## WEEK 1 ASSIGNMENT

**1. Create and share a list of all the data, software, and hardware assets you need to complete this course. Explain why it is important to have an inventory of hardware, software, and data assets.**

Hardware Assets: Computer, Network Components, Internal Computer Components

Software Assets: Operating system, Commercial Applications, Individual Applications

Data Assets: Documents, Photos, Music/Videos, Email

It’s important to have an inventory of all IT related assets like computers, hardware, software, and data for simple basic tracking of course but more importantly for future developments. This could be a project that requires changes to be made to existing structure or requires more assets to be but in place. Having a list of all those assets that is current allows for easier scope defining and planning for those future projects/changes.

**2. Provide an example of a confidentiality threat to one of more of those assets. Identify the asset that is at risk, the likelihood of the threat occurring, and the impact of that threat on your asset. Describe the types of controls you would put in place to protect the asset.**

Some of the most common confidentiality assets that is monitor and broken the most is data. Documents are often detailed in confidentially agreements that they should not be transmitted outside of the company or even sometimes with your department, group, or team. Yet confidentiality is not just limited to data. For companies that specialize in certain physical technical assets like prerelease computer components or other devices this confidentiality is also very important. This is often a more serious threat since these assets are even more secure and important to the organization than internal memos and data.

To prevent breaks in confidentiality there is of course agreements that are signed by employees, but constant oversight and management is what often takes place to manage data confidentiality. This can often be achieved with private internal networks that monitor data transfer and access, but it could also be something simple like using a file sharing system that only allows whitelisted users to access the data.

**3. Provide an example of an availability threat to one of more of those assets. Identify the asset that is at risk, the likelihood of the threat occurring, and the impact of that threat on your asset. Describe the types of controls you would put in place to protect the asset.**

A common availability threat would be to data where unauthorized parties have accessed that data that is supposed to be confidential. Depending on the existing methods that are in place for data security that risk could vary. For most organizations the risk is minimal if they have security systems in place that are robust but of course there is also the factor of physical assets getting lost and misplaced those results in this availability problem.

Common controls for this like I stated in confidentiality are to have internal networks or sharing systems in place that require accounts to access the data behind them. But to get even more heavy in protection there should be daily password or SSO systems that are required to be used to limit that problem of physical assets having complete access with no other safeguards.

**4. Provide an example of an integrity threat to one of more of those assets. Identify the asset that is at risk, the likelihood of the threat occurring, and the impact of that threat on your asset. Describe the types of controls you would put in place to protect the asset.**

A simple integrity example could be that external users have gained access to data and changed information. This could result from improper security, increased availability like above, or lack of confidentiality with employees. This threat could also be internal if the level of confidentiality per department should be very high, but the availability of that data does not match. For large organizations this issue is very high since they have a lot of data, and it is hard to keep track of all the access levels and points of access that people have.

As stated above internal networks or sharing systems are the ideal ways to prevent threats to integrity of systems but also other assets. Internal networks often allow more control over computers and there communication too other devices on or outside the network.

Backups are also very key to data integrity and great ways to prevent changes being permanent if they are ever improperly made. Often having overlapping controls like backups and high-level encryption at multiple access points is enough to prevent threats to data integrity.