Over the past eight weeks, we learned a lot about adopting a secure coding standard, in addition to not leaving security as an afterthought. One of the first things you will learn in basic programming courses is to follow established best practices for writing code. It’s not hard to understand why writing code with a focus on security is essentially one of those best practices that all developers should hope to achieve. Security is a big topic and it is not easy to implement a functional security system into a project that is already planned and developed without any focus on how security fits in or will affect the overall project or application being built.

Part of writing secure code and eventually secure applications and services requires the ability to evaluate and assess risks and the costs associated with mitaging these risks. Being able to identify likely targets for hackers and the risk associated with that vulnerability being exploited is important because as developers, we can’t defend against every single risk out there. Focusing on the risks that could be the most devistating if exploited should be a priority for those working to keep things secure and the developers who are designing and implmeneting a product or service.

Zero trust means that a system should not trust any users by default regardless of their location or device. Users trying to connect from home and users at the office will go through the same authentication and authorization prior to accessing internal resources. Most companies implement this by funneling all network traffic through a single proxy or gateway that can perform authentication, authorization, and allow the traffic to reach an internal network resource if the user has authorization and was successfully authenticated. Zero trust helps simplify security because internal services and resources need only accept connections from a single source and the sign-on server can tell the various resources what kind of authorization the user has.

Learning about secure coding and best practices is great, but it does not mean much if developers and teams fail to implement and follow the recommendations of a security policy. Part of making sure this is not an issue among development teams is educating everyone on the team about the security policy in-place, why it exists, what their role is within the security policy, and making sure everyone understands why it is so important that everyone on the team adheres with the principles and practices outlined in the security policy. As the old saying goes, you are only as strong as the weakest link in the chain. This logic is exactly why every person on the development team needs to be on the same page when it comes to understanding a security policy, why it is important, and that everyone has a role to play in keeping a project, application, or service secure.