

**Central Queensland University**

**COIT11241 – Cyber Security**

**Technologies**

**Term 2, 2022**

**Assessment 2**

Lecturer: Jamie Shield

Tutor: Shakir Karim

Dimas Abiyoga Mauldy – 12148875

**Task 2 – Plan**

In this assessment 2, I will be covering different type of cybersecurity risks. In this assessment, I will then be having a meeting discussion with my friend. My friend and I will discuss about common cybersecurity risks, such as commercial data spills, identity theft, malware, ransomware, and weak passwords and risk controls such as updating their devices, activating MFA. This assessment will also then include a report in which I will talk about different type of risks in cybersecurity.

Additionally, in this report I will also be going through different risks in cybersecurity perspective. This report will be sectioned into 8 sections, there are; (1) Discussing and analyzing common cybersecurity risk with my friend, (2) frame risk tolerance, (3) data inventory, (4) non-data inventory, (5) data flows, (6) risks, (7) risk rationales, and lastly, (8) controls. In all separated sections I mentioned above, tables and diagrams will be provided appropriately for better visualization.

**Cybersecurity risks Analysis**

In this section, I will be analyzing my friend’s cybersecurity risks and to help her to prioritize her digital assets, identify her cybersecurity risks, visualize their data flows, and plan control to reduce her cybersecurity risks.

My friend just like me, we access internet a lot, such as internet banking (local banks or internet banking such as PayPal), playing video games, online shopping, storing and sharing personal digital assets to the cloud (google drive, dropbox, etc.), personal classified emails or messages (social media and email), as well as career or job-related use of internet (school/university, work email, etc.). These usage of internet will sure come with its own cybersecurity risks, and for the accounts to be potentially get compromised. This section of the report we will breakdown any potential cybersecurity risk and to ensure my friend that her personal details will be safe on the internet.

Common Cybersecurity Risks:

* Commercial Data Spills: Commercial Data Spills is a security incident which result in the transfer of classified information onto an information system not authorized to process or store that information
* Identity Theft: Identity Theft is when someone steals your personal information (impersonate you/the owner) to commit fraud
* Phishing: Phishing is a type of cybersecurity attack in which a malicious actors send messages pretending to be a trusted actor or entity (fake websites, fake emails)
* Malware: Malware is a type of virus which is in a form of file or code typically delivered over a network, that infects your device(s) and attempt to steal and explore any personal or classified information virtually
* Weak Passwords: Weak passwords can be easily done by account holder/owner. Account owner tends to use the same password for several logins or apps as it would be easy for them to remember to all the accounts the owner created. This is a bad pre-cautious of cybersecurity risks, as this allows potential hacker to be able to compromise, and take control of all the owner’s accounts once the hacker cracks or solves the password of the owner
* Risks Control: To control the risk that my friend might encounter from the above potential cybersecurity risks, it is recommended to use:

- VPN, to protect your network while she browses on the internet

- Antivirus or Antimalware software, to protect personal or office machine system (computer or laptop) from any virus that she might be carrying over as she downloads software, files, data from the internet

- Two-Factor Authentication (2FA), to protect account from getting compromised, this can be used in email accounts, banking accounts, and gaming accounts. This will let the owner to set a code generator device (usually on a phone) which then generates random code when the owner tries to log into the account she desires

**Frame Risk Tolerance**

In this section I will be providing an overview of my friend’s cybersecurity risks.

The amount of subscription my friend is willing to pay per week as follows below:

* VPN: $3/week
* Antivirus/Antimalware software: $5/week

**Data Inventory (Top 5)**

Data inventory will be covered in this section of the report. Below is a table which illustrates my friend’s top 5 data assets. Classification/value explanation is also provided below appropriately.

