We need to adopt a secure coding standard from the start and use it continuously through the DevSecOps lifecycle. This will benefit us in many ways. For starters, by not leaving security to the end, we avoid having catastrophic issues that have resulted from compounding bugs and vulnerabilities that were placed into the code through the entire development process. Instead, we continuously test to ensure that each new unit/component we create is secure and upholds the standards that we live by. The combination of adopting a standard and not leaving security to the end will provide us with a great chance of mitigating security concerns in our application.

When it comes to assessing risk and the cost-benefit of mitigation, there are a few things we need to consider. When we are assessing risk, we aren’t looking at it through one dimension. We can’t simply see a problem that is likely to be exploited and jump on it. There is a cost to the time that we spend on an issue while another issue is left unfixed. This could be an unlikely attack point that holds sensitive data, but there is a vulnerability that needs patching. We could leave it as the likelihood of us getting attacked from that point is slim, but if we are attacked, the results would be catastrophic. That is the key in any evaluation. You are looking for compounding factors that could cause user data to be leaked or money to be lost. Creating a threat matrix is a useful tool to attempt to crack this situation down.

“Zero trust” is a principle that should be held tightly when constructing new systems and managing existing ones. This principle can be applied both as a security protocol as well as a user security protocol. I was reading another student’s discussion post when they mentioned public wifi connections. The “Zero trust” principle can apply in situations like that just as well. As a user, going in with the mindset that people are trying to trick you and steal your data could allow you to gain a position of advantage in a world where hackers and scammers are trying to use the internet to steal money from companies and individuals alike.

When it comes to implementing security policies. This needs to be an “all hands on deck” situation. We need everyone at a company to comply with the new policies and standards, otherwise, they won’t work. If one person decides to not use data sanitization as they are moving data from one system to a sub-system, they are putting the entire company at risk. They are essentially undoing their coworkers’ work. That is why a full adoption of security policies is essential to work towards creating a secure system and a secure company for that matter.