I feel very fortunate to be in a position where I am currently a “junior” in a developing role within this industry especially as I have been going through this course. So many of the topics touched on within this course have been topics of discussion within my own team as they are trying their best to acclimate me and skill me up to produce useful programs. If you were to ask me three years ago about secure coding when I started this degree, I simply wouldn’t understand what kind of practices might be used to do such a thing, nor would I be able to mention which tools I might use to help with the implementation.

“Secure coding” itself is one aspect of being secure, and it’s crazy to me that in many ways I have already participated in many secure coding practices throughout my entire life, I’ve just never really been aware that’s what the practices were called. Now I would just tell any person looking to start a business and was asking me questions about information security to really just, “have a gameplan”. Secure coding starts with first understanding the data in which your company will be processing. At a minimum there should be employees who will need to access some sort of computer, and hopefully your company is receiving some sort of financial transactions, so that data will need to be secured as well. If both of those things are accounted for, then comes the hard stuff. Physical security of the premises and the data, having a good developer who understands good coding practices, and implementing a flexible yet comprehensive policy to address current and future threats that may arise at any given point in time. In a nutshell, if you can ensure those three things, then you’ve got a really solid system in which to start working from. The thing is, security takes investment and depending on the type of business you are, may take greater investments. For instance there are many hacking tools dedicated to cracking financial institutions because your business is handling money, so you become a natural target for anyone interested in financial gain, so it would make sense to protect yourself against those inherent threats immediately. You may not always win, but you will definitely win more often than not, and if you compartmentalize and segment your data you’ll find that even when you’re vulnerable you’re never completely at the mercy of someone else. Secure coding is something that is done from the start and repeatedly improved upon. As the business grows and its needs diversify, so too must the security expand maybe even faster than the growth of the company to account for the future growth the company hopes to achieve.

When talking to people, or businesses about risk assessment or evaluating the security needs of a businesses needs I view those assessments as very circumstantial. There are many variables to consider. The amount of revenue your company processes, what type of business is being conducted, how reliant on data is your business, how many employees work for you, is your workforce primarily remote or local, etc… etc.. Considering all of these factors means that you will not just go for the first 3rd party software solution that you come across and will first assess which tools are right for you and your company. The security has to do its job, but can’t hinder productivity, or limit the growth potential of the business. There’s just so many things to consider that the answer is never a one size fits all solution. I myself really like a lot of cloud computing solutions because in general they’re just easier to set up, not as costly to maintain, however they are pretty expensive to use and depending on the level of service you need can become pretty expensive especially if you have to hire a specialist to troubleshoot your issue. Doing nothing though should never be an option. A really good example are ATM’s. ATM’s are virtually everywhere, they’re supposedly secure, however 90 percent of them even today are running on Windows XP or Vista software. This is a huge risk because even though the ATM companies have since come up with patches or updates, the businesses themselves don’t pay for the update or patches which open up these machines to all sorts of attacks. ATM jackpotting is becoming a very real and present danger for many businesses, and it’s purely because they don’t want to pay the small upfront costs of maintaining a machine because it may lessen their profits for a period of time. I’m willing to make a bet and say that if you knew the ATM was running on something like Windows XP or Vista, you may think twice before putting your credit card into, right? Now, imagine if your credit card information was hacked and you found out it was due to that ATM, I’m willing to double down on my bet and say that you probably would never use that ATM machine again. Lastly, you may be so upset, that in turn, you then sue the business that had that ATM and never updated the software for negligence, thus making that company lose even more money than if they would have just spent the money upfront to secure the machine, right? The point I’m trying to make, is that not only is there a potential loss in terms of revenue, but trust, loyalty, and in some cases the businesses validity as a whole. Security ensures your companies reliability to perform the promised service, and part of that service is ensuring the safety of all of the information willingly given to you by each consumer. Betray that trust and you immediately lose the trust of not just that consumer, but every other potential consumer that person may talk to about your company.

In terms of recommendations, honestly I can’t give overarching recommendations regarding security. However I think there are some just, general rules to abide by when thinking about security. No one has your best interests at heart, except for you. Security starts with how you regard the information that you store/process. Start with picking a secure facility. Ensure that you have a good process to ensure who has access to your facility at any given time. Once your facility is secure, all of your processing needs to start being secure. Learning about simple tools is really important. Every computer has a terminal, and every computer has the ability to network. If you can operate on a closed network, then that is ideal. However, closed networks mean internal tools, and those are expensive. If you must use a network, I would suggest using a virtual network to access your tools. Information should be compartmentalized. Your business credentials should never be stored alongside customer credentials. Credentials should never be stored alongside user information, and financial information should always be stored elsewhere as well. The point is, don’t put your eggs in one basket, ever. Finally, be consistent, and ensure your consistent with a policy that you and your coworkers can abide by. If you can’t abide by your own rules, then it’ll never be followed. Make sure you can adhere to the principles.