Sera Hill
CIDM 6341-70

**Personal Risk Assessment**

To better understand my personal surface attack area, risk posture and risk appetite, a personal risk assessment is important to perform on oneself. For the personal asset inventory and personal risk assessment, I audited my assets for each of the systems as described by the NIST Risk Management Framework. These systems included people, procedures, data, software, hardware, and networking. From this list, I chose five assets with one from each group as well as a system to perform the risk assessment. The specific assets I chose for the risk assessment are as follows: myself, my physical mail handling procedure, my daily planner, the Apple Wallet app on my phone, my personal laptop, and my home network system. To calculate the risk value, I used the formula provided, as well as used the values predetermined by the example for ARO, control effectiveness, and priority.

To conduct this inventory, I first focused on the first category of people. I went through the contacts on my phone, social media friends and family members to determine who might know personal information about me that could potentially be compromised in some way. For procedures, I had taken a few days to make note of what I did consistently for each day and made note of anything I did repetitively as far as handling emails, regular mail, and daily routines. Next, I went through all items that could potentially hold personal data by going through each room in my house, my purse, and even digital devices like my laptop, cell phone and smart household appliances. Next, I went through any kind of software that may hold my personal data on my laptop, phone and iPad as well as hardware which ended up being a similar list as the data section. Finally for networking, I have my WiFi router and two WiFi extenders.

The categorization for my personal information assets were based upon the NIST Risk Management Framework and categorized based on those systems mentioned above. From there, per the assignment requirements, I then selected five assets and one system to examine for my risk assessment. To identify possible threats and vulnerabilities, I looked at Confidentiality, Integrity, and Availability to determine where those risks might lay. For prioritization, I looked at how much I would be affected should that asset be compromised

in any way. If it significantly affected my day-to-day operation, it was classified as high and the asset value was quite large as well. To determine the value, I looked at things like my yearly salary, how much the item in question was worth, money in my connected bank accounts, what it would cost should there be any legal fees associated with certain vulnerabilities, and cost of retrieving information or appointments stored in those assets. I selected my home network system as the system category for my risk assessment. This decision was based on its role in connecting various assets (such as my laptop, phone, and smart devices) and its potential vulnerabilities that could impact multiple areas of my daily activities, especially since I am an online student and a hybrid-remote employee.

Following the personal information asset inventory, a risk assessment was done on five assets and one system. I will discuss the person information asset first which is myself. I have come up with the Asset Value of $505,800. This amount comes from five years' worth of my annual salary ($400,000), cost to replace my computer ($1,500), how much my car is worth ($36,000), amount I typically have in my personal bank accounts ($18,300) and any potential fees associated for any data breaches regarding my job ($50,000). For the most part, each threat categorization is rated as high because things like losing power, no internet connection, and oversharing personal information on social media would affect my day to day life pretty drastically. With that said, I believe the controls I have in place such as minimal drinking and no drugs (0.9), and always locking my computer before getting up from my desk (0.8), are quite strong and help prevent breaches for confidentiality, integrity, and availability. My uncertainties for these items are also quite low as I am confident in my ability to abstain from overdrinking or doing drugs, and I am always in the habit of locking my computer while away. The overall risk value is $140,936.

For the procedure asset, I examined my physical mail handling routine. To determine the asset value for this, I looked at which bank accounts were connected to my paper bills which include my own personal bank accounts as well as any other joint accounts I share. This value ended up being $38,000. The threat categorization values for this asset were also rated as high. This is because any compromise, such as unauthorized access to my mail or accounts, could expose sensitive personal or financial information. This would not only

harm my financial stability, but it could also lead to identity theft or fraud, which would have a detrimental impact on my livelihood. Unfortunately, I think the way I handle this asset could use some improvement. I do store some mail in a filing cabinet in my house (0.6), but when I am ready to throw it away, I typically tear it up a few times and throw it in the regular trash can (0). I noted I should invest in a document shredder to shred these personal documents when they are no longer needed to reduce the potential risk associated with this asset. The overall risk value is $22,800 which is the highest risk value to asset value ratio I have compared to all other assets.

