Jessie Smith

SNHU

CS 405

30 June 2024

8-2 Journal: Portfolio Reflection

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

Adopting a secure coding standard ensures that best practices, security, vulnerabilities, etc. are all being taken into consideration. This also helps ensure that security is not left to then end and prevents bugs and errors that could occur. Including security in every step of development helps ensure that we are following best practices, save time and money, and ensures that programs and software are secure.

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

Evaluating and assessing risk before it has occurred helps to avoid that risk, reduces the chances of it happening, and allows us to prepare if that risk comes to fruition. Spending extra to evaluate and assess risks helps us save money in the long run as well, preventing the risk from occurring which could result in more cost.

**Zero trust**

Zero trust is the idea that no one should be trusted with full power. Internal breaches and attacks could occur, zero trust helps us prevent that. Implementing least privilege access, authentication, authorization, accounting (triple A), etc. are all good ways to implement the idea of zero trust.

**Implementation and recommendations of security policies**

When recommending security policies, it is important to keep in mind what type of software is being created. Software that includes a lot of personal information of its users may want a heavy data protection security policy, while networks may want to focus more on detection systems and firewalls. When implementing, I think a presentation is good to ensure that everyone is on board and following the policy, as well as training sessions to ensure that everyone understands the policy fully.