**Secure Coding Standard**

The idea of not leaving security to the end is one of the most important ideas that I am taking from this entire class. I imagine it would be easy for a developer that isn’t security focused to try to meet the functional requirements of a piece of code and not necessarily worry about how security will be implemented until the module is already built, if at all. Trying to create a culture of security focused developers would help to keep security on the front of everyone’s mind and make them solve for secure code while they’re also solving for functional code. Having a security standard that everyone works to helps to drive this as a focus.

**Risk and Cost Benefit of Mitigation**

I really don’t feel like this should be much of a discussion. It doesn’t take much of an internet search to turn up the millions of dollars lost by companies to security incidents, not to mention the loss of trust that impacts their potential customers going forward. When Target had a breach years ago and lost customer credit card information, they had to deal with the fallout of people not really wanting to shop there because they were afraid it would happen again. Mitigating the risk of security will always cost less than a security incident.

**Zero Trust**

Creating a zero-trust security policy means that the company is going to have to always monitor the systems. It is a big undertaking, but it is necessary because people are always the weakest link in a security policy. Making sure that regular audits happen that allow them to monitor the networks for strange usage or keeping access limited to only what is minimally necessary can help to keep some of the risk down. If zero-trust isn’t implemented, then the security policy for the company is much weaker.

**Security policies**

Implementation of security policies is important because it sets a common standard for everyone on the team to work toward. Without this, people could have different levels of what they think is important to secure and what can be left for later. Making it standard across the company eliminates any of those questions and keeps the overall security of the company much stronger.