers early in development aids in constant and consistent protection of both system components and sensitive data. Second, the potential cost of a successful attack can easily outpace the upfront cost of the security layers that could have prevented the attack.

Zero trust security policies dictate that every piece of data, every inner component, every outside connection, and every user in a system be treated as a potential attack vector through which, the system could be compromised. In practice, this means that regardless of privilege, all users follow the same security guidelines; regardless of origin, every piece of data is verified to be non-malicious before being consumed or operated with; and regardless of prior connection history, every outside connection is verified to be secure and non-hostile before system access is granted. Zero trust security is both about holding zero trust for users and data and not needing trust for users and data because the security procedures within the system validate all potential attack vectors to be safe and secure.