Jeffrey Semon

INFA 610 9045

Short Paper

The point in the section Sift to a “Cloud First” policy is that current systems that the government is using have become antiquated compared to the performance of cloud systems. As in the example that the 25 point implementation provided with cash for clunkers, the government will be able to provide much more agile services to its users if a cloud is implemented. Not only will this implementation make government systems more agile, but it will make them more economical and faster. More economical systems will be available because cloud computing offers a pay as you go approach. This allows systems to be scaled up or scaled down according to consumer demand. Not only is this useful for economy of the system but it also makes the system faster. By being able to scale a system up and down with demand quickly it also offers the elimination of long procurement and certification processes as well as a wonderful selection of alternatives to be implemented with the new system. Along with wonderful innovation comes security challenges. At this time the cloud is not perfect and needs improvements and security is one of the gaping holes that can be seen in cloud computing.

There is much information that needs to be protected in the cloud. All of the information that is flowing into the cloud is going to need secured. Not all information is going to flow to the cloud, however. Sensitive information should be kept in the organization and not deployed to the cloud in order to mitigate security risks. Still there will be information on the cloud such as consumer information and a lucrative database full of consumer metrics that are sensitive and will need to be protected. The biggest issue here is that the security protocols are not in the hands of the organization that is using the cloud anymore. All of the responsibility for security now lies with the company hosting the cloud. This is the ultimate dilemma with security when it comes to cloud computing. This is one of the reasons why cloud computing is not perfect, amongst many other reasons. As a result of this weakness in security one can imagine how this limits the choices in cloud computing. Users of the cloud

are most certainly going to utilize cloud services that allow the best security. With this in mind one can consider using cloud services of a company located within the United States versus one located outside of the United States. The major issue in this situation brings us to the issue of risk.

The risk in this situation is that if there is a problem, such as a fraud in the organization, how will the company that utilizes the cloud be able to procure and secure the necessary hardware and data when the hardware lies overseas and the laws of the country that governs the equipment is not the same as the United States. The difference in laws is just the beginning. There is also the huge problem of jurisdiction of the United States judicial system. One cannot just issue a subpoena for equipment in India. The U.S. has no jurisdiction there. This can introduce some serious threats and vulnerabilities. Continuing with the example of using a foreign supplier for cloud services we can see some threats emerge to security. If parties are aware of a company's inability to obtain the necessary evidence to prosecute individuals that are tampering with their systems in the cloud they may become emboldened to continue attacks and possibly even widen the scope of their attacks from an isolated part of the system to a much larger attack that can be even more crippling. The impact of such a problem can hurt an organization tremendously. If we think of the cash for clunkers example in the 25 point implementation, we can imagine the frustration and problem that would occur when millions of people are waiting for their rebates and a system is continually crippled as a result of poor security in the cloud and an emboldened threat. Along with the threat of the immediate environment such as where the hardware is located and the legal aspects of this environment we should turn our attention to some of the practices in the workplace that can also be a security threat. As technology continues to grow individuals are using their home PCs to do more and more work at home. There is a double edged problem here when it comes to security. As Hocking discusses in his document security can be compromised in the cloud or at the point of interface of the user. As far as security problems with the cloud are concerned in this instance, malware introduced in the cloud is not something that the user at

a remote point is not going to detect (2011, pp.18). When we think about this for a moment one can understand how the malware can move through the network and contaminate the remote users PC that is doing work at home. If this person then brings this PC to work and docks with a network disconnected from the cloud it is possible that the network can be infected, especially by viruses that are very stealthy to slip past virus scanners. This role can also be reversed and a person who uses their personnel PC for work can introduce a threat to the cloud if security is not appropriate.

An adoption of standards set forth by the National Institute of Standards and Technology will most certainly bring security problems domestically in line. Foreign sources that wish to compete with domestic services will also adopt the standards to remain competitive. However, this will not eliminate the problem with legal jurisdiction when it comes down to getting the appropriate evidence into court, so selection of foreign sources must be done carefully. Addressing the security problems that can arise as a result of an individual using their personnel PCs at home to do work, Hawking discusses that technology called a "trusted client", which allows an unmanaged PC or thin client to be turned into a secure network access point can be used to eliminate the problem (2011, pp.19). Hawking states that the trusted client works as follows, "Typically, the 'trusted client' has a very small footprint so can be loaded onto a USB stick, DVD or directly on to a laptop or thin client. Rebooting the device using the 'trusted client' creates a secure isolated environment where users can safely access the corporate network, data and applications. Only the host machine's memory, processor and keyboard are used, so the network is protected from malware and data accessed is encrypted."

References

Hocking M. (2011). Thin Client Security in the Cloud. *Network Security, 11*(6), 17-19. Retrieved from ABI/Inform.