Throughout this course, I have learned why it is important to adopt secure coding standard. Implementing a secure coding standard ensures that a project even when written by multiple people will be consistent, while also being as secure as possible. I have never been one to think that security is unimportant or that it is okay to cut corners when it comes to security, however I did not realize just how in-depth security is within IT. I did not realize just how bad of a position you can put yourself in by waiting until the end to implement all the security features or test for potential exploits within a system.

We have studied and learned about not just how important security is but also why it is important. As a company you are not only putting yourself at risk by not adhering to proper coding standards and security implementations but you also put other 3rd party companies, along with all your users and employees at risk as well. If a breach does occur you are looking at potential fines, large money losses from having to restructure all your security as well as a damaged reputation and perhaps a massive loss of users/customers. The types of private information that you potentially expose are things like names, social security numbers, credit/debit cards, addresses and banking numbers. This can have brutal effects on people’s lives as well as the company itself which is why it is so important to test thoroughly and often as well as ensure you are following secure coding standards to mitigate this as much as possible.

The zero trust (no one is safe) policy assumes that individuals, devices, and services (even those inside the network) attempting to access company resources cannot be automatically trusted. While implementing this will slow things down a little bit as authorization will have to happen more often and multiple steps of verification will be needed, it is still very important as things like Defense in Depth (DiD) still does not give you 100% protection. I imagine that zero trust does not give 100% protection either or it would be the “fix all” to software security, however implementing all these security policies on top of following secure coding standards will give you the highest chance of not being compromised. This works by not allowing access to the network unless the user’s name and IP address are authorized by the company system, and even upon trying to access the system from a verified device you still have multi factor authentication to get into the user account.

I think it is important for every company no matter the size to implement a security policy, Defense in Depth, and the zero-trust policy. It may have a larger start up cost but in the long run it is going to save time, money, headaches, reputation, and worry. As a company your primary objective is to keep private data secure as a breach has the potential to ruin you, there are a lot of different ways that security can be implemented which is why it is important to choose a policy that works the best for you. This does not mean the cheapest one, but depending on what your company does some policies may work better than others. It is important to have a few administrators but you do not need too many as the more admin accounts you have the more likely someone is to be able to get into your network. Implementing AI to do things like create/monitor logs of user and employee activity can help you spot potential malicious attacks before they happen. Having 2FA or MFA (two-factor authentication or multifactor authentication) can be a large wall for someone who is trying to breach the system. When it comes to deciding what you are going to do you can hire your own head of cybersecurity or you can hire a company who specializes in software security to come in and start implementing these practices.