|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Asset Name** | **Description** | **Sys ID** | **CIA Asset Value** | **Priority** | **Threat Categorization** | **Vulnerability Description** | **ARO** | **Controls in Place** | **Uncertainty** | **Risk Value** | **Controls Needed** | **Action Plan ID** |
| 1 | Chidinma Aniekwena | Myself | People | $3.5 Mil | Vital | Integrity, High | Drunk, health complications leading to memory loss, compromised password, phishing emails | low, 0.05 | Avoid dangerous places, no drugs, health insurance,use of strong passwords for personal information security. Active mind, work out. (.8) | 0.2 | $42,000 | Health Insurance, Life insurance plan | Update my life insurance plan |
| 2 | Contact List | My personal and business contacts | Data | $1 Mil | Critical | Confidentiality, High | Unauthorized Access, Lost of phone or damage | Very Low, 0.01 | Restrain unauthorized Access with strong password, Backup to cloud, manual copy (.9) | 0.1 | $1,100 | Improve backup system, Accept the risk | Weekly back up to cloud |
| 3 | Mercedes GLK | My car | Hardware | $5 Mil | Medium | Availability, moderate | Drunk or impaired, Accident, health challenge | Very Low, 0.01 | Do not drink at all, no drugs, Auto insurance(.8) | 0.2 | $12,000 | Auto Insurance, transfer the risk to insurance | Install system measures like not being able to connect a phone, while the vehicle is on motion. |
| 4 | Gmail Account | My email account | System | $1 Mil | High | Confidentiality, High | Unauthorized Access, cyber attack, malware, phishing | Very Low, 0.01 | Use strong, unique passwords and two-factor authentication where possible(0.9) | 0.1 | $1,100 | 2-factor autentication password, back-up important emails, delete phisihing emails | Purchase strong back-up system |
| 5 | Data Backup | My Company customer’s data backup | Procedure | $70,000 | High | Integrity, High | Unauthorized Access, cyber attack, malware introduction, Data Loss | Low, 0.05 | Manual copy of customer data backed up every Friday(0.8) | 0.2 | $840 | Unauthorized access restrained, weekly manual back-up up-to-date | Continous wekly data back-up manually and electronically. Restrain unauthorised access |
| 6 | Bank Mobile app | Mobile banking app | Software | $500,000 | Vital | Confidentiality, High | Unauthorized access, password breach, lost of phone | Very low, 0.01 | 2-factor authentication, security question access login, Access login to 2 devices deactivated(.8) | 0.2 | $1,200 | 2-factor authentication, strong password use | Use of strong passwords, Restrain unathorized access to device |

NAME: Chidinma B. Aniekwena

BUFF ID: 1108372

COURSE: Current Issues in Cybersecurity

WEEK 6: Assignment

ASSIGNMENT TOPIC: Personal Risk Assessment

ASSET NAME: Chidinma Aniekwena

SYSTEM: People

On risk assessment for my people system ID, I choose to assess myself. As an individual, my personal safety and well-being are vital to me. To ensure this, I take personal safety measures such as avoiding dangerous places and situations. I assigned a priority value of high to myself, as the asset cannot be easily replaced. My CIA was capped at $3.5million which is broken down into risk of losing my current job as a graduate assistant ($14,400 a year \* 2years). Loss of future income as a Business Analyst, valued at $120k for 25years, loss that can occur due to disclosure of personal information of my clients at my travel Agency Business in Nigeria, which can lead to lawsuits and penalties amounting to ($100,000). My threat categorization was considered high because of some confidential information on my job and business which if disclosed without authorization through theft, physical assault, cyberbullying, or social engineering attacks, it can cause company disruption and lawsuits from clients. The vulnerabilities associated with my confidentiality threat includes drunkness, health complications leading to memory loss, compromised password, phishing emails. My ARO was rated 0.05, though the impact of this threat can be devastating as I get phishing emails. I have been trained on not to open or click on any link I did not subscribe to. My uncertainty of control I put in place is at 0.2 because to mitigate this risk, I avoid dangerous places, don’t do drugs, have a health insurance, I use strong passwords for personal information security, had trainings on phishing emails identification. I plan to regularly review my personal information security measures and update them as needed. I have chosen to transfer the total risk value of $42,000 by updating my life insurance plan.

ASSET NAME: Contact List

SYSTEM ID: Data

My contact list consists of personal and business contact information of my clients, friends and family. My contact list data has been built up for over 2 decades. I categorized the disclosure value at $1million, because it represents the value of confidential information that might be lost if it is used wrongly to impersonate my identity to individuals on my contacts. Maybe in demanding for money or other valuable information. The priority is critical. This vulnerability can be due to unauthorized access to my phone, loss or damage of phone, data backup breach. Threat categorization was rated high and confidential. The ARO is rated very low at 0.01 indicating that the likelihood of this threat occurring is minimal, because of control measures in place, as a restrain unauthorized access to my phone by use of strong password, use encryption to protect the data, implementing multi-factor authentication to prevent unauthorized access backup my data to cloud and also have a manual copy of my contacts to be able to reach out if such risk arises. My uncertainty is low at 0.1 and my total risk value is $1,100. I have chosen to accept this risk as I improve my backup system and ensure an action plan for weekly backup to cloud.

