Adopting secure coding standards was something that we explored through the Projects, and it was a useful exercise. It was valuable to see what some of the risks associated with various standards are, such as high probability and high severity risks, as well as some of the mitigation techniques. It also just showed me a valuable tool for creating secure coding – following a coding standard/set of coding standards to guide your code. This also helps with the next point, which is not leaving security to the end. As the Federal Trade Commission (2015) wrote, a big component of this is being cautious with information you gather – don’t gather information you don’t need, don’t retain information you need, and don’t use personal information that isn’t necessary/pertinent. All of these steps help you start with a mindset that is already thinking about security from the outset. Additionally, there are many other steps to help start with security, but the overall concept involves not making it an afterthought like designing tests AFTER all the code is designed, built, and practically ready to ship. Model threats, design with security in mind, use automated testing tools, etc – every step of the way can involve security.

We also evaluated what can happen if you do NOT practice secure code, and I investigated a LinkedIn data incident where their API was scraped and the data was sold, which could result in easier social engineering and manipulation of their users – a PR disaster. When weighing decisions about what security to include, it comes down to a cost-benefit analysis. What do we gain by increasing security? What does it cost? Though security should definitely be an extremely high priority, there will have to be certain cutoffs because you can never be 100% secure and safe. Would you spend millions of dollars and hundreds of hours to increase a minor security vulnerability? It is probably not worth it in that instance. If it was one MAJOR vulnerability – it might be worth it, especially if you’re a massive organization with more exposure.

The risk conversation leads nicely into the concept of Zero Trust. Zero Trust is exactly what it sounds like – you can’t trust anyone or anything. While that may sound harsh, Kueh (2020) wrote about the five main pillars of Zero Trust – Device Trust, User Trust, Transport Trust, Application Trust, and Data Trust. This means that IT should manage your devices (such as not using an unsecured home computer for accessing work content), user authentication methods should be secure (like MFA), least privilege access should be applied, Single Sign-On should be utilized when appropriate, and protections should be in place to prevent data leaks/breaches. So, Zero Trust is just yet another security precaution that helps us be proactive and avoid risky situations.

Finally, reading about all of these concepts and working on our security policies was great practice for implementing (or simply working with) these types of practices in the workforce. If a company I worked for had no security policy, I might try to pitch that we should have one, as I’d have concerns about our safety. Or I might view it as a red flag to start the job search and work for a more secure organization. The experience of writing the policy and presenting it just gave me an idea of what to expect in such a document – such as what I would include if given a chance or what recommendations I might include if in such a position. Basically, it’s a chance to show an organization how to put everything that we learned in this class into practice by considering what is most important and finding a way to make it come to life as a security policy.

**References**

Federal Trade Commission. (2015, June).  *Start with security: A guide for business: Lessons learned from FTC cases*. Retrieved February 16, 2023, from <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

Kueh, T. (2020, January 15). *A practical guide to zero-trust security*. Threatpost. https://threatpost.com/practical-guide-zero-trust-security/151912/