|  |  |
| --- | --- |
| A picture of a winding road and trees  Task 2: Plan  COIT11241 CyberSecurity Technologies | Assignment    Eric Steyn  12053766 |

Table of Contents

[Frame Risk Tolerance 1](#_Toc111302104)

[Data Inventory 1](#_Toc111302105)

[Non-Data Inventary 2](#_Toc111302106)

[Data Flows 3](#_Toc111302107)

[Risks 4](#_Toc111302108)

[Risk Rationales 5](#_Toc111302109)

[Controls 6](#_Toc111302110)

# Frame Risk Tolerance

My friend has basically no security.

* Default password on his router
* Only using Windows defender
* No firewall in place
* WPA-2 for authentication method on the router.
* Using the same password for everything.
* No password manager
* Smart Home User using google home and will do online purchases through google.
* Running old SW.

Risk Apatite

* My friend seems to have quite a high risk apatite but mentioning financial loss made him a bit more conscious and has seem to have lowered in apatite.
* My friend has accepted that he might have to invest in a better router and at least an antivirus SW.
* My friend has put forward a most $500.

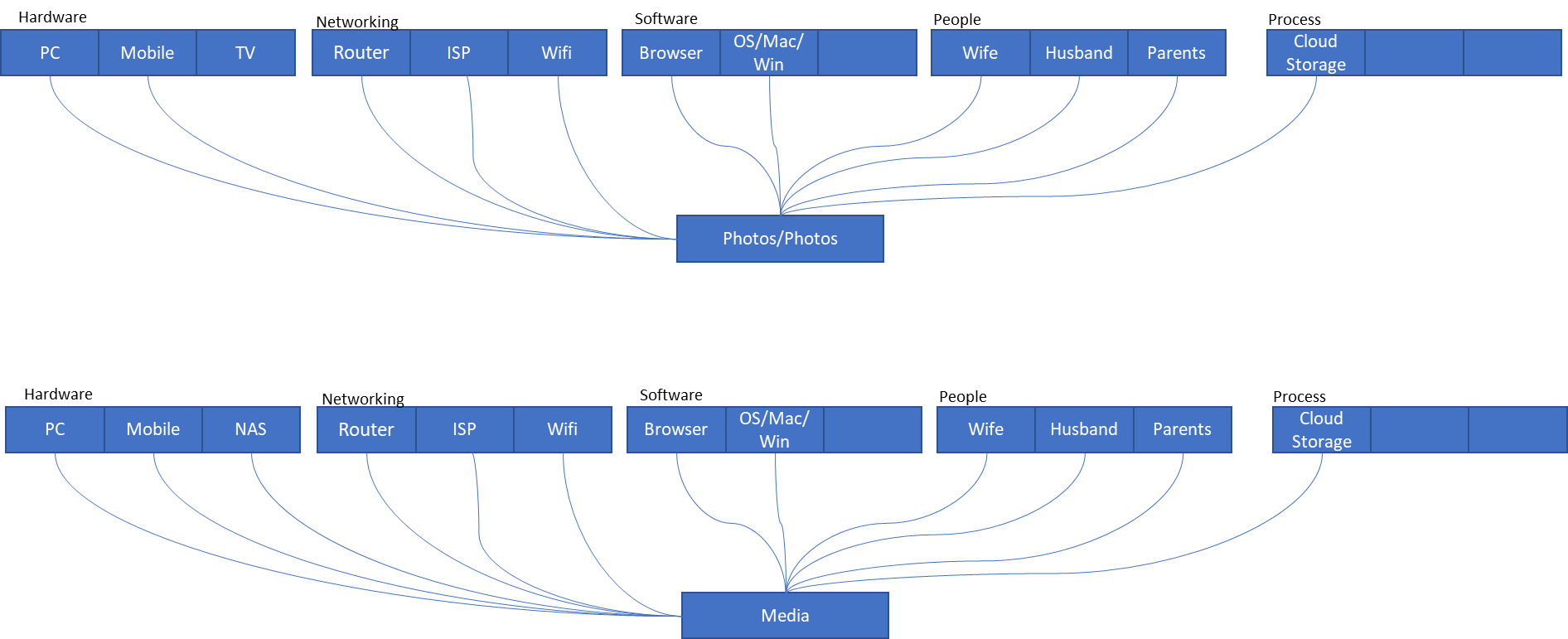
# Data Inventory

|  |  |
| --- | --- |
| Data Asset | Classification Valua |
| Bank Accounts /Webapages | Confidential |
| Photos | High Value |
| Documents | High Value |
| Media | High Value |
| Sensor Data | Confidential |
| Passwords | Confidential |
| Transactions | Confidential |
| User Input (Social Media Posts) | Confidential |

