Joshua Womack

8-2 Portfolio Reflection

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

We frequently believe that it is impossible to implement security throughout the Software and just save it until the end of the development lifecycle. Nevertheless, implementing security principles must be placed into everyday practices to lessen the dangers related with security. Being proactive requires taking on secure coding principles right out of the door. Throughout the code standards and guidelines, security must frequently be examined before any coding is finished. The gamble related with security is extraordinarily diminished, if the programmers utilize in-depth implementation from the start.

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

Threats to security can originate from any source, both internally or externally. Risk related to any decision-making process should be driven based off of daily decisions. The expense of tending to the dangers is little compared with the expense of relieving the dangers created with an un-secure system. Using very basic coding methods, performing static analysis, and conducting early and frequent tests code examinations after each code correction are helpful ways of mitigating these risks. Computerized unit testing and penetration testing must be carried out on a regular basis.

**Zero Trust.**

Zero Trust security is where all clients or programmers, whether they are in or out of the association's organization, should be confirmed, approved and consistently validated for security arrangement consistently. In order to maintain access to applications and data, this must be granted.

**Implementation and recommendations of security practices.**

The FTC has learned several lessons because technology has evolved at such a rapid pace. Normal weaknesses have influenced many of the security norms. This includes controlling access to data, user authentication, and even storing/transmitting data. Software should also be kept up to date and security patches are applied when accessible. Passwords are a requirement.