**Cloud Computing Security**

Frances Coronel

CSC 120-13

April 15, 2016

**Introduction**

By definition, a system is considered secure when it is in a state free of potential danger or threat (“Security”). This idea is applicable to not just one system, but globally to organizations, companies, states, countries, and so on. All entities on earth must address some form of security one way or another and not all security is created equally or ethically.

With security, certain procedures or measures are always taken to ensure the safety of that system. There are many types of security and therefore various ways of handling it ethically. Computers, food, school, home, airports, shopping centers, viruses, money, etc. -- security concentrations lie all around us. It is therefore increasingly important to ethically scrutinize, especially in the technological realm, given that “software is eating the world” (Andreessen).

**Security in the Cloud**

In all major cloud storage services, security has become a primary focus. The news of all these data breaches and public safety image are both large factors in that decision. This ties in with what was mentioned earlier with perceived versus real risks. Unfortunately, many cloud services scramble to patch security holes in order to avoid major cyber attacks (Rancourt). However, on the other hand, companies that are more well know for their security tend to consider the following ten components in their cloud security: corporate security policies, organizational security, data management, access control, personnel security, physical and environmental security, infrastructure security, systems and software development and maintenance, and of course disaster recovery and continuity (Symantec).

For individual users, security is not typically an issue although the media recently has attacked Apple for the celebrity photo leaks that occurred this past August through their cloud based service, iCloud. Apple has claimed already that the breach was very specifically targeted towards those celebrities and therefore did not represent an actual vulnerability in the iCloud services itself. Regardless, the leak did raise more public awareness of the possible dangers in sharing sensitive information through cloud-based storages (Gurman).

So again, going back to the original question, the average user does not face substantial threat but as of right now, large companies and business face a much higher risk because the information they handle are extremely valuable. The standards are then much higher for these organizations that handle a lot of data each second across multiple platforms. Even if these online data storage services claim user data are encrypted, there is no real way for the average user to actually find out. So most people put all their trust into these cloud services, hoping they don’t become the next hacked victim (Symantec).

**Conclusion**

Personally, I don’t believe our private information is ever 100% secure. It may secure on the surface and one can always take small measures to ensure more levels are added to their accounts for maximum security, such as stronger passwords, 2-step verification, using an anonymous browser like Tor, logging out afterwards, and so on and so forth, BUT in the end, the ultimate amount of security your data is protected by depends entirely on the company itself. So the more transparent the company you depend on is in terms of data security, the better for their users. So while, indeed, the Cloud may never be completely secure, each user can take extra precautions to make sure that they are at least not negatively affected because of an error of their own, but rather because of a flaw derived from the service itself.

**Bibliography**

Andreessen, Marc. "Why Software Is Eating the World." *The Wall Street Journal*. Dow Jones & Company, 11 Aug. 2011. Web. 03 Apr. 2016.

Gurman, Mark. "Apple Denies iCloud/Find My iPhone Breach, Says 'very Targeted Attack' Hit Certain Celebrities." *9to5Mac*. 9to5Mac, 2 Sept. 2014. Web. 02 Apr. 2016.

Rancourt, Chris. "Cloud Security: Making Sure Your Information Is Safe." *NextAdvisor Blog*. NextAdvisor, 27 Oct. 2014. Web. 03 Apr. 2016.

“Security.” Oxford Dictionaries. *OED Online.* Oxford University Press, 30 Apr. 2007. Web. 02 Apr. 2016.

Symantec. "Securing the Cloud for the Enterprise." *Symantec White Paper* (2011): *Symantec.com*. Symantec and VMWare, 1 May 2011. Web. 04 Apr. 2016.