Megan Moore
Buff ID: 1014735

Personal Risk Assessment

In order to truly do a proper inventory of one's assets and what potentially could bring the most risk, you must first fully know yourself and your own behaviors. A risk profile if you will. While this sounds simple, it can actually be somewhat challenging. Taking a look at myself, I perform many different roles. I am a graduate student, a full time Technology Business Analyst in an IT/Financial services company, a mother of two kids and I live out of town from almost all family members and relatives. Each role represents only a portion of who I am or what I do. Over time as I've gained each role, I have noticed a change in my patterns and hobbies. Upon first finishing undergrad, I was vastly more risk happy and took on almost any challenge or curiosity that peaked my interest. The value of my assets could be said to be lower at this point as income was lower, intellectual property hadn't truly begun to grow and training was beginner. The next phase was becoming a parent. I'm sure most people who become parents also adjust their lifestyles and behaviors as well. Hobbies which were more intense or riskier have either been paused or replaced, such as sky diving for myself and accumulation of higher income and retirement accounts. When asset values rise, one is apt to lower risk and be more purposeful in their exposure. Then when I started graduate school, I became even more intentional in my career choices and invested my time in pursuing certifications as time became a most critical resource. For my career, I began to focus only on opportunities which brought the best benefits, work life balance and joy for my mental health. Work environment plays a crucial role in many things as so much of our days are spent working and with our work colleagues. This again, in turn raises the value of my personal assets, such as myself, and pushes the need to lower risk in best practice for protecting my personal assets.

Assets which are part of a system come in many forms from people to procedures and physical hardware to digital data. Each asset should reflect both a sensitivity as well as security priority. Risk is assessed based on the likelihood of adverse events and effects on information assets when a risk event occurs. Defining the appetite you have for risk and uncertainty of exposure to loss is the next step in building a personal risk profile. Risk tolerance is one's ability and willingness to accept the tradeoff between potential loss in favor of a chance of some kind of possible gain. Most people tend to focus the lens of risk tolerance specifically in terms of financial decisions but there's risk in all aspects of life. Understanding the risks you are exposed to can help you to plan for them and make better informed decisions. I would definitely say I am not a conservative individual. I tend to take chances on things where I feel the payoff or resulting experience justifies the risk. Am I a gambler willing to aggressively risk everything for a chance? Absolutely not. When it comes to information security or assets, risk tolerance is the amount of data and systems which can be risked to an acceptable level and still be protected against confidentiality, integrity or availability compromises. Many drivers play into this but the key ones to keep in mind are privacy risks, data/asset value, personal preferences and industry/competitive pressure. Another important factor is risk tolerance doesn't always remain the same. It can shift over time because as your goals or priorities change, the strategies you use to achieve them follows that change. All sorts of things play a factor from age, environment, family, market conditions, income, past experiences and overall subject knowledge. I have noticed this shift time and time again throughout my own life and personal experiences. How well you can recognize, plan, adapt and accept risk is key.

Megan Moore
Buff ID: 1014735

Personal Risk Assessment

When completing my own personal asset inventory, I felt I needed to conduct the identification process in a systematic way. I felt I needed to approach this very methodically because so much risk around things one is used to handling or dealing with every day simple feel benign or so routine, you don't actually stop to think about what you are really doing. Similar to locking the door when you leave your home, it's easy to get down the road and then question if you locked the door or not as the motion is extremely routine and not truly focused on. For myself, I took a hard look at my routines and which assets are touched by them. I debated back and forth on how to group, whether by people or type of data but I decided routine frequency would be best for me. This is how I grouped my assets. Some of my routines are daily, while others are monthly, quarterly or even annually. Within each routine, every type of system component is involved. People, procedure, data, software, hardware and networking.

