Jykeim Giddens

CYSE 425W

Professor Pitman

11/14/2020

To start, I want to discuss the problem that arises from cyber security in the 21st century. As we grow in the digital era, there has been a bigger advancement in technology. The given connection between society and mandatory cyber security training would be that the society would be safer due to the fact that everyone knows the basic fundamentals of cyber security and why it is important to learn about it. While technology will continue to grow, mandatory cyber security training can no longer be an option for society.

Furthermore, there are numerous social factors that led to the development of mandatory cyber security training. The first one would be dealing with the advancement in technology. Technology is not only in our homes, but is also surrounding us by land, air, and space. New and rising technology, causes great harm to society because this will lead to a diverse network of attacks on multiple systems and organizations. The complexity of cyber security geographically is widely accessible.

A cyber attack can happen from another country to the United States within a matter of seconds. Being able to have a society that is completely cyber security literate is one the concerning reason for developing a mandatory cyber security training policy. “Cyberspace is the fifth domain of conflict”, this quote emphasizes that dealing within the cyber realm or what the society considers the internet, has problems within itself that the society should prepare for before engaging with it. (Russell, 2018, 5).

In addition, another social factor that influences the development of mandatory cyber security training is the lack of knowledge the common person in society has about cyber security. For example, individuals that work at specific jobs such as office work, or front desk assistant may not have the capability to understand cyber security due to the fact that it is not deemed necessary in the work environment. Implementing mandatory cyber training along with the correct risk management decisions would lead to a more efficient cyber awareness work environment. (*Cyber Situational Awareness*, 2016, 10-12)

With the introduction of COVID-19, this had led to great influence on all cultures. Since the pandemic started, a majority of jobs and schools have transitioned into an online or web based environment. Throughout the current pandemic, there has been an increase in cybersecurity attacks trying to gain leverage over the average computer user. (Sheperd, 2020, 4-10). Some schools have already experienced cyber breaches in their database and have been held for ransomware by attackers. The average computer user does not understand basic fundamentals of protecting themselves in the cyber world. This had definitely become a social factor that led to the development of the policy mandatory cyber training.

With implementing a mandatory cyber policy, there have been many social consequences involved. The most recent one that can be observed in society is the abundance of people who are getting involved in cyber security. Society is starting to understand basic principles of cyber security and what it means to be cyber safe. Being trained about cyber security makes society feel confident and safe that they can protect their own information from cyber attacks. Many cultures have shaped this policy through the use of media and news. Many people know in today’s society that information from your past is so easily accessible. From that standpoint, it causes individuals in society to want to try and protect their information from the public. Many

Works Cited

**Bibliography**

Building Future Generations of Elite Cyber Professionals (CNODP). (2014, April). *Journal of Information Warfare*, *13*(2), 7. https://www.jstor.org/stable/26487119?Search=yes&resultItemClick=true&searchText=Mandatory+cyber+training&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DMandatory%2Bcyber%2Btraining%26acc%3Don%26wc%3Don%26fc%3Doff%26group%3Dtest%26cty\_journal\_facet%3Dam91cm

*Cyber Situational Awareness* (Vol. 1). (2016). Army Cyber Institute. https://www.jstor.org/stable/26267298?Search=yes&resultItemClick=true&searchText=cyber+in+workplace&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dcyber%2Bin%2Bworkplace&ab\_segments=0%2Fbasic\_SYC-5187\_SYC-5188%2Ftest&refreqid=fastly-default%3A7e61ce39b6c71f

Guinchard, A. (2011, Summer). Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy. *Journal of Strategic Security*, *4*(2), 24. https://www.jstor.org/stable/26463928?Search=yes&resultItemClick=true&searchText=media+and+cyber+security&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dmedia%2Band%2Bcyber%2Bsecurity%26acc%3Don%26wc%3Don%26fc%3Doff%26group%3Dtest%26cty\_journal\_facet%3Dam91

Russell, S. (2018, Winter). Operating in the Dark: Cyber Decision-Making from First Principles. *Journal of Information Warfare*, *17*(1), 15. https://www.jstor.org/stable/26504126?Search=yes&resultItemClick=true&searchText=technology+and+cyber&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Dtechnology%2Band%2Bcyber%26acc%3Don%26wc%3Don%26fc%3Doff%26group%3Dtest&ab\_segments=0%2Fbasic\_SYC-5187\_SYC-5

Sheperd, L. A. (2020, June 21). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. 20. https://arxiv.org/pdf/2006.11929.pdf