Ethan Hutchison

Module 8 Journal

Adoption of a secure coding standard is very important because of how much having a standard that is used by everyone makes everything more consistent and helps developers work together because they will understand what each other is doing for security. It is also important because it helps with security because developers will follow the standard which should be designed in a way to maximize security. One big part of a coding standard should be to not leave security until the end because it can make it harder to notice vulnerabilities and is less efficient than working on security while creating the program.

Evaluation and assessment of risk is simply looking for vulnerabilities and assessing how much of a risk they are. Doing this can help you decide which vulnerabilities need more resources and which ones don’t need as many. This helps towards cost benefit of mitigation because only using as many resources as needed saves on time and cost of running the system.

Zero trust is important because you never know where an attack may come from whether internal or external. This keeps users from getting into areas in the program where they shouldn’t be, which attackers will try to do. If an attack were to come from internally this zero trust policy still helps keep everything secure.

Implementing a security policy can be difficult because it means possibly having to train staff on the new policy and going back and changing old programs to be in line with new policies. All of this can take up development time and cause delays and more cost. On the other hand it can save money in the future and is worth the cost if it adds more trust in your systems.