Creating an inventory is essential for managing assets and thus, by extension, mitigating against information asset risks. After compiling my own inventory and beginning to think of the value and priority behind everything I identified, I can state that an information asset inventory is truly one of the most crucial information assurance principles as it requires every single asset be accounted for. Looking ahead, doing this inventory should next aid in determining the level of protection the asset needs within my own security plan to mitigate threats. When completing the inventory assignment, I sought to answer the question "How can you expect to protect important personal information (assets) if you don't even know what all you have?" Relevance is everything. One important thing I also learned from taking an asset inventory and then grouping those assets as a system was how to then categorize that system. Categorized systems are described in terms of security category information type such as confidentiality + impact, integrity + impact or availability + impact. Each of the three types listed (confidentiality, integrity and availability) represent security objectives. The FIPS 199 definition for each is listed below.

- A loss of confidentiality is the unauthorized disclosure of information.
- A loss of integrity is the unauthorized modification or destruction of information.
- A loss of availability is the disruption of access to or use of information or an information system.

From that, the categorization process is able to more easily determine the potential impact for a threat. Aside from threat impact which is highly important to assess, overall relative value of information assets is key in order to determine which asset should be given the highest priority. The main thing I felt I should reflect on is what key assets loss or compromise could cause the greatest liability to myself or immediate family. Once categorized, I was able to more clearly identify vulnerabilities in instances of where I might disclose information I had not agreed to or accidental exposure from phishing type attacks. Most of these types of things I determined I could mitigate through either covering myself with liability insurance or accept the risk where both probability and uncertainty were low.

In the inventory assignment, I decided to group my systems by routine. I started first with the routines that happen less frequently – annual types of routines. This first system would include visits from key people such as relatives, filing tax returns, renewing policies such as home or car insurance, renewals of software or app memberships like Amazon prime or PMI, and even decorating the house with things like ornaments made by my child from fingerprint paint every year. Next were the more

Personal Risk Assessment

common routines practiced from monthly to quarterly time periods. This second system would include data such as month end bank statements, utility bills, reviewing monthly scheduled doctor appointment cards thumbtacked to a board, requesting a quarterly pest spray of my home or reviewing monthly credit card statements and credit score reporting. Finally, the third system would be anything used in my daily routine, whether for work or personal use. Upon grouping my inventory list this way, I also recognized that some assets are used multiple times depending on the procedure I happened to be currently going through.

To complete this Risk Assessment Assignment, I select five of my assets I identified during the inventory assignment. I selected one from each asset group: person, process, data, software, hardware. I identified each based on the frequency I might interact with the asset, how much impact the loss or disclosure of the asset could expose me and how much personal harm the exposure could bring. Under each explanation, a snip of the template calculation is displayed.

For the person information asset, I selected myself. As this is myself, the priority would be the highest value of Vital – any disruption to my person through death or illness would have immediate impacts. Threat was categorized as confidentiality of high; integrity as high; availability as high as I am depended upon daily for many things both personal in family and for work. Probability of attack is high as I am exposed to phishing attacks every day but with effective controls in place for how to behave along with a low uncertainty as I am aware of best practices to avoid accidents through driving or through personal impairment which can happen through drinking. Being a responsible person on top of a parent almost rules uncertainty to zero but there's always a chance so I set that to .1.

Asset Name	Description	Sys ID	CIA Asset Value	Priority	Threat Categorization	Vulnerability Description	ARO	Controls in Place	Control Effectiveness	Uncertainty	Risk Value
Myself	Myself as an individual and the things I represent - income, retirement/savings accounts, etc. Value represents income for 10 years at $100K, existing retirement accounts of $250K, and legal costs of $100K in the case of stolen identity.	System 3	$1,350,000.00	Vital	Confidentiality - High	Unauthorized disclosure of personal information - identity theft, accounts hacked	1	Experience to avoid unsafe circumstances; Training to not fall for typical phishing attacks	0.8	0.1	$ 297,000.00
					Integrity - High	Accident - through own impairment through alcohol or vehicular wreck	0.1	Drink conservatively; carry full accident insurance coverage	0.8	0.2	$ 32,400.00
					Availability - Moderate	temporarily unavailable when ill or on vacation	0.1	Follow phsyical healthy plan; avoid large gatherings of potential ill people	0.8	0.1	$ 29,700.00

