8-2 Journal: Portfolio reflection

I think that the adoption of a secure coding standard is important for a company. The beauty of coding to me is that there are different ways to get the same results. I think this is what make a coding standard important. One way of doing things can leave the system at risk, so making sure to tie up those lose ends can help to protect the system. Making sure that there aren’t any opening for a hacker to exploit the system is important. like what we read about sql injections. I never heard of that method and wasn’t aware that a system could allow SQL commands to be executed if a hacker was to enter them in certain fields. I found that interesting. Some as simple as doing that could open the door to your infrastructure. This is a big reason not to leave security to the end. If developers think of the methods a hacker may try to use to gain access, then they could do their best to write code that eliminates those opportunities.

When it comes to elimination and assessment of risk and cost benefit, I feel that we need to think of what exactly is at risk. If a company is responsible for keeping track of their medical records compared to say a company that stores someone’s photos, I think the company in charge of the medical records would spend more money on security vs the photo company. Not to say that the photos aren’t important but depending on what we are protecting will come into play. We should even think of things like disaster recovery. A company should have things in place if data is every locked up by a hacker. There should be backups stored at another location incase breaches happen. Now that probably costs a lot of money and time to implement and manage, but at the end of the day you know your data is safe say a breach occurs.

When it comes to zero trust, I think its important. now adays a username and password isn’t enough to protect systems. For that reason, we see MFA used for everything. You can’t change your password anymore without getting an email, and sometimes that isn’t enough. I see the purpose of it though. We learned that hackers are constantly looking for ways to get user credentials so its important to have other methods to protect the systems if those credentials are leaked. With zero trust companies would then look are the device that those credentials are being entered from. Some networks wont even except devices on them unless they have been verified. I know that at my company we make dns entries and put most devices in dhcp. This helps to validate that that device has permission to be on the network.

When it comes to implementing and recommending security policies, I think its important that all users are on the same page. Having a security policy makes sure that everyone is. Its not an option if one should be implemented anymore, it should be required. This makes sure that all users are following the same methodologies. It makes sure that the best practices are being used by everyone. It helps for user to be informed at the potential risk, and how to mitigate those risks.