Sera Hill
CIDM 6341-70

Personal Information Asset Inventory

What Did I Do?

To create a comprehensive list of my personal information assets, I followed the six groups of information assets presented in the presentations for this week's topic, "Assessing Risk". The following are the six categories: 1 - people, 2 - procedures, 3 - data, 4 - software, 5 - hardware, and 6 - networking.

To determine the list of my people information assets, I went through my text messages in my phone. This helped me determine who I communicated with the most. I then went through the rest of my contact list on my phone to determine other people I contact but may not talk to frequently, so I grouped them together. I then noted the people I have as friends on my social media and other accounts that have a "friends list" which include Facebook, Instagram, LinkedIn, Goodreads, and Spotify.

Next, I recorded my daily routines over the course of a few days. I discovered I had certain patterns that I repeated every day. I have regular things I do in the mornings when I get ready to go to work and get my daughter ready to go to school. I do the same kind of things when I come home during lunch from work. I also have a nighttime routine that involves me getting my daughter ready for bed, and then what I do for myself when I get ready for bed. I also follow certain steps when I check the mailbox outside of my house, and how I handle emails that I receive on my personal and school email accounts.

For the data category, I split up this section into physical and digital data. To determine my physical data, I went room by room and took inventory of what kind of data was held in each room. I started with the rooms and closets in the front of the house and worked my way to the back rooms, ending with the basement. This included files and documents stored in closets, receipts and credit cards in my purse/wallet, documents like tax returns, mortgage information, bills, and my marriage license that is stored in a filing cabinet in the basement. I went through my purse and wallet to determine what other hard data was in there like credit/debit cards, banking information, and receipts. I also considered notes I have collected in notebooks for school and work. These notes give insight into what my knowledge base includes, what kind of information I collect during work, and even small details about myself including personal interests. In addition to these more freeform notes, I also keep a daily planner that includes my daily tasks, meetings, doctor appointments, vet appointments, and any afterschool activities or weekend trips. The filing cabinet I have contains previous tax return information, and paper bills from the last couple of years.

The digital data category has a lot more data associated with it than the physical data as I have most of my bills and account information delivered and stored electronically. Also, with the presence of social media accounts, and the fact that mostly everything is a subscription service now, the amount of digital data a single person has is staggering. To take an inventory of my digital data, I first audited my phone. I went through each page of apps and took note of what types of data were contained in each that could be accessed by my phone. I went through a similar process with my laptop by going through the list of applications installed on my computer and noting what kind of data was stored and accessible from my computer for each application. Again, this process was repeated for my iPad, and smart watch. I went through a similar process for my work computer. This obviously has more data associated with my job, but I do have personal data tied to that device as well such as work history, contact information, browsing history, and personal interests. Then I moved on to the items that held less personal data, like the smart appliances and other smart devices in my home. These devices are connected to my WiFi network, but that’s about it.

For the software section, I went through each of my devices with software installed on them. First, I checked my phone and created a list of applications that I used the most. I repeated this process for my personal laptop, work laptop, and iPad. For each device, I also grouped the applications that I have installed on them, but do not use on a regular basis or not at all. In addition to the applications and programs on my computer, I also audited my most frequently visited websites that I have login information saved to my browser as well in this section. Even though they may not be programs installed on my device, it is still accessible from my devices and holds information about myself.

Next, I audited the hardware throughout my house, going room by room again and taking note of everything in each. This list also includes some of the items in the data section as I felt it made sense to include them in both areas. One, because the hardware itself hold data, and two, the devices are actual, physical items. For the last category, Networking, I only had the WiFi Router to add and two WiFi extenders. I also included the router in the hardware category as well because it is still a physical piece of equipment.

What Were the Results?

Doing this activity really helped me become more aware of how many information assets I have, and it made me think about the things I own in a different way. For me, it's easy to forget that smart devices have a means to connect to a network, which means they are also vulnerable to attacks. My personal attack surface is quite large, and it surprised me just how large it is. Each of the assets I noted adds to my attack surface by serving as a potential entry point for attackers. For example, the number of devices I have connected to my WiFi network increases the number of ways hackers could exploit. Also, my social media accounts store personal data that provides another possible vulnerability. It is also interesting to see how much it can and probably will grow over time with the creation of even more smart devices and new things in which you must have an account for.

The amount of physical data was interesting to see around my house as well. After doing this audit, I discovered there are many different areas in my house where physical data is located. One thing I need to work on is how I store that physical data and what I do to protect it or get rid of it when I don't need it anymore. My disposal of physical data could do with some improvements.

It was interesting to see how much data is stored on my phone alone. It contains my contact information, banking information, location, frequently visited locations, personal interests, and social media information. A lot of this digital data is repeated on my laptop computer, with some variances as to which apps track my location, document storage, and the addition of different apps not available for my phone. Even though a lot of these items were repeated in different categories, it makes sense to put them in more than one to account for not only the fact I have a certain program on my computer, but also to be mindful of the data it holds about myself.

With that said, the size of my personal attack surface is even larger than I originally thought. Going through the inventory and discovering how much personal data is accessible made me see there are many ways I could be compromised. For instance, my family and close friends, who know a lot about me, could unknowingly share personal information that might help hackers figure out passwords or common phrases used for security questions. Additionally, the number of connected devices and accounts I use increases the potential access point for hackers, especially if I don't have these systems properly secured.

While this exercise was for my personal assets, I can only imagine how much more involved it would be completing this for a business. However, it is a crucial step to take when learning about your organization and creating ways to defend it from possible hackers. The quote by Sun Tzu mentions that if we do not know ourselves or our enemy, we will always lose the battle. Completing an information asset inventory for a company can help shed light on the different areas of possible vulnerabilities and provide guidance on where they should beef up their security and educate their employees.

What Did I Learn?

One thing I've learned from this that stood out the most was just how much information assets cover. It's not just an online presence or data you have stored in a computer, it's quite literally everything you have or people you talk to that have some kind of information about you. You should discuss with family members how to handle external inquiries about your family so they don't accidentally leak information that should have been kept secret.

I also learned that many items throughout my household fall under different categories than just one. This has helped me thing about different ways an item like a phone could be compromised. For example, if my phone was stolen and the thief was able to gain access into my phone, they could gain access to my bank accounts, credit card, personal information, and even contact family members. I've learned just how much everything I have is connected as far as devices and accounts, and it is likely if one item gets compromised, it wouldn't be very hard for others to be compromised as well since login information is shared.

As mentioned before, even though this exercise was for personal assets, it's easy to see why companies should perform this type of inventory on themselves. It would be very beneficial for them to perform a regular audit of their assets so they can be sure they are aware of potential areas of weakness. Having this comprehensive list of assets will help companies create a security plan that reduces their attack surface. Additionally, the list of information assets could help inform organizations on where they might be able to use tools like Recuva and CCleaner for proper data deletion or recovery.

Sera Hill
CIDM 6341-70

References

Jennex, M. (2021). Threat Analysis and Risk Assessment. [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-3042018-dt-content-rid-56699107_1/xid-56699107_1