How has COVID influenced the cybersecurity of employees working in a new environment

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Davin Um
Fall, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____Davin Um_____ Date ____3/28/21_____
Author Name

Approved _____Sharon Tsai-hsuan Ku Date ___5/8/21_____
Advisor name, Department of Engineering and Society

Introduction

It is inevitable that the pandemic caused a total shift in the working environments of employees. According to Dwivedi et al (2020), the way of interacting with another and working for the organizations have drastically changed, which people who are working in academic fields are required to set up the home environment for online teaching and come up with different methods of socializing such as utilizing online platforms to meet. Most companies are utilizing digital technology in response to the pandemic, as large online businesses are working effectively in a remote environment. Donthu and Gustafsson (2020) fully supports the notion that internet-based companies are thriving, such as online entertainment, food delivery, online shopping, and online education. The employees are provided with great resources to solve conflicts and work efficiently even when they are working remotely.

These changes in the work environment must have affected employees' way of working, which could introduce human elements to cyber threats. The topic itself is an important issue, as the pandemic caused the society to work remotely and affected how the workers communicate between others. Organizations had to approach cybersecurity problems in a new way since cyber threats became more common for individuals working at home without proper network protection or device protection. With the research it can reveal how the perception of the employees towards cybersecurity has changed as well as how companies reacted to the threats, and find out how the future workforce management will be different.

Research Question

The research involves one major question which is "How did the employees' perspectives towards cybersecurity change?" The employees in the workplace prior to the

pandemic worked in a secure environment, in which the security system was already equipped with their devices and the network was protected. However, as the work environment shifted virtually, it was responsible for them to follow company's security policies and take educational programs that would prevent them from making mistakes, such as clicking phishing emails or not properly connecting to VPN. The employees themselves would need to take responsibility for securing their devices, otherwise they could be exposed by the cyber threats, ultimately resulting in virus and malware attacking the devices and interpreting the data. It should be interesting to study how employee's perception of cybersecurity and its importance shift in time before and after the pandemic. Another research question would involve "What kind of cyber threats have been trending since the pandemic?" Attackers are trying to take advantage of the situation that workers are working in poorly secured environments, and are trying to infiltrate their devices. There must be correlation between the two, and the type of attacks that increased should be evident. Researching this question will allow deeper understanding of the trend in cyber-attacks and witness how companies are responding to such attacks.

Literature Review

History of Cybersecurity: Cybersecurity does not have a fixed solution and is continuously evolving, as the history shows its context. The "network" between different computers began in the early 1960s, according to Warner (2012). At that time, the security issue related to the computer wasn't a serious problem, as it was only necessary for computers to hide data that belonged to another. Warner also states that in the 1970s, innovation in computer programming led to enhancement of security, such as administrator privileges, file systems permissions, and hashed passwords. But the development of technology had its downside as viruses and hacking became a threat to computer systems. For example, in 1979, the US Air

Force tested out different methods of attacking information security in which the military computers that held sensitive information were easily penetrated. Furthermore, in November 1979, an anonymous individual from the North American Air Defense Command (NORAD) infiltrated into the online missile warning computers' test scenario data and caused false alerts. The increasing amount of threats happening virtually caused the importance of cyber security to rise, which led to developments of anti-virus programs and strong security systems. Nowadays, social engineering has become a popular threat method infiltrating cybersecurity. Hatfield (2018) mentions different threats that affect social engineering, including impersonation to gain access to targeted networks, third party authentication to use the privilege of victim's account, phishing attacks to perform malicious actions, and many more. Many organizations are developing better ways to prevent cyber-attacks of such types.

Definition and types of Cybersecurity: Cybersecurity, according to Galinec, Možnik, and Guberina (2017) "is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries." Galinec et al (2017) describes the general key components and relationships related to cybersecurity, as threats are trying to attack the control (policy, encryption, anti-malware), then infiltrate into the asset (people, network, software, device), and if they are successful then they are able to achieve their goal of destroying or compromising the data. In order to protect themselves from such threats, organizations are developing cybersecurity strategies that can reduce the vulnerability in their systems. One of methods include cybersecurity risk management, which analyzes the security status of the system and takes necessary actions to respond to risk threats. The management system will be able to identify vulnerabilities and whoever's responsible for answering to the attack will deal with the

problem. Organizations also use the Cyberattack model, in which the development team creates an attack model that the intruders might use and recognize which vulnerabilities could lead to infiltration.

Trend of cyber-attacks: As employees are being more dependent on digital infrastructure, it becomes clear that online network reliance is becoming more and more important to businesses. Muton and Coning (2020) gives several examples of attacks that are trending, which one of them includes phishing attacks. Phishing attacks involve tricking the victim with false information and leading to a suspicious website or URL, ultimately causing information or grants given to the attacker. Fake URLs have become popular with the rise of COVID, which the scammers are taking advantage of people making typos when typing URLs, which leads to scam sites and trick people. Physical attacks involving social engineering are still happening, fake news involving the companies are being spread, and malicious sites such as fake COVID maps have also been trending since the pandemic. One of specific victims of these cyber-attacks has been healthcare organizations where the frequent use of telecommunications such as Zoom, Skype, email, has led employees to be more susceptible to phishing attacks. Williams, Chaturvedi, and Chakravarthy (2020) have found out that healthcare organizations were also receiving ransomware attacks. A cybercrime group called "Netwalker" was able to hack into University of California, San Francisco's (UCSF) system and demanded money in exchange for not releasing confidential information, which the group also hacked Champaign Urbana Public Health District website. It has become clear that there has been an increase in attacks through networks, as well as using mistakes of human elements to infiltrate into the database of businesses.

Cybersecurity issue and the approach: Managing security issues has become a significant

issue when the working environment has changed. O'Reardon and Rendar (2020) states that a shift of the working environment has exposed new threat vulnerabilities in terms of personal cybersecurity and third-party service providers. The attackers are trying to take advantage of the situation and access the personal information of businesses and individuals. However, companies are not being responsible for taking care of their employees when it comes to preparing cybersecurity. According to Furnell and Shah (2020), the data indicates that 30% of UK companies are well prepared for user education and awareness. This is directly related to how the companies have a set of rules on cybersecurity that explicitly sets what the employees are demanded to perform with their devices. The percentage shows that the employees are not well trained with regards to cybersecurity, which can lead to leak of information in unprotected networks. Funnel et al (2020) also demonstrates that 25% of companies are well prepared for home and mobile working, which indicates that there is a lack of cyber security-framed, written rules that employees should follow.

These results clearly show that many companies are lacking proper ways to secure their information and protect themselves from threats. In response to the situation, there are many methods suggested to prevent cyber-attacks. O'Reardon and Rendar (2020) provides many ways to successfully work from home, which include virtual meeting applications that only specific users can join. This prevents any confidential information that could be leaked using telecommunication such as email or messenger. The employees can also increase their awareness of phishing scams, avoiding any suspicious emails received through company accounts. Home network security is a major component of cybersecurity in remote working environments, in which robust security software will deny attacks from outside resources and employees should only download software that is from trusted sources. Some other minor methods that are

suggested by Funell and Shah (2020) include protecting email by using a strong password, installing the latest software updates, turning two-factor authentication for emails, and having back up data.

Reminder: This existing literatures are done in a context that individual and workspace are separate, and the literature review is being done under assumption that the COVID pandemic will affect the current standing of cybersecurity.

STS Framework and Method

For the research, the SCOT framework was utilized as to defining which social groups are involved in the project itself. The SCOT framework allows to define social groups such as companies, employees and attackers, which I can analyze how different social groups interact with each other and negotiate the problems they face. This framework is very effective in the research as I can specifically dive into those social groups and find relevant information that could be related to the research question, which analyzing and gathering data from company and employee social groups can provide answers to the research question that questions about change in the perception. The research will find different interpretational flexibilities of each social group, which the secureness should apply to the customer side while the flexibility and professionalism should apply to the employees group.

There are several social groups related to the topic, which the key players are the employees, attackers, and the companies. Among them the shared artifact is the cybersecurity and cyber threat issues. Both the employees and companies group face to protect themselves from cyber threats by using technology, which the attackers are trying to infiltrate the other social groups with cyber threats. The employees and companies group go through process of negotiation to have employees protect their devices and networks by following the guidance

given by the company, in return the company is able to fully operate securely. However there is always conflicts between the attackers and other social groups as attackers try to take advantage of the weaknesses that the employees or companies group has. Therefore the only solution left for employees and companies group is to have strong security implemented to their remote environment and prevent the cyber threat from happening, which there cannot exist any negotiation.

This is also closely related to ethical concepts as digital ethics have become a serious issue over the past years. When we think about digital ethics, there are privacy regulations and internet governance among nations. Different nations can hire professional hackers that can attack private companies or government sectors of other nations and cause damage, which is currently happening between many countries. There has to be set of regulations regarding cybersecurity and cyber threats, as the regulations will set guidance on how the nations should be dealing with problem related to cybersecurity, as well as consequences of not following the regulations.

Methods for Data Collection:

I would need to conduct quantitative research based on the employees who have changed their working environment. The data would be collected by conducting surveys to the employees, answering survey questions that I've created. Potential groups that could participate include companies that I have worked as an intern, which I can use the connection to find specific members for the survey. The IT department from the university could be another potential group for the survey. The number of participants will be expected to be 50 people, with an anticipated number of at least 10 people. I would also like to conduct documentation analysis, which will act as qualitative research for the question. It will involve using published journals

and articles and thoroughly studying the data that was collected. There should exist studies and articles from different companies and researchers that analyze employees' perception towards cybersecurity. Data analysis then can be used to find more specific information of employees' perspectives, which then can be compared to the quantitative data collected from the survey.

Data Analysis

Numerous scholar journals and articles published by different organizations show relevant information to how COVID has impacted the way that cyber threats are currently happening. According to a journal article published by Bernardi Pranggono (2020), due to the pandemic many people have become unemployed or have moved their working environment to their individual place, where they heavily rely on the usage of the Internet. As a result, the scammers are trying to take advantage of the situation using phishing attacks. One of the most common attacks that were found was scamming and phishing attacks. The data that was provided by the Sjouwerman (2020) illustrates that there were an increase of 600% coronavirus-related phishing email attacks in Q1 2020. These phishing attacks included password checks (40%), CDC Health Alert Network (10%), PTO Policy Change (7%), and many more. The other attacks included malware, which the hospitals became the main victim of the attack. In June 2020, the University of California San Francisco (UCSF), which the department was working on COVID-19 vaccine, was the target of a ransomware attacks and forced to pay $1.14 m to cybercriminals called Netwalker. DDoS became another common attack type, which the US Department of Health and Human Services Department became a target for DDoS attack back in March 2020. It is clear that one of the trends during the pandemic is that some of these cyber-attacks are being focused on healthcare organizations. Because the attackers know the importance of the data that is stored in the organizations'

systems, they take advantage of them and use ransomware to take control, asking money in favor of relieving the problem.

COVID-19: Cyber Threat Analysis, which was published by the United Nations Office on Drugs & Crime, also shows the common attacks that were done during the pandemic. The main attacks that the article discusses are phishing emails and malicious domains. Phishing has always been a common threat to cyber network, but has become more common. The emails are sometimes disguised as reports of the pandemic from the government, advertisement of facial masks, or a sale of a map that shows the coronavirus' outbreaks. These various emails have attachments or suspicious links that the user can click, which can expose ransomware to the user's device or steal private information of the user. As for malicious domains, fake websites or campaigns disguise themselves as real sites, alluding victims to click certain buttons on the site and releasing the virus. From the analysis, another trend can be found is that cyber threats are closely related to topics that involve COVID. The scam usually involves information related to the virus, whether it's an advertisement for a product or a recent news related to the virus. People are getting interested in these types of emails since the topic has become notorious among the society and want to know more about it.

Articles published by different companies such as Deloitte and Varonis support these trends. According to Deloitte's article written by Nabe (2020), Switzerland reported 350 cyber-attacks compared to the norm of 100 to 150 attacks, which the difference in the security level of the working environment is the main cause of the issue. The article illustrates that 47% of employees working from home fall for phishing attacks, and the video conferences that the employees are using are being hacked. Varonis' article goes into detail about different types of attacks, which include phishing, DDoS, and malware. The trend analysis done by Sobers from

Varonis (2021) gives a more detailed picture of how the cyber threats have been occurring. Phishing scams have increased from 1 in 10000 for 2019 to 1 in 4200 emails in 2020. Knowing the advantage of the COVID pandemic situation, the ransomware's payment rose 33% in 2020 over 2019. Healthcare organizations have been experiencing numerous attacks, of which 93% of the organizations have experienced data breaches in their systems.

From the analysis of different articles, it became evident that the cyber threats are attacking the most vulnerable parts of society. Not only the criminals are attacking public services, they are also attacking individuals who are vulnerable of getting attracted into false information. Products and information related to the pandemic tricks people into clicking spam and phishing emails, which in return gets attacked by cyber threats. The pandemic has caused the cyber threats to critically damage part of society that are essential to us, such as education and healthcare.

The survey was done to analyze the change in perspective of cyber security among the employees. It was fortunate enough to have the surveys done by the company that I worked before, which was Verizon. I asked my former manager if it was possible to conduct a survey related to the topic, and she was kind enough to have 10 respondents answer the survey questions. The survey questions included what kind of changes did the employees notice due to the pandemic, their initial response to the change, their change in perspective of cybersecurity and asking whether they have changed or not. All 10 respondents answered that they are now working remotely, and the common response for noticing the change included communicating online, working at home with a weak security network, and not being able to work in a safe place. Most of the respondents did think that they were working on a weaker environment since the remote environment was insecure compared to the working environment inside the

company. When asking for their initial response to the change, 55.6% said that working normally as they have done before would be sufficient while 44.4% said there needs more emphasis towards securing their devices. Surprisingly, when asking for their change in view towards cybersecurity, 60% of the respondents answered that they have changed their thoughts. Some of the responses included “Was working at an environment where security was provided for granted, now have to pay attention to what I do with personal device,” and “Already knew about remote working, and knew the importance of having secure systems on the devices when working remotely.” 40% of the respondents answered their point of view towards cybersecurity hasn’t changed, as some say “Because the company has provided devices with secure system, I will be good to go as long as I'm careful enough,” or “I knew security would become number one issue when working remotely, and knew the importance of it.” The 40% who responded that they haven’t changed their mind did not mean that they all do not care about the security, but already knew the importance of it. The final question asked a core difference of cyber security between working at the company and working remotely, and most of the respondents answered that less humane errors should be made, properly using a secured network and system is important, and improper use of the devices were needed to be avoided.

The survey is able to illustrate that no matter what type of employee you are the new social-technical condition they are faced in has affected their perspective towards cybersecurity. Because of change in the working environment, employees have to be extra cautionary when they are working and follow the security guidance that is provided by the company. Those who are familiar with cybersecurity will adhere to the rule and keep their devices safe, and those who aren’t familiar with cybersecurity will face some difficulties of protecting themselves from threats. With these changes, the employees have acknowledged

how important it is for cybersecurity to protect their devices from threats since the remote environment can be exposed to different kinds of threats. Those who thought of cybersecurity as something that is granted now see the importance of it and strictly follow the guidance. It seems that because the employees have shifted their working environment from company itself to their personal houses, they have become extra cautionary of what they are doing, which indicates that their awareness of cybersecurity has significantly increased.

Conclusion

The COVID pandemic has truly shown its impact on the trend of the cybersecurity threats. One definite trend is that organizations that are closely related to the pandemic, such as the government or healthcare organizations, have become the target of the attack. These targets hold valuable information which could be used as a hostile in return for either money or other secret information. Another trend that is seen is these cyberattacks involve topics related to the pandemic itself. Many phishing attacks or scams involve individuals that fall into false advertisement or information, which they leak their private information or are exposed to malware in their devices. Lastly, these trends show that the human element is a big part of cyber-attack during the pandemic. Most of the cyber-attacks that were trending in 2020 included phishing attacks and malwares and these happen frequently because people are not careful enough of what they are doing.

Bibliography

Crowther, K., & Rust, B. (2020, September 1). Built-In Cybersecurity: Insights Into Product Security for Cyberphysical Systems at a Large Company. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy, 18(5),* 74 - 79.

Donthu, N., & Gustafsson, A. (2020, September 1). Effects of COVID-19 on business and research. *JOURNAL OF BUSINESS RESEARCH*, 117, 284 - 289.

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Upadhyay, N. (2020, December 1). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55.

Furnell, S., & Shah, J. N. (2020, August 1). Home working and cyber security – an outbreak of unpreparedness?. *Computer Fraud & Security*, 2020(8), 6 - 12.

Galinec, D., Možnik, D., & Guberina, B. (2017, July 1). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, 58(3), 273 - 286.

Hatfield, J. M. (2018, March 1). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102 - 113.

Hawdon, J., Parti, K., & Dearden, T. E. (2020, August 1). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *AMERICAN JOURNAL OF CRIMINAL JUSTICE*, 45(4), 546 - 562.

Jang-Jaccard, J., & Nepal, S. (2014, August 1). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences,* 80(5), 973 - 993.

Kramer, A., & Kramer, K. Z. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility. *Journal of vocational behavior, 119, 103442. https://doi.org/10.1016/j.jvb.2020.103442*

Mouton, Francois & de Coning, Arno. (2020). COVID-19: Impact on the Cyber Security Threat Landscape.

Nabe, C. (2020, December 15). Impact of COVID-19 on Cybersecurity. Deloitte Switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

O'Reardon, M. E., & Rendar, M. (2020, September 1). Managing Security Risk: How COVID-19 Pandemic and Work-from-Home Arrangements Pose New Security Considerations. *Employee Relations Law Journal*, 46(2), 62 - 67.

Pranggono, B, Arabo, A. (2020) COVID-19 pandemic cybersecurity issues. Internet Technology Letters. 2021; 4:e247. https://doi.org/10.1002/itl2.247

Sjouwerman, S. (2020, April 9). Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%. Blog. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600.

Sobers, R. (2021, March 17). 134 Cybersecurity Statistics and Trends for 2021: Varonis. Inside Out Security. https://www.varonis.com/blog/cybersecurity-statistics/.

Warner, M. (2012, October 1). Cybersecurity: A Pre-history. *Intelligence & National Security*, 27(5), 781 - 799.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020, September 1). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*, 22(9), N.PAG.