The next asset I chose to look at for the data category is my daily planner which includes any scheduled meetings I have for work, when vacation is planned, after school activities for my daughter, and any doctor appointments I have. I came up with the value of $500 for this asset which includes the cost to replace the actual planner ($30), cost to reschedule missed appointments ($100 – average $25 per doctor's office), time spent to get that information back ($100), estimated cost for missed client meetings ($270). Overall, the threat for this category is quite low. I take strong precautions to minimize the chances of my leaving my planner in public spaces by only keeping it at work or home (0.8), I refrain from recording extremely sensitive information in my planner like account numbers, passwords, etc. (0.9), and I keep a backup of scheduled appointments in other places such as the calendar on my phone or computer (0.9). The control I listed for my planner that I could possibly implement to further enhance the security of this asset would be to lock it in a drawer in my desk when I am away from my desk for an extended period. The risk value for this asset is $35.36.

The next asset is from the Software category, and I chose to assess the risk associated with the Apple Wallet app on my phone. To determine the asset value for this, I accounted for the average amount of money I keep in the account tied to my Apple Wallet which is roughly $6,000. The threat categorization for this asset is high as any compromise to my bank account would negatively impact my financial situation. With that said, the controls I have in place currently such as keeping my phone password confidential (0.8), being able to quickly freeze my bank account if needed (0.8), and always knowing where my

phone is located and not leaving it out anywhere when I am in public (0.9) are all high controls and am confident in my current ability to keep this asset secure. A control I should think about implementing to further increase the security is possibly changing the password to get into my phone yearly to avoid potential hackers guessing what my password is. This is important in case someone was to find an old password I have used in the past, and adds to the difficulty of an unauthorized user accessing my phone. The overall risk value is $165.

For the final hardware asset, I chose to do the risk assessment on my personal computer. To determine the value, I looked at the cost to replace the computer ($1,500), and the cost of losing the information stored on it which includes all my school notes since January 2022, online records for my house, etc. ($5,800). The threat categorization for this is high because I do depend on having my computer for a lot of things regarding online bills and my school work. The current controls I have in place such as keeping my password confidential (0.8), always locking my computer when not in use (0.8), and keeping my computer at home (0.8) are all quite strong for me. I have a low level of uncertainty for each of these controls just because there are minimal ways for an unauthorized person to get ahold on my laptop. One thing I should probably start doing is updating my password annual to reduce the risk of somebody guessing what my current password is. The overall risk value associated with this hardware asset is $255.50.

For the system, I chose to do the risk assessment on my home wireless network. To determine the value of this, I looked at the cost of the actual equipment like the router ($100) and wifi extenders ($200), the monthly fee I pay for the service ($80), as well as half a day's salary ($200) as that is usually the amount of time my internet has ever been down. I felt it necessary to put my pay in the asset value since I do work from home some of the week. This resulted in an asset value of $580. The controls I have in place to help prevent this from happening is using a private password to connect to the network (0.8) and keeping the router's firmware updated (0.8). To further secure my network, I could make the WiFi network invisible from scanning devices and use a mobile hotspot as a backup in case I were to lose service. The overall risk value is about $82.36. Even though I have quite a few

smart devices/appliances, I do not rely on an internet connection to use them and most are not even connected to my WiFi so I did not factor them into the vulnerabilities as it would not matter to me if they were connected or not.

In conducting this personal risk assessment, I gained valuable insights into my risk posture and the areas where I can improve my security practices. All in all, my overall risk posture is moderate as I have some major controls in place to protect the highest valued asset, but there is still a lot of room for improvement. For the majority of the assets listed, the percentage of risk fell below 30%, with my procedure at the most risk of 60%. This supports my conclusion that my risk posture is moderate. My risk appetite levels are generally moderate as I do allow some risk, but the risk (for the most part) does not exceed the asset value. For example, I am okay to do with minor internet service disruptions, but I put more controls in place to avoid identity theft and data breaches. To help balance my exposure to risk, I do implement strong controls for the areas I feel are the most important like myself, data, software, hardware, etc. Ultimately, this exercise has highlighted the importance of self-awareness and makes me think more about how I handle things and what opens me up to potential risk. Assigning actual monetary values to these items also brings to light how important it is to stay secure and vigilant to any possible risk.