Dale Ayers

SNHU

12/14/2022

[dale.ayers@snhu.edu](mailto:dale.ayers@snhu.edu)

**8-2 Journal: Portfolio Reflection**

**Secure Coding Standards & Security Philosophy**

As much as cybersecurity is about technology, it is also about an organizational philosophy. Practically this philosophy can be called a security policy. According to Ray Dunham, contact auditor for a leading CPA firm, there are specific goals that a security policy should strive towards. *"The goal when writing an organizational information security policy is to provide relevant direction and value to the individuals within an organization with regard to security" (Dunham, 2021).* Creating and applying an information security policy has a number of positive outcomes. From a policy perspective, every organization needs to put security into every aspect of its decisions. Security that is *left to the end* is a bad security policy. This is because instead of prevention and risk mitigation, the organization will be post-hock implementing half measures that may or may not be applicable once the project is finished.

**Zero Trust**

Zero Trust is a best practice to help prevent shortfalls in cybersecurity. Simply put everyone, and everything needs to be authenticated continuously. This principle is not only good for cybersecurity it also allows things like remote work to be possible. How could an organization allow remote work if they didn't know who they were letting into their systems?

**Risk Evaluation**

When it comes to risk evaluation, it is essential to understand what kind of organization you are protecting. From that, you can better understand the classification of risk you need to be concerned about. A simple example of this is the difference between a school and a bank. Both hold sensitive information, but the nature of each is different, with different types of risk involved. From there, you can start to perform a cost-benefit analysis on what is best for your organization. If you're a bank like Chase, you may want to invest in the encryption that money can buy to protect your internal communications. Different or more modest measures will be appropriate if you're the local school district, for example, or a government agency.

**Implementation of Security Policies**

My broad recommendations for the implementation of security policies are to make it a part of the working culture. I've said this several times throughout the class. Still, it's the one thing that I will remember, we can have all the most powerful technology in the world, but that doesn't solve an employee sharing their password because they don't take security as seriously as the security team. *"No one is safe"* and *"Zero Trust"* shouldn't just be coding standards of IT best practices but company-wide philosophies that everyone thinks about daily.

**References**

Dunham, R. (2021, October 26). The importance of a company information security policy. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/