The Impact of COVID-19 on Cybersecurity

Ayanna Armstrong
Computer Science Department
Hampton University
Hampton, VA
(Faculty Advisor: Dr. Chutima Boonthum-Denecke)

Abstract- This report will discuss the impact of COVID-19 on cybersecurity. This report also discusses cyber threats in the home office, the healthcare and public health (HPH) sector in attackers' sight, and the rise of COVID-themed phishing attacks targeted towards remote workers and internet users. Tips on mitigating cyber risk will also be touched upon. This study utilizes surveys conducted to identify the effects this ongoing pandemic has had on businesses and people.

I. Introduction

The COVID-19 outbreak was formally classified as a pandemic in March 2020 after it spread to more than 100 nations. For almost three years, the world has been battling this rare virus. The disease's expansion not only had apparent impacts on people's health and the economies of entire nations, but it also precipitated abrupt and profound changes in the way of life for millions of people. Videoconferencing has taken the place of social and commercial gatherings, and work and study have moved indoors. Concerns about cybersecurity have only grown because of the big shift online [6].

Businesses immediately adjusted by abruptly converting workers to remote working in response to the COVID-19 pandemic, also known as the Coronavirus, an upper-respiratory illness that hit Wuhan, China in 2019 and spread throughout the world in January 2020. Groups, crowds, and mass meetings were strongly discouraged as part of social distancing measures implemented to maintain a physical separation of 6 feet or 2 arms lengths between individuals to prevent the spread of this extremely contagious disease [5]. Employees of all ranks were either laid off or instructed to work from home (WFH) for safety because of self- and government-mandated quarantines. Organizations today face the problem of safeguarding sensitive data from dangerous employee behaviors targeted by hackers and social engineering as WFH or teleworking became the norm [10].

In the most prevalent COVID-19 cyber threat, emails promise useful information but instead send harmful malware for cyberespionage, ransomware installation, and credential theft. Examples comprise:

- A coronavirus safety measures PDF that contains a remote access trojan
- Through a shipping-related email campaign with a coronavirus theme, information-stealing malware was spread. Through a coronavirus-themed paper, a virus was spread.
- A ransomware infection called "Coronavirus" that made use of a bogus version of the WiseCleaner site for Windows system tools through an email with the subject "Emergency Regulations," which appears to be from the Chinese Ministry of Health

Up to this point, a lot of coronavirus social engineering cases have taken the form of official government or public health pronouncements. As the virus spreads to the United States, some actors may modify their strategies to assume the personas of other well-known public figures, such as legislators and regional health authorities.

Phishing scams have been on the rise since COVID-19 took its peak. Malicious actors have taken extreme steps to impersonate reputable companies.

Phishing campaigns target Microsoft Outlook and Office365—as well as credit card information—while pretending to offer infection-prevention strategies, information on fresh cases, and general COVID-19 "knowledge" [4]. Scam artists claim you can:

- Provide food, water, and medical attention in exchange for bitcoins, occasionally with a QR code.
- Gain access to information that "your government is not telling you about"
- Invest in hand sanitizers, vitamins, supplements, and other anti-infection items.
- Order a COVID-19 vaccine through a phony PayPal link and pay with bitcoin.

II. Methodology

This study will use a combination of a literature review and a user survey to collect data and gather results directly related to my thesis. The survey will be comprised of the participant declaring whether they work from home and any security awareness their employer has implemented as well as the occurrences of phishing scams since the COVID-19 pandemic. These questions will help in the analysis of how the COVID-19 pandemic has impacted cybersecurity and the advancement of malicious actors. Analysis of these components will create a very clear understanding of the essay's matter.

A. Literature Review

In phishing scenarios, social engineering, which seeks to take advantage of internet users' vulnerabilities, is crucial. Fraudsters utilize emails to target people and seek financial or personal information by using sophisticated and difficult social engineering techniques. Additionally, harmful content is installed on target systems or devices by tricking users into opening attachments or clicking links in phishing emails that include dangerous content. The primary idea behind social engineering was to utilize socially customized tactics to access computer systems by obtaining sensitive information such as passwords or usernames [2]. However, the reach of social engineering has expanded to include internet users' personal and financial data. Three socio-psychological elements of social engineering while preying on human weaknesses are "alternative paths to persuasion, attitudes and beliefs that affect human relationships, and strategies for persuasion and influence" [10]

Attackers use social engineering to trick victims into giving out private information. In a frequent form of social engineering attack called phishing, thieves pose as reliable organizations to take advantage of their intended victims. Attackers frequently use the victims' fear, curiosity, altruism, or apprehension to influence them into providing their credentials. People rely more on internet services as ordinary everyday tasks move online. Cybercriminals now have more options to entice victims thanks to the shift of tasks from traditional, paper-based processes to online ones.

Cybercrime normally consists of three basic elements: (1) a victim who is the target of a cyber-attack, (2) a motive, or the reason why the assault was carried out, and (3) a weakness or opportunity that allowed the crime to be committed [34]. The first two prerequisites will be satisfied when user's internet presence rises. The third element for a successful attack is influenced by various principles, including distraction, time constraints, compassion, and need [35]. Attacker activity typically increases when the parameters are satisfied because they can optimize their chance of success [38]. Natural disasters have historically been used as a golden chance by adversaries to conduct social engineering. For example:

Ebola Virus Outbreak: The longest Ebola outbreak, which lasted two years in west Africa, was in 2014. Even though the Ebola virus did not spread globally, hackers used phishing and other schemes to target vulnerable populations of individuals [1].

