**Reflection**

Hope R. Exnicious

Southern New Hampshire University

CS-405-H7070 Secure Coding 23EW2

Professor Ahlam Alhweiti

December 17, 2023

**Reflection**

As I think back on this course, which has helped me learn a lot about safe coding techniques and how they intertwine with cybersecurity, I want to talk about some of the most important things I've learned and how they've changed how I think about and approach these important topics.

Having the awareness that security is not a secondary concern but rather an essential component of the coding process has been one of the most important adjustments in my outlook. In order to build reliable software, secure coding standards must be followed. We may prevent several potential vulnerabilities from being exploited in the future by including these techniques from the beginning. The readings emphasize the importance of this proactive approach, which prevents security from becoming an afterthought and instead makes it an integral part of the development process. It's the same as installing home security surveillance prior to a break in or accident, instead of waiting for a situation to arise. It is said that is better to have and not need, versus need and not have.

The importance of understanding the balance between risk and cost-benefit cannot be overstated. There is a cost to every security measure, whether it's money, speed, or the way users feel about the system. The readings for this course stressed the need of taking a practical approach, which involves weighing the advantages and disadvantages of potential risks and then taking action accordingly. This way of thinking makes sense to me because it fits with real-life situations where resources are limited and choices need to be safe and profitable at the same time.

The idea of zero trust has completely revolutionized the way we approach security. The key is to treat every request as if it were coming from an unprotected network and check for vulnerabilities. This is true not just for hazards that come from the outside but also for those that come from inside. Moving from a security strategy based on border protection to one that is more reactive and aware of the situation is like switching to a zero-trust model. In today's world, where risks are getting smarter and come from both inside and outside the network, this way of thinking is very important.

Organizational security relies on effective security practices. These regulations, I've realized, need to be explicit, legally binding, and flexible. They should give best practices guidelines, rules for following them, and a plan for what to do in case of a security issue. In order to put these principles into action, as we covered in class, the leadership must set an example and stress the significance of security at all levels of the company.

To summarize, my comprehension of safe coding methods, risk assessment, the zero-trust paradigm, and the significance of strong security rules has been significantly enhanced as a result of my participation in this course. I'm equipped to see security as an organization's culture and mentality, not merely a collection of technical difficulties, thanks to the readings and discussions. In addition to being essential for my present coursework, this information will serve me well in my future cybersecurity-related job.

Top of Form