**Name:** Amarachi Anthony

**Buff Id:** 1130441

**Course:** CIDM 6341(Cybersecurity)

**Assignment**: [**Personal Information Asset Inventory**](https://wtclass.wtamu.edu/webapps/assignment/uploadAssignment?content_id=_3042020_1&course_id=_66575_1&group_id=&mode=view)

**What Did You Do?**

For this exercise, I followed a systematic approach to conduct an inventory of various assets, focusing on categorizing them into people, hardware, software, data, procedures, and network components. The objective was to gain a comprehensive view of my digital and physical environment and identify the potential areas of risk.

First, I began by placing key individuals in my personal and professional circles into categories such as family, friends, social media contacts, and work colleagues to establish different levels of access and interaction within my digital environment, which could pose security risks.

Next, I documented all the physical devices I frequently use, including household appliances and personal electronics like televisions, laptops, cameras, and radios. Each device was categorized under hardware based on its function and connectivity. Many of these devices, especially those connected to the network, could be targets for cyber threats.

I listed applications and programs currently installed and in use in the software category. This included mobile apps for banking and communication, school-related software, antivirus protection, and office productivity tools. The software group was divided into specific categories, such as security apps, work-related apps, and entertainment platforms, to better understand their potential security risks.

For the data category, I focused on both electronic and soft data. This included phone contacts, email accounts, and school-related data stored on my devices. Sensitive information such as social security numbers, birth certificates, and financial records were categorized as soft data, representing high-value targets for potential cyberattacks.

I also included procedures in my inventory. These are daily tasks or routines, such as starting work, eating dinner with family, or meditating. While they are not directly technical assets, these routines represent patterns in my use of the devices and data, which could help understand behavior patterns that may introduce vulnerabilities.

Finally, I reviewed my network components, particularly the home router and wireless devices that connect all other hardware and software, as they are crucial for securing access to the broader environment.

In cases where assets could belong to multiple categories, such as work-related contacts or devices used for personal and professional purposes, I placed them in their primary function category. For instance, work-related apps were placed under software, and laptops used for personal and work purposes were grouped under hardware, cross-referenced with their associated functions.

**What were the results?**

**Asset Inventory and Risk Assessment Table Template**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Asset Name** | **Description** | **Sys ID** |
| P1  P1A  P1B  P1C  P2  P2A  P2B  P3  P3A  P3B  P4  P4A  P4B | **People**   * Family * Ng * Olu * Nne * Friend * Nk * Ezzy * Social Media * John * Peter * Work * James * China | Family Contact  Sister  Sister  Sister  Close Friends  Best Friend  Neighborhood friend  LinkedIn /Instagram  LinkedIn Contact  Instagram contact  Coworker  Coworker | PE1  PE2  PE3  PE4  PE5  PE6  PE7  PE8  PE9  PE10  PE11  PE12 |
| PR1  PR2  PR3 | **Procedures**  Meditation  Start Work  Dinner | Start the day with meditation and prayer  Go to work  Eat with family for the night | PRA1  PRA2  PRA3 |
| D1  D2  D2A  D2B  D2C  D2D  D2E  D2F  D3  D3A  D3B  D3C  D3D  D3E  D3F  D3G | **Data**   * Electronic data   + Phone Contacts   + Email Contacts   + Laptop Data   + Social Media   + USB Drive   + Cloud storage * Soft Data   + Birth Certificate   + School Degree   + Driver’s License   + Social Security Card   + Credit /Debit   + Resume   + Car | Data stored in a digital device  Phone contacts’ number  Email account  School and work data saved  My work history is stored on LinkedIn.  My school and personal info saved  Personal/work data on google cloud  Information on my computer desktop  Family birth certificate  School transcript and results  Identification information  Nation security number  Banks/credit cards  Work and personal history  Registration, insurance, and car maintenance manual. | DA1  DA2  DA3  DA4  DA5  DA6  DA7  DA9  DA10  DA11  DA12  DA13  DA14  DA15  DA16 |
| H1  H2  H2A  H2B  H2C  H3  H4  H5  H6  H7  H8  H9  H10  H11 | **Hardware**   * Digital Electronics.   + Televisions   + Radio   + Laptop   + Fans   + Cameras * Appliances.   + Fridge   + Oven   + Microwave * Car * Sudan * SUV | Hardware devices  Digital Electronics  Living and bedrooms Televisions  Living room and car radio.  Computer device for school and work  Fan for hot weather and cool temperature  Taking pictures and store for future remembrance.  Household food devices  Kitchen and garage fridge  Kitchen and balcony oven  Kitchen Microwave  Toyota Rav4  Sienna | HH1  HH2  HH3  HH4  HH5  HH6  HH7  HH8  HH9  HH10  HH11  HH12  HH13 |
| S1  S2  S3  S4  S5  S6  S7  S8  S9  S10  S11  S12  S13  S14 | **Software**   * Phone apps * Banks Apps * School Apps * Social Apps * Laptop software * McAfee * Microsoft Office * Management Studio   TV Apps   * YouTube * Ruko | Bank apps and other applications  WTAMU App for school material  social networking apps, (What’s App, Facebook, and LinkedIn)  Software inside my laptop system  Anti-virus protection  Word/Excel/PowerPoint  SQL coding software  Social media /entertainment  Streaming Software | SS1  SS2  SS3  SS4  SS5  SS6  SS7  SS8  SS9  SS10 |
| N1  N2  N3 | **Networking**   * Router * Wireless Router | Internet provider box  Digital device box | NN1  NN2 |