Classification/Value:

* Confidential: Only owner (my friend) is the only one who must know or hold this asset or information
* High Value: Owner needs to authorize the assets in this category for someone to know or hold this asset or information

|  |  |  |
| --- | --- | --- |
| **No.** | **Data Assets** | **Classification/Value** |
| 1. | Bank Accounts | Confidential |
| 2. | Email Accounts | Confidential |
| 3. | Digital Files and Documents | Confidential |
| 4. | Passwords | Confidential |
| 5. | Photos | High Value |

Table 1: My Friend’s Top 5 Data Assets Table

Graphical user interface, application

Description automatically generated

Diagram 1: My Friend’s Top 5 Data Assets Diagram

**Non-Data Inventory (Top 10)**

Non-data inventory will be covered in this section. Below are table and diagram which illustrates my friend’s top 10 non-data assets.

|  |  |  |
| --- | --- | --- |
| **No.** | **Asset Type** | **Description/Location** |
| 1. | Hardware | PC |
| 2. | Hardware | Mobile Phone |
| 3. | Hardware | CCTV |
| 4. | People | Me |
| 5. | People | Her friend |
| 6. | Software | Messengers |
| 7. | Processes | Internet Banking |
| 8. | Processes | Video Games |
| 9. | Networking | TP-Link Router |
| 10. | Networking | NBNISP |

Table 2: My Friend’s Top 10 Non-Data Assets Table

**Diagram

Description automatically generated**

Diagram 2: My Friend’s Non-Data Assets Diagram

**Data Flows**

A diagram and a table of data flows will be shown in this section of the report as shown below.

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Type** | **Asset** | **Involvement** |
| 1. | Data | Bank Account | N/A |
| 2. | Networking | TP-Link Router | Transmitting |
| 3. | Networking | NBNISP | Transmitting |
| 4. | Hardware | PC | Storing |
| 5. | Hardware | Mobile Phone | Storing |
| 6. | Software | Browser | Transmitting |
| 7. | People | My Friend | Processing |
| 8. | Processes | Internet Banking | Processing |

Table 3: Data Flow Table

Diagram

Description automatically generated

Diagram 3: Data Flow Diagram

**Risks**

I will be going through the list of risks in which I will categorize them of its likelihood to encounter threats. I will go through this table with my friend where I will call her, and she and I will discuss about her priorities over her top 10 risks, and helping her to understand the threats, vulnerabilities and the likelihood and impact of the risks.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **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** | **Technical Obsolescence** | **Theft** |
| Data | Bank Account |  | 3 |  |  |  |  |  | 2 |  |  |  |  |
|  | Email Account |  | 1 |  |  |  |  |  |  |  |  |  |  |
| Hardware | PC | 6 |  |  |  |  |  |  | 7 |  |  |  |  |
|  | Mobile Phone | 4 |  |  |  |  |  |  |  |  |  |  |  |
|  | CCTV |  |  | 10 |  |  |  |  |  |  |  |  |  |
| Networking | TP-Link Router |  |  | 9 |  |  |  |  |  |  |  |  |  |
|  | NBNISP |  |  |  |  |  |  |  |  |  |  |  |  |
| Processes | Internet Banking |  |  |  |  |  |  |  |  |  | 5 |  |  |
| Software | Messengers |  | 8 |  |  |  |  |  |  |  |  |  |  |
| People | Me |  |  |  |  |  |  |  |  |  |  |  |  |

Table 4: My Friend’s Risks Table

**Risk Rationales**

In this section, I will be explaining even further about the top 10 risks I have discussed with my friend above.

Likelihood levels: High, Medium, Low. High for most likely and Low for least likely

Impact levels: High, Medium, Low. High for the most impactful and Low for the least impactful

Risk levels: High, Medium, Low. High for the riskiest and Low for the least risky

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Asset | Threat to Asset | Asset Vulnerable To | Likelihood | Impact | Risk |
| 1. | Email Account | Trespass | Trespass can occur due to having the same password to all other accounts, or to have a non-unique password | Medium | High | High |
| 2. | Bank Account | Software Attacks | Virus or unauthorized files gained due to download files or apps from untrust worthy websites | Medium | High | High |
| 3. | Bank Account | Trespass | An unauthorized access can be gained once the password for the account is cracked. e.g. passwords are too similar to other accounts and passwords are not a unique password or easy to be guessed | Medium | High | High |
| 4. | Mobile Phone | IP Compromises | Mobile Phones is vulnerable, if the owner is not being careful on what and where to download files or access website from, this will lead into trespass of an unauthorized personnel | Low | High | High |
| 5. | Internet Banking | Technical Software Failures or Errors | Internet Banking can be vulnerable if there is any software update, or maintenance which lets the owner not being able to use it as normal | Low | High | High |
| 6. | PC | IP Compromises | PC is vulnerable to any unauthorized access that the owner might have gained from downloading or accessing from untrust-worthy websites | Medium | Medium | Medium |
| 7. | PC | Software Attacks | PC is vulnerable to any unauthorized virus or files in the computer that the owner might gain from downloading or accessing from untrust-worthy websites | Medium | Medium | Medium |
| 8. | Messenger | Trespass | Messenger apps can be vulnerable due to downloading files or accessing from an untrustworthy websites | Low | High | Medium |
| 9. | TP-Link Router | Forces of Nature | Router is vulnerable from any nature that makes TP-Link Router itself to not functioning properly (disconnected, or broken) | Low | High | Low |
| 10. | CCTV | Forces of Nature | CCTV is vulnerable from any nature that makes CCTV inactive (broken, disconnected from the network), or for unauthorized access from the internet | Low | High | Medium |

Table 5: My Friend’s Risk Rationales Table

**Controls**

In this last section of the report, I will be going through in explaining what precautious or steps to prevent my friend’s cybersecurity risks. Below is a table in which I have elaborated for my friend’s control risks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Control** | **NIST Step** | **Explanation/Rationale** | **Responsible** |
| 1. | Enable the Two-Factor Authentication (2FA) for email account(s) | Protect | Current email accounts are vulnerable to password attacks due to lack of 2FA authentication. 2FA will ensure that only the owner will be logging on to the account by sending a code to owner’s phone | Friend |
| 2. | Antivirus on your devices to protects the banking app from software attack | Protect | Devices such as phones and PC are vulnerable to any potential software attack via virus that infects the device. Antivirus/Antimalware software will help the devices to prevent that from happening | Friend |
| 3. | Enable the Two-Factor Authentication (2FA) for bank account(s) | Protect | Current banking accounts are vulnerable to password attacks due to lack of 2FA authentication. 2FA will ensure that only the owner will be logging on to the account by sending a code to owner’s phone | Friend |
| 4. | Having to subscribe to VPN to ensure that phone’s IP address is protected | Protect | Having VPN for your phone while using or accessing via the internet is a must as it will allow the user to have a protected IP address on the internet and hide the device’s IP address | Friend with the help of me |
| 5. | Being able to identify if internet banking is out of service (e.g. maintenance) | Identify | Having the ability to identify whether the internet banking is out of service will lead you into being cautious and to get prepared for when the internet banking is out of service | Friend |
| 6. | Having to subscribe to VPN to ensure that PC’s IP address is protected | Protect | Having VPN for your PC while using or accessing via the internet is a must as it will allow the user to have a protected IP address on the internet and hide the device’s IP address | Friend with the help of me |
| 7. | Having to subscribe to Antivirus/Antimalware to ensure that PC’s is protected from virus | Protect | Having an Antivirus/Antimalware software, will help the PC protected from any possible or potential virus and malware to the PC | Friend with the help of me |
| 8. | Having a secondary messenger app in case of any problem such as maintenance occurs with the primary messenger app | Respond | Understanding that some messengers application might have downtime for maintenance, in that case, always have a secondary messenger app that lets you stay communicated | Friend |
| 9. | Turn back the router on or make sure that nothing is going to turn it off or disconnect it from the internet | Detect | Current router setup might need a little adjustment such as higher place for the router so whoever uses the connection should get the best out of it, and to prevent extra dust | Friend with the help of me |
| 10. | Turn back the CCTV on or make sure that nothing is going to turn it off or disconnect it from the internet | Detect | Current router setup might need a little adjustment so that no rain, or dust debris from outside can disconnect or turn off the CCTV which can cause a functionality issue to the CCTV | Friend with the help of me |

Table 6: My Friend’s Control Risks Table