Name: Robert Bogart

Student ID: 1674137

Program(s) of Study (Major): Cyber Security with a concentration in Secure Programming.

Adoption of a Secure Coding Standard

Starting with a secure coding standard right from the beginning helps keep security a part of the development process, rather than something you deal with later. By sticking to a set of guidelines, developers can write code that’s less likely to have common security holes like SQL injection or cross-site scripting. This approach catches problems early on, making fixes easier and less expensive. Plus, it sets a clear path for the whole team, so everyone knows they’re responsible for keeping security in mind as they code.

Not Leaving Security to the End

If you wait until the end of a project to think about security, you’re asking for trouble. Tackling security issues at the last minute usually means extra work, delays, and higher costs. Instead, by focusing on security from day one, you can spot and fix potential problems as you go. This way, you end up with software that’s not only finished on time but also secure and reliable. It’s much easier to build security in from the start than to try to add it in at the end.

Evaluation and Assessment of Risk and Cost Benefit of Mitigation

When it comes to risks, it’s all about figuring out what could go wrong and whether it’s worth the effort to fix or prevent it. This means looking at how bad the problem could be and how much it would cost to deal with it. Not every risk needs to be fixed right away—some might be minor and can wait, while others are more serious and need attention now. The goal is to find a balance so that you’re focusing your time and money on the things that really matter.

Zero Trust

Zero trust is a security approach that basically means "don’t trust anything without checking first." Instead of assuming everything inside your network is safe, you continuously verify every user and device, no matter where they are. This is especially important now that people work remotely and use cloud services. Zero trust helps keep your systems secure by making sure only the right people can access your stuff, which lowers the chances of a security breach.

Implementation and Recommendations of Security Policies

Putting security policies in place is all about setting up rules that everyone in the organization needs to follow to keep data and systems safe. But it’s not enough to just have these rules—they need to be simple, easy to follow, and kept up to date. Recommendations for security policies should focus on making them user-friendly, with clear instructions and training so everyone knows what to do. And, it’s important to regularly check and update these policies to keep up with new threats and changes in technology.