**CS-405 Module Eight Journal**

Andrew Emilio DiStefano

SNHU

Professor Brian Enochson

February 27, 2025

**Reflect on and include a discussion of the following topics, using readings from throughout the course to support your views.**

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

Developing a secure coding standard (Scheila & Seacord, 2018) designed for the needs of a specific organization helps keep its members in sync in their efforts to maintain system security. This is especially important for C++ coding due to the vast number of different vulnerabilities which can result from the improper writing of C++ code (Gaynor, 2019) for memory optimization. A lack of properly defined security standards within an organization can leave data and system components vulnerable to a wide variety of attack types (Gaynor, 2019) including buffer overflow and SQL injection attacks resulting from a lack of appropriate input validation methods (Ballman, 2016), for example.

Not leaving security to the end involves addressing the need for system security at every phase of the development process, and within every department of an organization (Federal Trade Commission, 2023). Failing to address security at early stages of the development process leaves projects vulnerable to technical debt, which describes the incremental compounding of the complexity of solving uncaught issues as a system is further developed (Akamai Developer, 2021). For example, if a variable declared as the wrong data type is left unattended and volumes of new code are written referring to the variable as the incorrect data type, much more of the code will need to be changed in order to solve the issue that would have been if it were addressed early on. The larger and more complex the project, and the longer the issue goes unresolved, the more resource-intensive and time-consuming the process of correcting the issue becomes.

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

Risk evaluation and assessment involves “identifying critical assets, including hardware, software, sensitive data, networks and IT infrastructure and cataloging potential threats and vulnerabilities” (Downie & Finio, 2024). As potential threats are identified, the potential impacts of relevant risks are evaluated, and the likelihood and potential damage which could be caused by them is determined (Downie & Finio, 2024). “Cybersecurity assessments make it easier to share information about potentially high risks to stakeholders and help leaders make more informed decisions regarding risk tolerance and security policies” (Downie & Finio, 2024). Stakeholders can then make informed decisions as to which measures are most appropriate.

**Zero trust:**

Zero-trust systems use a comprehensive series of redundant security measures to keep systems secure even from users who are already within the system, whether through having gained unauthorized access or otherwise. These types of systems assume that anyone interacting with a system component is a potential attacker so that malicious actors who have gained unauthorized access are unable to fully access the system’s data and functions (Kueh, 2020). Since modern organizational networks require multiple team members in different geographical areas connecting to a system (Check Point Software, 2019), allowing users to access only the data and system functionality required for them to fulfill their responsibilities within the system prevents potentially unauthorized users from taking full control or accessing sensitive data (Okta 2019).

**Implementation and recommendations of security policies:**

The implementation and recommendation of security policies is an important step in the implementation of an effective DevSecOps pipeline (Palo Alto networks, 2025). Security policies define the overall security stance and lay out several strategies for strengthening organizational security measures (Grimmick, 2024). “A large and complex enterprise might have dozens of different IT security policies covering different areas…[which]...depend on the technologies in use, as well as the company culture and risk appetite” (Grimmick, 2024). These organization-specific specifications must be carefully considered for the formation of a comprehensive security policy which meets company goals while still providing the necessary versatility for organizations to achieve their goals.

**Sources:**

Akamai Developer. (2021, March 5). *CI/CD Explained | How*

*DevOps Use Pipelines for Automation* [Video]. YouTube. <https://www.youtube.com/watch?v=M4CXOocovZ4>

Ballman, A. (2016). *SEI Cert C++ Coding Standard*. Carnegie Mellon

University.   
 [https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-](https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-cert-cpp-coding-standard-2016-v01.pdf)

[cert-cpp-coding-standard-2016-v01.pdf](https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-cert-cpp-coding-standard-2016-v01.pdf)

Check Point Software. (2019, November 21). *What is Zero Trust Security?*

[Video]. YouTube. <https://www.youtube.com/watch?v=1D5mg9an19o>

Downie, A., & Finio, F. (2024, August 9). *What is a cybersecurity*

*risk assessment?* IBM.

<https://www.ibm.com/think/topics/cybersecurity-risk-assessment>

Federal Trade Commission. (2023). *Start with Security: A Guide*

*for Business.* [https://www.ftc.gov/business-guidance/](https://www.ftc.gov/business-guidance/resources/start-security-guide-business)

[resources/start-security-guide-business](https://www.ftc.gov/business-guidance/resources/start-security-guide-business)

Gaynor, A. (2019, August 12). *Introduction to Memory Unsafety for VPs*

*of Engineering.* Alexgaynor.net.

[https://alexgaynor.net/2019/aug/12/introduction-to-memory-](https://alexgaynor.net/2019/aug/12/introduction-to-memory-unsafety-for-vps-of-engineering/)

[unsafety-for-vps-of-engineering/](https://alexgaynor.net/2019/aug/12/introduction-to-memory-unsafety-for-vps-of-engineering/)

Grimmick, R. (2024, November 13). *What is a Security Policy? Definition,*

*Elements, and Examples.* Varonis.   
 <https://www.varonis.com/blog/what-is-a-security-policy>

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

Okta. (2019, January 7). *What is Zero Trust Security?* [Video]. YouTube.   
 <https://www.youtube.com/watch?v=d-Jk3GzjwlM>

Schiela, R., & Seacord, R. C. (2018, May 2). *Top 10 Secure Coding Practices.* Carnegie

Mellon University.  
 [https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+](https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices)

[Practices](https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices)