Cybersecurity Article Review: "Cybersecurity Risk in a Pandemic"

Herald Anacta

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Science

Dr. Brian K. Payne, PhD

September 30, 2021

Article Reviewed:

Williams C, Chaturvedi R, Chakravarthy K. (2020, September 17). *Cybersecurity Risks in a Pandemic.* Journal of Medical Internet Research. https://www.jmir.org/2020/9/e23692

doi: 10.2196/23692

Cybersecurity Article Review; "Cybersecurity Risk in a Pandemic"

The article "Cybersecurity Risk in a Pandemic", written by Williams, Chaturvedi, and Chakravarthy (2020), talks about how a global scale pandemic like the COVID-19 increases the risk and likelihood of cybersecurity threats happening, not just in the United States but also to the rest world. The effects of cybercrime have already costed the world an upwards of trillions of dollars. It will continue to rise unless proper safety procedures and protocols, like implementing a timely, systematic upgrade procedures for both software and hardware, and a more consisted testing and securing of computer networks are put into place. The unpredictability of COVID-19, combined with the urgent dependency to technology became an avenue for cybercriminals to conduct cybercrime.

How it Relates to the Principles of Social Science

In almost every field of work or study, one must always adhere to principles. Without rules or code of conduct, the legitimacy of whatever work or study being done becomes questionable. With that being said, the article clearly follows the core principles of Social Science. It showed Relativism in a way that it showed how everything is related and connected. When the COVID -19 pandemic started last year, several if not most forms of business, either stopped and suspended their operations, or completely shut down. Other than essential and needed services like hospitals and grocery stores, those business who stayed open were forced to

employ and adapt a “work from home” approach for their employees. This led to the utilization of video conferencing software and applications like Microsoft Teams, Google Rooms, and Zoom. However, since this type of approach is somewhat new, not a lot of people knew how to work with it at the beginning of the pandemic. The sudden influx of utilizing these videoconferencing software and applications together with the unfamiliarity of the users, caused a lot of problems. One of most famous one is called “Zoom-bombing”. Basically, it is when an unregistered and unwanted user suddenly shows up uninvited in a Zoom meeting. The “Zoom-bomber” can gain access by just simply joining a random meeting. These incidents were deemed very dangerous since a random person can just show up to a company meeting and gain confidential information. Eventually, proper safeguards were put into place. Zoom meetings now required passwords, private meetings cannot be accessed anymore, unless you are part of the organization holding the meeting. The authors also displayed Objectivity in writing the article. They did not let their values and emotions dictate what they wrote. Lastly, the article displayed Parsimony. The whole article was simple and easy to understand. It did not contain words and technical jargons that would make it difficult to comprehend.

Article Hypothesis

The advancement in technology changed the way the healthcare systems work, this advancement in conjunction with COVID-19 caused data breaches in hospitals and phishing scams to patients, to be more prevalent during a pandemic. The fear of the unknown because of COVID-19 together with the heightened emotional response from people caused them to become more susceptible to phishing scams. Fraudulent websites, fake phone calls offering false government relief started to abound. The strain caused by the overcrowding of patients in hospitals together with the shortage of staff also affected the effectivity and monitoring of

computer networks. In these times of uncertainty, in times of a pandemic, the threat of cybercrimes greatly increases.

Types of Research Method Used

Archival Research and Case Study were the two primary methods of research that were used in the article. By comparing and highlighting the problems that were caused by previous natural disasters like Hurricane Katrina, they able to gather similarities that are cause by a large-scale catastrophe. It was mentioned in the article, that back in 2005, when Hurricane Katrina happened, hundreds of fake websites appeared online luring unsuspecting victims Another method of research that was used is Case Study. The article talked about the cyberattack that happened to the University of California, San Francisco (UCSF). The university was attacked by hackers who demanded payment in exchange for not releasing confidential information. It showed the readers that a similar type of attack can happen anytime to anyone, especially during a pandemic.

Types of Data and Analysis Done

Since a global scale pandemic rarely occur, it is very hard to get an actual comparative analysis. Additionally, since most of the world's data with regards to COVID-19 is only about a year's worth, the future trajectory and its impact to the world is still hard to predict. Despite of that, the authors were able to convey the increased risk that we are exposed to in the cyberworld as result of a pandemic The article were able to analyze and show what possible financial, economic, and social problems that might arise due to the rise of cybercrime in a time of pandemic.

Concept in Class that Relates to the Article

One concept from class that resonates with the article is the concept of ethics. Ethics can be described as the moral principle of a person. What is right, what is wrong? What is socially acceptable and what is not? In times of a pandemic, one would think that people would join hands, unite and help one another. Sadly, that is not the case. People still find ways to take advantage of people. Another concept that was discussed in class that would also relate to the article is the concept of psychology. More specifically, the psychology or the mindset of a hacker. An unethical hacker who steals information or bait people into phishing scams, during a during a pandemic, when people are suffering, clearly does not have the correct moral compass nor the correct state of mind.

How it Relates to the Marginalized Group

The article taught readers that certain marginalized sectors of the society like the elderly and those who do not have access to technology are more prone to the being victims of cybercrime during a pandemic. The elderly because they lack the sufficient knowledge or are not fully aware of the current trend of technology that we have in the world. Those who do not have access to technology like those who cannot afford a computer are also more likely to be victims of cybercrime. A good example would be the distributions of the stimulus check during the pandemic. Some of the people who opted for a physical check because they did not have access to computer, had their physical checks stolen or were sent to the wrong address.

The Article's Contributions to Society

Overall, the article was able to clearly convey to the readers the increased risk of cybercrime that happened and might happen again in a pandemic. It reminded the readers that as technology advances, the threat of cybercrime also goes up. That no mater what the situation is,

people who have a low moral compass, would do bad things. The article reminded the readers, that it is everyone's responsibility to be vigilant, be conscious, and adapt to the ever-changing world of technology.

References

Williams C, Chaturvedi R, Chakravarthy K. (2020, September 17). *Cybersecurity Risks in a Pandemic.* Journal of Medical Internet Research. https://www.jmir.org/2020/9/e23692 doi: 10.2196/23692