# Non Data Inventary

|  |  |  |
| --- | --- | --- |
| Hardware | Laptop (Wife) Apple Mac Book Pro | Apple MacBook Pro |
|  | Laptop Lenovo | E595 |
|  | Phone (Wife) | Iphone 8 |
|  | Phone | Samsung S22 |
|  | Phone Parent 1 | Huawei P20 Pro |
|  | Phone Parent 2 | Huawei P30 Pro |
|  | Desktop |  |
|  | Smart Fridge | SRF 7500 |
|  | Smart TV Sony | Bravia BZ 55 |
|  | Smart Heater | Kogan |
|  | Cameras Hikvison | HikVision |
|  | Invertor | Bosch BPT-S |
|  | Printer | Brother L2730DW |
|  | Lights | Phillips Hue |
|  | Security Cameras Hikvision | DS-2CD2145S |
| Networking | POE Switch (Unmanaged) Netgear | Netgear GS-116PP |
|  | Gneneric Router( Telstra)(Huawei) | Huawei |
|  | ISP | Vodafone |
|  | ISP | Telstra |
|  | Cat 5e Cabling |  |
| People | Wife |  |
|  | Mother in Law |  |
|  | Father in Law |  |
|  | Himself |  |
|  | Kids |  |
| Software | Windows /OS |  |
|  | Microsoft Suite | Powerpoint, Word, ETC |
|  | Photoshop | Adobe |
|  | Browsers/Google/Opera/Firefox |  |
| Processes | Internet Banking |  |
|  | Cloud storage/Google |  |
|  | Games Steam |  |
|  | Streaming Service/Netflix |  |
|  | Smarthome/Camera monitoring |  |

# Data Flows



* Example 1 🡪 Photos

The photos are stored in Google photos cloud storage.

The photos could be accessed via the Browser on multiple devices or through the photos app on IOS/Android.

The data can be reached by everyone with a google account and access.

The photos can be stored or downloaded to the devices that you access it through.

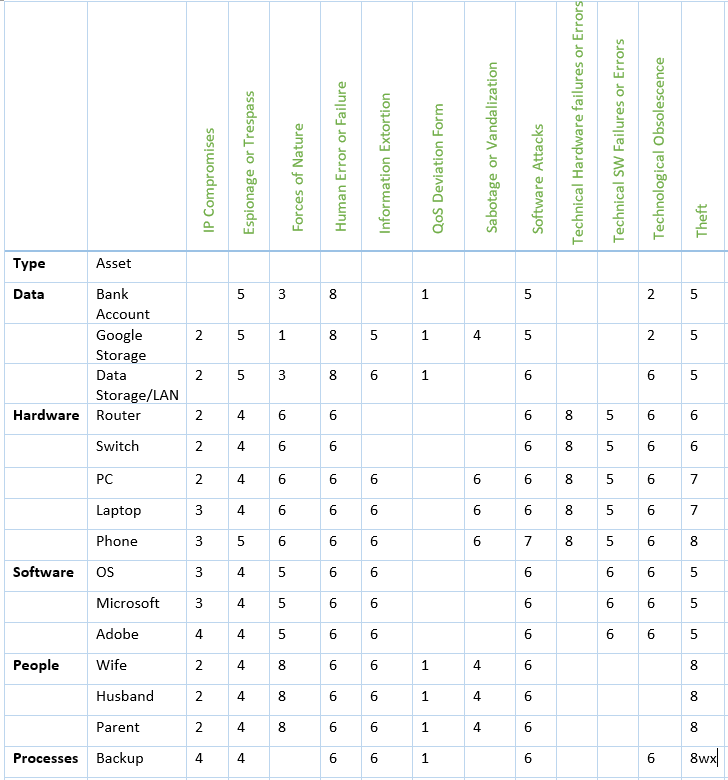
* Example 2 🡪

Media that is created for instance a home video

It could be stored locally but also in the cloud.

