Katelin Kaneen

Southern New Hampshire University

CS-405-J8206 Secure Coding 23EW4

August 20, 2023

Throughout this course adopting secure coding practices from the beginning has played a crucial role in building a secure software/application. Never containing assumptions that things will be secured and working without issues. And identifying risks right away and evaluating how those might cost as they are found.

There isn’t time to play with fire but rather build the walls to prevent them and to not wait till the end. There are many key reasons to implementing them now and to not wait. This builds trust with users, reduces costs and adapts to best practices and security standards. Not only will your code be overall better for it, its helps identify those security requirements that need to be made sooner than later.

As an organization, its important to assess what potential risks might attack your software or program. By identifying those, you can figure out the impact it could have on the overall software. As we learned throughout the course, there are many risks that have higher level of severity over another. By evaluating these risks and the cost to not just continuously monitor them but to identify how and when they will be needed to monitor is important and vital for the success of your software.

Zero trust should be implemented across all levels of access between users and those who are building the software. Inside or outside the system, there should never be an assumption that those controls will be safe with the user who access them. It is always best practice to implement multiple layered security and trust with devices and users who may be using those devices and systems. There should always be security implemented regardless of who you are.

Overall, this course has taught me numerous approaches to security and implementing security standards for best practices. Implementing these standards earlier, even within the design process is best practice above all. Don’t wait to the end to think about security because it will not only cost more money but always take more time. Identify, automate and continuously monitoring all access across devices and systems to ensure that the end user can build trust that they can implement their personal data without risks.