Adoption of a secure coding standard, and not leaving security to the end

When I first began this course, I had barely heard of secure coding standards. I didn’t think it was all that important, but from what I have learned over the past 8 weeks, it is pretty important. This is needed to have secure code and prevent hackers from getting in. I also had no idea that some companies or people left security to the end. I thought that was insane and to be honest, stupid in my opinion. Leaving security to the end is not the wisest decision. Sure it can save some time, but you’re going to have to do it anyways. Why not make things secure in the beginning and update as time goes on? Or get to it before it’s too late?

Evaluation and assessment of risk and cost benefit of mitigation

Pretty much every risk comes with a price, and those need to be evaluated. These costs can be actual money of the company, or the company’s reputation and both are highly valued. If a breach happens to a company, not only can it cost a lot to be fixed, but customers might not trust that company anymore. Look at the T-Mobile incident, a ton of customer information (including names, credit cards, etc.) were stolen. After the breach and T-Mobile said that it was all fixed, they lost a lot of customers which is completely understandable. This can hurt a lot of companies so looking at vulnerability reports, having secure coding standards, etc. can all help prevent these kinds of costs.

Zero trust

With the job I have now, Zero Trust is already implemented so I knew what it was about. I am not only an admin, but a super admin for IT and with that comes a ton of power. Being an admin, I get to help build the defenses for the other users that work for the company, basically checks and balances. Proxy servers, cloud apps, etc. have no impact to the user thankfully, but some users freak out when they know how many authorizations just went through to get to some data. We hear all the time “What, you don’t trust us?”, and quite frankly, no, that’s the point of zero trust. We do this with devices as well. Only our company PC’s can access data, if the PC name/IP is not in our database, a user cannot get in. This helps keep unauthorized users out and preventing information getting stolen.

Implementation and recommendations of security policies

After taking this class, I believe every company should have security policies (if they don’t already) as this is the easiest way to keep the company secure. Most people think that having virus protection solves all issues, but that is not the case. My company has so many security policies but it keeps the company safe. For example, being an admin, I have to get an admin password every single morning and it only lasts 8 hours. I also have to use my phone to verify I am who I am with facial recognition to get said password. Then using that password for the applications an admin needs, I need to use my phone yet again for the two-factor authentication. While it may be extremely annoying some mornings when I just want to go into a certain database and run my reports, I get it now after taking this class. There are many ways a company can make a security policy, either they make it on their own with their security team or they can hire someone to assess the company.