The video could be stored in Drop box or something similar

# Risks



# Risk Rationales

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Asset | Threat to Asset | Asset vulnerable to | Likelihood | Impact | Risk |
| 1 | Bank Account | Human Error | Forgetting to sign out of an account such as google account | Moderate to high | High | High |
| 2 | Bank Account | Software  Attack | Malware picked up from downloading untrusted SW. | Moderate to High | High | High |
| 3 | Bank Account | Theft | Bank Information stored on Drives, Browsers or through Cameras | Moderate to high | High | High |
| 4 | Photos/Google | Human Error | Forgetting to sign out or downloading photos to unsecure hardware. | Moderate to High | High | High |
| 5 | Photos/Google | Software attack | Malware from WIFI connection, Email downloads and so on. | Moderate to High | High | High |
| 6 | Photos/Google | Theft | Personal information stored on a stolen device | Moderate to High | High | High |
| 7 | Mobile Phone | Theft | Data stored on the device and loss of data | Moderate | High | High |
| 8 | Laptop | Theft | Loss of Data and data being vulnerable | Moderate | High | High |
| 9 | Wife/Parent etc | Human Error | Human error Could have severe risks to humans and humans make mistakes | High | High | High |
| 10 | Wife/Parents etc | Forces of Nature | Forces of nature can impact humans severely | High | High | High |
| 11 | Hardware/PC/Router | Hardware Failure | Equipment failing could have significant damage or loss of data | High | High | Moderate |

# Controls

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Control | NIST Step | Explanation/rationale | Responsibility |
| 6 | Don’t store bank accounts in for instance browser. Make sure only your personal devices are signed into shared platforms such as Google. Make sure your notifications are turned on. | Detect | Google and apple are cloud services and sometimes you must use a PC that’s not yours to access your account like a work PC. Always make sure your signed out of those accounts. | Friend. |
| 5 | Sofware Updates | protect | Software Updates have the latest SW protection and also addresses known Vulnerabilities. | Me |
| 5 | Purchase reputable Antivirus | Detect/Protect | Implement the Antivirus software to detect and to protect again viruses, trojans, and to protect by quarantining the malware. | Friend |
| 7 | MFA for banking (Multifactor Authentications) | Protect | Protection further for bank accounts, protects the passwords a bit better | Friend |
| 7 | MFA for Google/Photos | Protect | Further protection so for cloud accounts | Friend |
| 6 | Password hardening | Protect | Change the passwords to congeneric passwords and create different passwords for different services | Friend |
| 6 | Password Vault account | Protect | Making sure that passwords are stored safely and not forgotten. | Friend |
| 8 | Insurance for theft and Forces of Nature | Protects and recover | Check the insurance to make sure hardware is covered for theft and natural disasters | Friend |
| 6 | Change all default passwords | Protect | Change all the default passwords of switches, routers and all other devices such as smart home devices | Friend |
| 6 | Purchase Router with Better firewall settings | Protect and detect | Purchase a router that will detect as well as alert to any unauthorised access. Also a router that you can set up certain firewall rules on. | Me |
| 7 | Data backed up | Recover | Make sure that data is back up and that configs are all backed up in the event of hardware failure no data is lost and that older configs can be restored quickly | Me |
| 6 | Write PowerShell Scripts to reference SW/Applications running on PC’s | Detect | Making sure that only the known is running on the machines and that no other unwanted SW is stealing your account details. | Me |
| 6 | Procedures of how to react in-case a notification comes through | Respond | Make sure your friend knows how to respond if a notification or MFA notification comes through that was not initiated by him | Me |
| 6 | WPA-3 Password on the router | Protect | Make sure your friends router is set up with the strongest password protections and that is does not broadcast to to far. | Me |