**Journal 8-2 Portfolio Reflection**

Thinking about secure coding from the start should absolutely always be a coder’s number one priority. The world pretty much functions with data, and it will continue to evolve as such. Security should be involved in all aspects of the architecture, design, and implementation of coding. Secure coding standards such as OWASP, and CWE can provide a clear understanding of the steps to take for secure coding. Code has to be written in with layers of protection. Without adequate layers of protection, there could be a risk that will cost an organization terribly.

The evaluation and assessment of risk. Risk assessment is at the very heart of any security program. Risk assessment will identify and measure any potential risks or vulnerabilities that are associated with the code. Risk assessment will also calculate the potential impact of those risks and vulnerabilities. The risk assessment will then determine the whether or not the cost of mitigation can be justified by the benefit of reducing this said risk. Risks are actually placed in categories based on the level of threat. But realistically, it is better to prepare for all potential risks, rather than just a few. I would want a clean and secure system fully, not just based on the level of threat severity.

Zero trust is essentially governing the access to anyone outside, or inside the company database. Personnel with access should only be allowed to access what they need to fully function in their role. Everyone must verify certain criteria in order to be able to connect to any type of system within the companies database. A good example of this, is the ability from people who can work from home. They are only allowed access to what they need in order to fully carry out their job description. This is relevant to the layer of security concept that I was referring to earlier. Things like multi-factor authentication, least privilege access, etc.

Security policies should be clear and duly noted by all who share a company’s business goals. There should always be regular training for things such as fishing. Every person within an organization should understand, and adhere to the fact that security is always number one priority.