# Unit 10 Assignment: IT 104 Assignment

Andrew Vasquez

Purdue University Global

Professor Steven Areges

March 16, 2021

# Unit 10 Assignment

If there is the transference of data, there will be security issues or cybercrime. Mobile devices, organizational networks, and home networks are increasing exponentially, but more so with mobile devices. The increasing number of devices being connected also brings new targets to be attacked by cybercriminals. Many of these new devices being connected will be vulnerable to cyber-attacks to obtain personal data such as emails, passwords, financial data, health information, and other sensitive information. Users also must worry about other things connected to a home network, such as speakers, cameras, and security systems; anything that has an IP address and can be pinged. For example, if you have two computers, three phones, a security system with cameras, and an Alexa Amazon speaker connected to the same network and someone were to access your home network, they could easily access everything. Usually, home networks and small businesses do not put cybersecurity at the top of their list, which ultimately leads to data theft, the biggest security issue amongst end-users themselves not being educated in the matter. These types of attacks can range from the various basic phishing attempts and clicking on a suspicious link and cause them to allow an unwanted guess connection to their network. Other times it does not have any security at all and having the front door wide open.

With the increasing number of devices being connected, there is a need for data storage. One recent way of storing data and having other uses such as networking, software, databases, and servers is cloud computing. This is a good and bad thing; cloud computing has brought a new way to store data easily; however, it has also brought more security issues to the table. These security issues include attacks on these cloud servers and using them for computing power to mine for bitcoin, and this is called crypto jacking. Other security issues include data breaches, denial of services attacks, insider threats, hijacking accounts, insecure applications, and overall

inadequate cybersecurity training. Denial of service attacks is a flood packet of data sent to a server to stop a service from being accessed by users. Data breaches are more damaging than you would think; for example, if you register an account on a certain website that has experienced a data breach, bad actors have now obtained your email, passwords, date of birth, commonly used username, and full name. They can then use that information to see other accounts associated with that information and further exploit it from there.

Furthermore, as we see technology steadily advancing, some of us might be able to see the theory of quantum computing come to real life. Some of the implications of quantum computing can be very destructive because it will leave all the previous encryptions that we use now utterly useless. However, with quantum computing also comes quantum encryption which will be used to encrypted data once quantum computing comes to light. As of right now, we use 2048-bit encryption which is used for public-key encryption. Even if we started using 4,096-bit keys, they would be cracked in a few hours. According to the U.S. National Institute of Standards and Technology, they say that they are working on sixty-nine new methods to encrypt data with quantum computing. Quantum encryption does not mean end-users will be one-hundred percent secure. There is still the potential risk of end-users being uneducated to cybersecurity and click on a misleading link or downloading malicious viruses to a system.

## Reference

Avey, C. (2020, June 09). 7 key cybersecurity threats to cloud computing. Retrieved March 16, 2021, from https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/

Denning, D. E. (2019, June 14). Is quantum computing a Cybersecurity Threat? Retrieved March 16, 2021, from https://www.americanscientist.org/article/is-quantum-computing-a-

cybersecurity-threat#:~:text=Cybersecurity%20researchers%20and%20analysts%20are,weren't%20encoded%20at%20all.

Fortinet. (2016, May 18). Managing challenges and risks in ubiquitous it systems. Retrieved March 16, 2021, from https://www.fortinet.com/blog/industry-trends/managing-challenges-and-risks-in-ubiquitous-it-systems