For the data information asset, I determined the best item here was my main credit card. This asset was categorized with a priority of critical (loss/theft of card would be a disruption that can not be dealt with after only a couple days at most). The threat categorization would be confidentiality as moderate as only a few details are exposed with my card such as the card number, name and perhaps billing address; integrity as moderate as card theft does happen occasionally and thankfully banks have policies in place to freeze the use of the card should unauthorized transactions occur; availability as high due to restoration priority of the asset high as it is needed to pay for bills, daily expenses, etc.

Asset Name	Description	Sys ID	CIA Asset Value	Priority	Threat Categorization	Vulnerability Description	ARO	Controls in Place	Control Effectiveness	Uncertainty	Risk Value
Credit card	A key personal type of ID. All centrally located with my wallet. Value represents full amount of credit line.	System 3	$ 80,000.00	Critical	Confidentiality - Moderate	Exposure of personal details - name, card number, credit line	0.9	Bank can freeze use, cancel card and reissue new one quickly	0.7	0.2	$ 25,920.00
					Integrity - Moderate	Card theft occurs due to data breaches at stores, online, etc.	0.9	Ability to protect credit line and charges	0.7	0.2	$ 25,920.00
					Availability - High	Card use restoration necessary due to daily charges and monthly expenses	0.9	Backup credit cards setup on accounts; significant other able to cover expenses in short term through emergency savings account that is separate	0.7	0.2	$ 25,920.00

For the procedure/process asset, I chose my vacation routine process which I placed a priority of high – vacations typically last 5-7 days when I would be potentially not easily available depending on my

Megan Moore
Buff ID: 1014735

Personal Risk Assessment

location. Threat categorization would be confidentiality as high due to the safety exposure of myself and family members along with the risk of leaving our home and other assets behind unattended for that period of time; integrity would be moderate as people do take vacations and sharing of this knowledge to key contacts is necessary such as employers, coworkers and any services such as pet sitting; availability ranked as low as this is not frequent with travel typically only planned for 1-2 trips a year.

Asset Name	Description	Sys ID	CIA Asset Value	Priority	Threat Categorization	Vulnerability Description	ARO	Controls in Place	Control Effectiveness	Uncertainty	Risk Value
Vacation routine	Setting of alarm systems, running security cameras, confirming spare key is available for emergency contacts to use	System 2	$ 470,000.00	High	Confidentiality - High	Safety concern to both myself/family members traveling along with assets remaining behind unattended	0.8	Alarm systems established along with key contacts for emergency access to home, accounts, etc.	0.6	0.4	$ 210,560.00
					Integrity - Moderate	Strangers do not know when to break in as they do not know your schedule unless you advertise it	0.7	Trips not shared on social media until completed so should access to these be broken into, there is no knowledge we are not home	0.6	0.1	$ 144,760.00
					Availability - Low	Frequency is low for travel throughout year - was zero during times of Covid-19	0.5	Routine updating of security systems and account access	0.6	0.1	$ 103,400.00

For my hardware asset, I chose my cell phone. My phone is a critical information asset due to the frequency I use it along with the access it has through contacts and software applications to all my accounts such as banking, work profile, emails and social media. Due to this, the threat to confidentiality and integrity are both high because of the liability and personal damage a phishing attack would warrant. Availability as high as access to my phone is a massive necessity for personal and work calls, daycare or school contacts for children, email access for accounts and password resets and finally all social media profiles and pictures saved on the phone. Controls in place are locked profiles, fingerprint access, and the ability to remote wipe the phone in case of it being stolen or misplaced.