ASSET NAME: My Car (Mercedes GLK)

SYSTEM ID: Hardware

My car as a Hardware asset can be assigned a damage and consequences value of $5million, this is represented by the value to replace the car if in accident as $50,000. The compensation charges to victims involved in the accident at about $3,500,000 say just an individual of about 45years is involved (calculating the number of years left to work and treatment to receive if he ends up not being able to walk), replacement and repair of properties damaged due to the incident at $1.4m. The rest goes to miscellaneous. The priority value is medium, indicating that while it is valuable, it can be replaced. The potential threats I identified includes, getting drunk, impaired vision, health challenges and experiencing an accident. The ARO was rated very low because I do not drink, and have my car fully insured. The threat categorization was rated moderate and availability. The control measures I have in place includes not drinking at all, no drugs and Auto insurance brings my uncertainty to .2. The total risk value is $12,000 which I have decided to transfer the risk by upgrading my auto insurance and I would also install system measures on my car that will reduce the likelihood of accident.

ASSET NAME: My Gmail Account

SYSTEM ID: System

The google email system is my personal email, I do not use it for official work in school or my business. However, it is used for every other need, including my banking transactions and enquiries I make on sites. I use it for social media posts, job haunting etc. The priority level is high because I use it for personal, confidential and banking/financial transactions and the vulnerability threats can be unauthorized access, cyberattacks, malware, and phishing.

Threat categorization is confidentiality, high as unauthorized access to the email will expose a lot of information about me. The CIA asset value was assigned a disclosure value of $1million which comprises of damages of access to my banking applications or credit cards to the tune of $1million. My ARO was rated very low at .01 because of controls I put in place like the use of strong, unique passwords, two factor authentication and back-up of important emails. I also delete unsolicited emails without opening them to avoid phishing emails which brings my certainty level to .1 because of constant receipt of phishing emails which I might not have a 100% detection. The total risk value is $1,100 which I choose to accept and will mitigate against such loss by purchasing strong back-up system.

ASSET NAME: Data Backup (My Company Files)

SYSTEM ID: Procedure

Gianna Travels and Tours Ltd is a travel company that relies heavily on its data systems to provide quality service to its customers. As such the confidentiality, integrity, and availability of its data assets are vital. The asset has a high value of $70,000 based on its revenue currently at $50,000 annually, a 20% loss of future revenues, 10% loss due to lawsuits and 10% loss on fines and is critical to the integrity of the company. The priority is high and threat categorization is also high. The vulnerabilities include unauthorized access, cyberattacks and malware introduction. To promote protect these assets the company has implemented cybersecurity measures such as firewalls, anti-virus software and intrusion detection systems. There is also a weekly manual data backup and recovery procedures in place, as well as access controls to limit unauthorized access. The level of uncertainty is .2 as cyberattacks and system failures can happen at any time, and there is a risk of data loss and corruption. The ARO is low at 0.05 due to the controls in place, but because of the high value of the asset, I assigned a moderate risk value of $840. Currently, the data is backed up manually and electronically every Friday and I have assigned a control value of .8 to this procedure. The company has decided to accept the risk and also mitigate this risk by continuous weekly data backups, restrain unauthorized access to data, regularly assess its cybersecurity measures and implement disaster recovery and business continuity planning.

ASSET NAME: Bank Mobile App (United Bank for Africa Plc)

SYSTEM ID: Software

This is the mobile application I use for my banking transactions. It warehouses access to my finance. This asset priority is vital and threat categorization is high. I have assigned a disclosure value of $500,000 which includes existing funds I will lose and even funds that might be borrowed as overdraft from the financial institution by impersonating me using the application. The vulnerability description includes, unauthorized access, loss of phone and password breech. My ARO is very low at .01 due to the control measures in place like, 2-factor authentication, security question access login, Access login to 2 devices deactivated, access to the app is deactivated on any lost or stolen device, which brings my uncertainty level to .2. The total risk value is $1,200 which I choose to accept as I will maintain a strong, unique password, 2-factor authentication and limit access to bank application to 1 device only.

In conclusion, after conducting my personal risk assessment, I have identified potential threats to my assets, evaluated the likelihood and impact of these threats, and developed a plan to mitigate the risk associated with each asset. By implementing the controls and action plans, I can reduce the likelihood and impact of threats and ensure that my personal and business assets remain secure.