**Module 8 Journal**

* **Adoption of a secure coding standard, and not leaving security to the end.**
  + Security must be implemented throughout the entire process of the Software Development Lifecycle (SDLC). If you wait until the end to start mitigating security issues, many vulnerabilities may exist. As the program becomes larger and every code section becomes integrated with each other, it becomes harder and more time consumer to review potential security threats. This is why programming with security in mind is important throughout the whole process.
* **Evaluation and assessment of risk and cost benefit of mitigation.**
  + Mitigating security vulnerabilities will save the company money and reputation. If you wait to check for security vulnerabilities until the end of the SDLC it will take a long time to discover all the issues. Since the security teams will have to back track through all of the code to find any issues. Also, since there is so much code to skim through, there is a high chance a security vulnerability will be missed. If most of the security vulnerabilities are not mitigated it can allow people access to the system and still customer’s Personally Identifiable Information (PII), such as credit card numbers, SSNs, phone numbers, etc. This can cause the company to lose trust and reputation from their customers.
* **Zero trust**
  + Zero trust is authenticating users for everything they want to do either in the cloud or on another network. This allows for more control on what users can see and access. Previously, a user would be authenticated at the “front door” of a network and be allowed free access to everything behind the door. This would cause many security issues since it is difficult to monitor what they are accessing pass that point. Zero trust adds roadblocks to everything they may want to access. If they do not have the right authentication they will be denied.
* **Implementation and recommendations of security policies.**
  + As stated throughout this paper, implementing security measures throughout the SDLC is important. Do not wait until the end to think about mitigating security vulnerabilities since many may be missed. I understand that corporations care about meeting time standards and want coding done quickly. However, it is our job as programmers to ensure that every block of code we write is as secure as possible.