The outcome of this asset inventory highlighted my attack surface, which represents the points in the system that could be vulnerable to attacks. By cataloging these assets, I was able to better understand the potential risks associated with each group.

The people identified in the inventory represent possible social engineering targets. Social media contacts, professional colleagues, and personal acquaintances all hold varying degrees of access and could be leveraged in phishing attempts or impersonation attacks. Their presence in the system indirectly expands the attack surface by creating external links to my network.

In terms of hardware, the wide range of connected devices increases the potential points of entry. Devices like smartphones, laptops, and home appliances are all connected to the network, and a vulnerability in any one of them could compromise the overall system. For instance, an outdated software version on a smart TV or a laptop could be exploited to gain access to other parts of the network.

The software category revealed that applications such as banking and social media apps have particularly high risks. These applications handle sensitive information and, if compromised, could result in financial loss or unauthorized access to personal data. The inclusion of antivirus software and system protection tools shows that some level of defense is in place, but they also need constant updates and monitoring to remain effective.

The data inventory revealed a significant amount of sensitive information stored across multiple platforms. Birth certificates, social security numbers, and financial records are all highly valuable targets for cybercriminals. The presence of this data across devices and cloud storage increases the risk, particularly if any of the storage methods are not sufficiently protected by encryption or access controls.

Network components like the router and wireless devices present a critical point of exposure. If these network devices are not properly secured, they can act as gateways for attackers to access not only the network but also the devices connected to it. The overall connectivity of my environment, where multiple devices are linked through the same network, increases the potential for an attack on one device to affect the others.

**What Did You Learn?**

Upon completing this inventory, I discovered that my attack surface is broader than I initially anticipated. While I had previously considered my digital footprint to be relatively small, the number of interconnected devices, coupled with the variety of software and sensitive data, presents a larger risk landscape than expected.

One key realization is that the extent of the attack surface is significantly influenced by the connectivity between devices. Since multiple devices are connected through the same network, any vulnerability in one could potentially expose the others. This level of connectivity, while convenient for personal and professional purposes, also introduces more points of exposure to cyber threats.

The inventory also made me aware that I am handling more sensitive data than I originally thought. The presence of both personal identification information and work-related data increases the potential impact of a breach. In terms of risk, this suggests a higher level of exposure than I had previously considered, particularly when it comes to the security of the data I manage.

In summary, while I had expected a moderate level of risk, this exercise has highlighted that my attack surface is larger and more complex than initially assumed. The number of interconnected devices, the variety of software applications, and the presence of sensitive data suggest that my current environment requires more robust security measures than I had previously implemented.