Personal Risk Assessment

Introduction of Subject

The subject of the risk assessment is me, Samantha. Samantha is a 25-year-old female. Samantha is not married and does not have any children. She has 7 siblings, mom, dad, stepmom, and stepdad. She is a student at WTAMU and is not currently involved in extracurricular activities on campus. Samantha lives with two roommates around the same age and works as a billing representative at Xcel Energy, where she mainly works from home. Her hobbies include reading, binge watching TV series, watching movies, travelling, and hanging out with friends and family. Samantha's eating habits are mainly ordering takeout, with cooking at least once or twice a week. Her water intake and physical activity is considered good.

Conduction of Inventory/Asset Categorization

While the inventory was conducted, four different systems were created. These systems include phone system (sys1), work system (sys2), apple watch system (sys3), and school system (sys4). The phone system included going through the apps on my phone and listing those, along with finding different data stored in my phone like messages, notes, phone calls, etc. Hardware included in the phone system is the phone itself, the phone charger, and my airpods. I, Samantha, am the owner of the phone. There are different procedures that involve the phone including taking photos, setting alarms, and how I control my phone overall like limiting screentime.

The work system category involved sorting through hardware I have here at home that I use for work. Tracking routines that included some of my daily activities by keeping log over the course of three days, going through apps I use during work, and listing some ways in which data is being stored. The work system includes very important assets and security measures used to ensure data privacy.

The apple watch system was similar to conducting the inventory for the phone system. The software includes apps on the apple watch like iHealth, the workout app, messages, and walkie talkie. One procedure was putting on the watch which is important due to a passcode being on the watch. Without this procedure, or someone else trying to open the watch, it will not be able to perform regular tasks. Data like calendar events are of extreme importance as this includes important dates for deadlines, events, etc.

The last system, which was the school system, included similar software to the work system, so two assets were listed in two different systems; Microsoft word and excel. I was able to go through my laptop and list apps that I use for school, data stored on my laptop, and also the people who control the laptop, which is also me, Samantha.

Threats/Vulnerabilities

Threats and vulnerabilities were identified by evaluating the risk of each asset. The most common vulnerability throughout the systems was the possibility of phishing attacks. A different email account is used for almost each system which then poses the threat of possible phishing

attacks. Measures are put into place to spread knowledge of phishing attacks and what those can look like; therefore, the risk decreases.

Asset Prioritization

The assets were grouped into four systems for my inventory: phone, work, apple watch, and school. Prioritization (the order listed) was determined based on how well the other systems work without one of them. For example, the phone system is used in each of the other systems for security measures, information, connectivity, and is heavily depended on for everyday use.

Determination of Systems

Systems were determined based on the use of assets and what system they are most effective in. Some assets were listed in two different systems like the messages app and the data stored in the messages app, the text messages themselves. More assets were included in the phone system, as that is where some of the most valuable assets reside.

Risk Assessment - Assets

1. Categorization {Integrity, High}
   The asset is Samantha. The CIA asset is concluded as $500,000. The ARO range is 0.1 (medium), due to the frequency of vulnerability. The current controls in place which are a consistent sleeping schedule and scheduled alarms are rated at being 70% (0.70) effective due to the already successful experimentations of these controls. I have rated the uncertainty as medium, due to my experience with alarm clocks not always being effective and needing to expand the control and set more alarms. The overall risk for this asset is $21,000.
2. Categorization {Confidentiality, High}
   The asset is a phone, the owner being me, Samantha. The CIA asset is concluded as $10,000. The ARO range is 0.05 (low), due to the probability of this vulnerability. The current controls in place are informative articles about keeping information on a phone safe or how to avoid being scammed. I have rated these controls at .75, being 75% effective. The reason being, I understand more than less what a scam call entails and how to avoid them. I have experience with iPhone for over 10 years and am educated in how to keep information safe. I have rated the uncertainty as 0.8, because of my personal awareness of scam calls and the iPhone device. The overall risk for this asset is $225.
3. Categorization {Confidentiality, High}
   The asset is the Gmail app. The CIA asset is concluded as $5,000. The current controls in place are similar to the controls in place for the phone asset, being informative articles and awareness. I have rated these controls at .75, being 75% effective. This rating stems from personal experience with phishing emails and knowledge of prevention on exposed information. I have rated the uncertainty as 0.8 based on personal experience and continued knowledge of possible phishing attacks. The overall risk for this asset is $112.50.
4. Categorization {Confidentiality, High}

The asset is taking photos. The CIA asset is concluded as $1,000. The current control in place to help mitigate the threat of possible loss of data is automatic and regular backups of photos. I have used the same backup and storage for many years and have not had issues with losing photos I wanted or not having all of my photos backed up; therefore, I have rated the controls in place at .80, being 80% effective. I have rated the uncertainty as 0.75 based on personal experience with backups involving photos. The overall risk for this asset is $17.50.

5. Categorization {}
   The asset is personal emails. The CIA asset is concluded as $1,000. The current controls in place to help mitigate the threat and vulnerability are informative articles in regards to phishing and changed passwords frequently in regards to exposed password threat. Changing passwords, not writing them down, often do help in less chances of getting hacked. I rate these controls in place at 0.85, being 85% effective. I have rated the uncertainty as 0.8 based on personal experience with changing passwords often and what phishing emails could look like. The overall risk for this asset is $13.50.

Risk Assessment – System

1. Categorization {(Confidentiality, High), (Integrity, High), (Availability, High)}
   The phone system is comprised of the following assets: Samantha, phone, phone charger, airpods, iPhone software, Gmail app, wells Fargo app, twitter app, Instagram app, apple music app, uber app, Netflix app, TikTok app, photo app, notes app, calculator app, contacts app, messages app, safari app, phone app, taking photos, setting alarms, managing screen time, storing contacts, sending emails, contacts, photos, notes, messages, phone calls, and personal emails. The system is used for contacting friends and family, storing important information and dates, saving photos, security, etc. The reason that confidentiality is high is because the "phone system" is secured with a password and includes personal emails and text messages. Therefore integrity, also high, would have an impact due to sensitive information. Its availability is due to using this system to make everyday communications.

   The vulnerabilities or threats to this system include phishing attacks, not enough sleep and health prioritization for the owner of the system, scam calls, possible loss of information, and possible exposed information. Controls in place are informative articles or new knowledge regarding phishing attacks, setting a regular sleep schedule, automatic backups for data, and changing passwords often. The resulting risk is $21,000. Additional controls needed are a sleeping app to better manage sleep, reporting process regarding scam calls and phishing emails, and more storage space that is secure.

Overall Risk Posture

This overall risk exposure is high, more being phishing attacks and scam calls. This is less risk than I am willing to accept, and more controls need to be put in place to help mitigate these risks further.