Asset Name	Description	Sys ID	CIA Asset Value	Priority	Threat Categorization	Vulnerability Description	ARO	Controls in Place	Control Effectiveness	Uncertainty	Risk Value
Smart Phone	Tool which has access to many personal datas or other information assets like social media accounts, work email, etc. Value represents phone cost of $1000, personal asset disclosure of $300K and work related exposure of $300K.	System 3	$ 601,000.00	Critical	Confidentiality - High	Unauthorized disclosure of personal and work information	1	Work from home reduces potential to leave phone unattended or misplaced	0.8	0.1	$ 132,220.00
					Integrity - High	Unathorized use for work could be severe; access to all personal banking and social media accounts	0.9	Phone encryption and passwords in place for both personal and work profiles saved on hardware. Can be remotely wiped.	0.9	0.1	$ 59,499.00
					Availability - High	Used at all times for calls, account access	1	Can be replaced shortly if damaged	0.7	0.1	$ 198,330.00

For my software asset, I chose my social media accounts: Facebook and Instagram profiles. The priority of these accounts I felt would be high as a disruption or loss of account could spread quickly through my network if odd posts were made. People would notice after a few days and then reach out to check in. Threat categorization would have confidentiality as high due to the amount of contacts each profile touches; integrity as high based on the type of content shared on these social media platforms; availability would be low as posts do not occur every day.

Asset Name	Description	Sys ID	CIA Asset Value	Priority	Threat Categorization	Vulnerability Description	ARO	Controls in Place	Control Effectiveness	Uncertainty	Risk Value
Social media profiles	Facebook, instagram - contacts, synced profiles	System 3	$ 150,000.00	High	Confidentiality - High	Personal information - images, contacts, names could be exposed through an attack	0.7	Limit devices which can login to accounts	0.7	0.4	$ 44,100.00
					Integrity - High	If hacked, reputation can be harmed through what is stolen or shared without permission	0.7	Password reset enabled should I be unable to access my account	0.7	0.4	$ 44,100.00
					Availability - Low	I do not share posts or look at these accounts every day so I do not need access every day	0.7	Low need to share personal experiences	0.7	0.4	$ 44,100.00

After completing the above reviews for each asset grouping – I looked at my overall asset inventory and I felt the most important thing to identify and analyze was the one asset that was weakest or could expose me to risk the most. For me, that system is my google email accounts. I have two specific google

Megan Moore
Buff ID: 1014735

Personal Risk Assessment

email accounts which routinely are used for all my communications or transactions such as bill payments, password reset inbox, career communication, personal contacts and family private information. Opening up my google email accounts would quite thoroughly tell a story about me, my life, my interests and things relating to my career and those close to me. This would rank this system as confidentiality high (large impact to damage if email access is exposed); integrity would be high as if exposed, the damage to reputation could be severe if mass password resets to other accounts are done as they route to these emails; availability would be moderate as I can go a few days without my email account, such as busy work days or vacation trips when I typically do not login. The vulnerabilities and threats to this system would be my login credentials if stolen by a browser/phish attack or key logging type software installed on a computer that isn't mine. The controls I have in place would be never using unsecure internet hotspots or public computers to log into my accounts along with a personal antivirus software to help aid in reducing a phishing attack.

This assignment was very enlightening in visualizing my own overall risk. Risk identification, which I began in the inventory assignment, is crucial to being prepared, not just for personal reasons but also for the role we each play in organizations and society. In my current role as a project manager, I'm constantly reminded of the responsibility of identifying and managing risk through the life of a project. Tools like an information asset inventory are wonderful aids in that endeavor. To manage personal risk, we need to know ourselves. Knowing ourselves involves understanding how information can be collected, stored or transmitted. It also requires the ability to identify information assets which are valuable to our personal selves, classifying each of those assets and then determining how each is protected from threats. Overall, I would say my risk is moderate based on my behaviors and current controls in place. I would like to spend time reviewing how I can place additional controls to safeguard my information assets more. Some risk I am willing to accept, in the example of using a smart phone as the high usage and necessity of being connected is very important and frankly nonnegotiable.