Information Assets

[Name of the Writer]

[Name of the Institution]

Information Assets

**Introduction**

Information assets are considered to be the bodies of knowledge that are managed and organized as single entities. The matter of fact is that the information assets of an organization tend to have financial value like any other corporate asset. Such asset value tends to increase in direct relationship to the individuals who can be making the use of information. As the information undoubtedly has a little lifecycle, therefore, it results in depreciating over time. One thing that must be considered is that there is always a high chance for an asset to lose its value which depends upon the manner in which information is provided (Peltier, 2016). It is also based on the accuracy of the information. There are some organizations in which the non-usable information is considered as a liability. The classification of an information asset can be done to any criteria. The perfect example in such a scenario would be of the data that can be broken down. The implementation of a data classification system can be done for making the information assets easier to find, share and maintain.

**The threat to Information Assets**

At times when data is seen to be falling either under compliance or regulatory restrictions, the choice of cloud deployment tends to hinge. Such obligations often fall on the user or tenant. There are a number of threats to information assets, and all of them needs to be addressed.

**Privacy Violations**

One of the most common threats to information assets is a violation of privacy. Information privacy is considered to be a relationship between the dissemination and collection of technology, data, policial and legal issues that surround them. In other words, it is also known as data protection or data privacy . When it comes to the challenge of data privacy, it is for using data while protecting the personal information and privacy preferences of an individual. It has been observed that privacy violations tend to occur outside cloud computing (Kar et al., 2016). In a number of scenarios, cloud privacy information exposures have occurred in different organizations.

**Compromise of Virtual Files and Hard Drive**

There is no doubt that the theft of information assets may occur in different virtual environments. A VHD is used to store the entire hard drive contents. The matter of fact is that the VMs or disk image includes all structural elements and data. The disk image or VMs can be stored at a place where there is an access to the physical host. Therefore, it becomes quite easier to transport it on a USB flash. The VHD file can be accessed by an attacker, and it would not even require the attacker to enter the data centre.

**Viruses**

There is no doubt that a computer virus is quite dangerous and costly to deal with. It can happen anytime if there is not any proper protocol in place for protection. A virus acts as a program that has the tendency to replicate and execute itself. It can simply interfere with a computer and may harm the information assets. One of the reasons behind viruses being a major threat to information assets is their ability to steal and corrupt data.

**Worms and Spam**

Worms are seem to be quite similar to viruses as they can be harmful to the information assets, but there is a clearer difference between the two of them. Unlike viruses, a worm requires no user interaction for spreading itself. On the other hand, spams are the junk email that clogs up the business servers for annoying the recipients working in an organization. The reason why spam has become a computer security threat is that it tends to contain harmful links that may overload the mail server.

**Strategies to Protect Information Assets**

In the current scenario, there is a high need to focus on protecting information assets. The room for information assets is broader which results in increasing the threats. As the threats for information assets are vast in number, therefore, all of them needs to be addressed in order to make the information secure. There are certain strategies that can be adopted with regards to this.

**Beware of Threats**

In a number of scenarios, it has been observed that the information assets that lie inside an organization can manifest due to certain errors. There is a high need to create awareness in the organization regarding the risk factors that may occur due to spams. Proper training should be initiated to teach the issues that may come due to such threats (Peltier, 2016).

**Updating Desktop Software**

Every hacker is aware that a business rarely updates its software. There is no doubt that the software that is out of date often contain security flaws that can be exploited. In order to tackle such risks, there is a high need to protect the information, and there must be regular patches and updates applied to the software (Sittig et al., 2016).

**Limiting the Outgoing Connections**

In the current scenario, there is a high need to initiate the strategies for managing risks that are associated with the inbound traffic to the IT environment. One of the best approaches here would be to use virus scanning software or simply known as anti-viruses. Apart from this, a computer can easily be infected due to malware which can connect back to the attacker. The possible solution here would be to restrict the services that can be used by a user outside the organization. All of this can be done with the help of firewall connections.

**Cloud Computing Decisions**

Studies and research show that there is an increase in the cyber attacks which has ultimately become a challenge in order to keep up. Cloud computing solutions tend to offer reliable security. However, there are certain risks in association with cloud computing. Therefore, it becomes quite necessary to carefully evaluate these risks. There must be a proper system of data backup.

**Ways to Respond to Threats**

The threats in information assets are undoubtedly crucial, therefore, it becomes quite necessary to respond to each threat.

**Threat 1: Privacy Violation**

If an organization faces a threat of privacy violation in its information assets, the organization must not store the privacy information on the servers that tend to lack adequate control. In order to address this threat, the organization should not select any unverified cloud provider (Kar et al., 2016).

**Threat 2: Compromise of Virtual Files and Hard Drive**

It is quite important for protecting VHD files when it comes to the strategies of information security. There are three elements required for such protection. A limitation of access should be implemented to the host data stores on which the VMs are presented (Saunders et al., 2016). The second element is to implement the access logging to acknowledge when does a breach occur. The third and last element is to physically isolate the storage network as it may provide access only to host and storage devices.

**Threat 3: Viruses**

Viruses undoubtedly affect information assets to a great extent. However, they can be tackled by installing anti-virus software within the system of organization. This software will stop the viruses to spread in the system, and the performance of the system will be enhanced as well.

**Threat 4: Worms and Spams**

Worms and Spam over e-mails can be avoided by deleting the e-mails of the sender which the organization does not recognize. The attachments within the email must be scanned before downloading them. Anti-viruses will be helpful in the case of Worms and Spams.

**References**

Kar, J., & Mishra, M. R. (2016). Mitigate threats and security metrics in cloud computing. *J Inf Process Syst*, *12*(2), 226-233.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications.

Saunders, A., & Brynjolfsson, E. (2016). Valuing Information Technology Related Intangible Assets. *Mis Quarterly*, *40*(1).

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, *7*(02), 624-632.