# **| Assignment 2 Portfolio**

# Task 2 Plan

# COIT11241 Cyber Security Technologies

# 

# Student ID: 12195171

# Student Name: Dilsha Keerthi Kumara Weliwita Angoda LiyanageIntroduction

For this review, I have created this document that contains the following sections: My friend has reviewed commercial data breaches, identity theft, phishing, malware, ransomware, weak passwords, and device Risk management such as updates, enabling MFA, and granular device protection required for scenarios.

Also discussed the Risk Tolerance Framework for Friends Cybersecurity Risks. And I've summarized the level of cybersecurity risk my friend is willing to face.

Finally, I briefly described the risks and also described the data and non-data inventories required for this assessment.

## Data Inventory (Top 5):

|  |  |
| --- | --- |
|  | **Classification / Value** |
| Bank Account | Confidential |
| Photos | High Value |
| CCTV Records | Confidential |
| Gmail | Moderate |
| Messages | Confidential |

## Non-data Inventory (Top 10):

|  |  |
| --- | --- |
| **Asset Type** | **Description / Location** |
| Hardware | Mobile |
|  | PC |
| Software | Android |
|  | CommBank App |
|  | Gmail |
|  | Fancy Messaging App |
| Network | Mobile ISP |
|  | Wi-fi Router |
| Process | Backup and Sync |
| People | Himself |

## Risks (Top 10):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Threats** | | | | | | | | | | | | |
| **Type** | Asset | IP compromises | Espionage or Trespass | Forces of nature | Human error or failure | Info extortion | Quality-of-service deviations from | Sabotage or vandalism | Software attacks | Technical hardware failures or errors | Technical software failures or errors | Tech. obsolescence | Theft |
| **Data** | Bank Account |  |  |  |  |  |  |  | 2 |  |  |  |  |
| **Hardware** | Mobile |  |  |  |  |  |  |  |  |  |  |  | 5 |
|  | Backup Drive |  |  |  |  | 6 |  |  |  |  |  |  |  |
| **Networking** | Mobile ISP |  |  | 3 |  |  |  |  |  |  |  |  |  |
|  | Wi-Fi Router |  |  | 4 |  |  |  |  |  |  |  |  |  |
| **Software** | Android |  |  |  |  |  |  |  | 7 |  |  |  |  |
|  | CommBank App |  |  |  |  |  |  |  | 1 |  |  |  |  |
|  | Gmail |  |  |  | 8 |  |  |  |  |  |  |  |  |
| **People** | Friend |  |  |  | 9 |  |  |  |  |  |  |  |  |
| **Processes** | Backup |  |  |  |  |  |  | 10 |  |  |  |  |  |

## Risk rationales:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **Asset** | **Threat to Asset** | **Asset vulnerable to** | **Likelihood** | **Impact** | **Risk** |
| 1 | CommBank App | Software attacks | Criminal access and malware attacks by unauthorized users. | Mod | High | High |
| 2 | Bank Account | Software attacks | Malware, e.g. on PC due to poor game download processes | Mod | High | High |
| 3 | Mobile ISP | Forces of nature | Access to private data with unauthorized access to create, modify or delete. | Mod | Mod | Mod |
| 4 | Wi-Fi Router | Forces of nature | Weak passwords without MFA make contact details easily personal and unauthorized | Mod | Mod | Mod |
| 5 | Mobile | Theft | Phone can be stolen, affecting easy access to contacts and data is automatically backed up and also available via Gmail | Mod | Mod | Mod |
| 6 | Backup Drive | Info extortion | Temporarily suspend easy access to data | High | Low | Mod |
| 7 | Android | Software attacks | Android is jailbroken & has an elevated malware risk allowing criminals access | Mod | High | High |
| 8 | Gmail | Human Error or Failure | Professional Data and Information | User susceptible to phishing attack particularly via Gmail enabling criminals’ access to private data of Contacts | Mod | High | High |
| 9 | Friend | Human Error or Failure | Deleting Important contacts Forgetting passwords for Gmail or any other application | Mod | High | High |
| 10 | Backup | Sabotage or vandalism | Data needs to be stored for future use and applications and files | Mod | Mod | Mod |

## Controls:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Control | NIST step | Explanation/Rationale | Responsible |
| 1 | Apply Two-factor authentication | Protect | Apply Two-factor authentication to ensure user vulnerabilities to prove entry to application | Friend |
| 2 | Open bank account that supports MFA to reduce | Protect | Current bank account is vulnerable to password attacks due to a lack of MFA. MFA protects the bank account by reducing unauthorised access | Friend |
| 3 | Develop a PowerShell script to check the unauthorized access by unsafe IP entrees | Protect | Script will detect the unsafe IP entrees to the mobile ISP | Me |
| 4 | Adding strong physical firewall that supports to filter networks | Detect | Ensure the passing network through the router that filtering safe IP locations | Me |
| 5 | Apply a phone locator | Detect | Locating the device with google location if its stolen by someone else | Friend |
| 6 | Develop a PowerShell script to check the integrity of backup files. | Detect | Although backups are automatic (File History), there is no integrity checking. Script will detect integrity violations. | Me |
| 7 | Updating the software to up-to-date and keep the device with secured apps from google or phone store | Protect | Helps to void the bugs of running applications and OS and keeping the safe way of all data and running applications | Friends |
| 8 | Apply google security protector | Protect | Can filter unwanted emails as spam and give more priority for safe emails | Friend |
| 9 | Keep the google drive up-to-date to void the data loss | Protect | Helps to keep the important data in secure way that voiding data loss from phone memory | Friend |
| 10 | Link the backup device with google drive to store important backup data | Protect | Duplicate files in both device and drive for a data safe and make sure it updated up-to-date | Friend |