A total of 200,000 spam emails with Ebola news updates and 700,000 phishing emails requesting donations to fictitious organizations were detected by Barracuda Networks [2].

Australia's Bushfire: Attackers used false identities from prestigious institutions, the government, or well-known charities during the Australia bushfire that occurred in late 2019 to trick victims into giving them money or sensitive information [8].

Contrary to these natural calamities, the COVID-19 epidemic has generated widespread terror [8]. As a result, criminals have begun using phishing or scam websites with COVID-19-themed content to prey on people's fear and sympathy [8].

One of the main targets of cyberattacks during the pandemic has been the healthcare industry. The issues with cybersecurity in the healthcare industry have been brought to light by hacking attempts on healthcare institutions. These consist of medical institutions, drug manufacturers, and research establishments [4]. Organizations in the healthcare sector are susceptible to cyberattacks. Since these organizations are supported by cities or nations, which frequently have very severe budget limits, one of the main reasons is due to the limited finances these organizations must safeguard their IT systems. To control medical devices throughout hospitals, for instance, many healthcare organizations continue to use old software or OSs like Windows 7 or Windows XP that are no longer supported [7]. In fact, according to Europol, healthcare facilities are seen as an accessible and lucrative target for ransomware. Computers now operate modern hospitals. Modern hospitals make extensive use of computers and the Internet of Things (IoT) to store, monitor, and manage medical equipment including ventilators and intensive care units (ICUs).

While new technologies, particularly platforms like the Internet of Things (IoT), have made it easier for us to work and complete our jobs, they have also provided hackers more opportunities. The extent and severity of the coronavirus epidemic have greatly increased the quantity, speed, and size of cyberattacks. IoT devices experienced a rise in cyberattacks, which caused IoT networks to become unavailable because of exposed access credentials. In fact, even modern equipment for the house is getting into corporate networks.

Since the epidemic began, enough time has passed for many organizations to have resolved any initial problems that came with the switch to remote work. Yet one issue has continued to have an impact on numerous firms. Many employees were obliged to utilize their own computers to access corporate networks and finish work-related duties due to a lack of company-owned laptops and devices. These people continued to browse the internet, use social media, shop online, and stream entertainment at the same time, which is more common and frequently hazardous. These personal devices are even more susceptible to infection because many of them lack desktop security and endpoint protection.

This error could be quite harmful from the standpoint of IoT security because attackers can still accomplish their objectives without having direct access to, say, a personal laptop. Through routers, tablets, gaming, and entertainment systems linked to the home network, as well as IoT devices like smart air conditioners, cameras, and home appliances, malware can be distributed inadvertently.

Bitcoin has grown to be one of the most widely used currencies that attackers request as payment due to its anonymity and speed of transactions. Every sort of organization faces a major threat from ransomware because it not only locks data from access but also sells the information if the user refuses to pay the demanded ransom. Well, the loss of life in these circumstances is not anticipated. However, serious human casualties could occur if an intrusion leads to a health emergency that affects the entire world. COVID-19 and malware provide hackers with a special, adaptable platform for attacks. Medical services are more important than ever and are frequently simple targets for malware. When clinics, emergency rooms, and public institutions are assaulted, the criminals are confident that the health organizations will pay the ransom since they are too busy treating patients to keep their networks down. During a pandemic, it might turn into a complete tragedy. In addition, Interpol warned hospitals and other healthcare facilities that they were vulnerable to ransomware attacks at times of increased anxiety and communication in the medical community.

Employees of healthcare organizations, who ought to have known about the hazard, hampered the work of the healthcare system. For instance, a guy fired from his position as vice president of the American business Stradis Healthcare in the spring of 2020 blocked the supply of personal protective equipment for doctors for several months as retaliation. He maintained a private account through which he allegedly undermined the efforts of his former coworkers, per FBI intelligence. In January 2021, it

was reported that he had received a one-year prison term [9].

Criminal activity has changed in response to COVID-19. While the threat of physical crime, such as home invasions and pickpocketing, may have decreased as a result of the epidemic, targeted cybercrime is on the rise as thieves take advantage of public concern over COVID-19 [7]. Cybercriminals are changing their strategies and increasingly attacking people in their homes, which are often also their offices in many situations. Companies now face more cyber risks as working from home opens the door to new types of data theft. Employees can also be a weak link in company IT security systems, making them more vulnerable to cybercriminals trying to acquire corporate data, consumer information, and intellectual property.

The expanding cyber danger is exceeding most organizations' capacity to manage it effectively as the economy becomes more and more digital. Personal information about employees, corporate data, consumer information, intellectual property, and critical infrastructure are all at risk. Although it is yet difficult to predict the COVID-19 crisis's long-term effects, it will undoubtedly have significantly accelerated corporate digitalization. However, the cyber threat is also escalating, and the fact that many employees are now working from home poses new dangers.

Many businesses did not give workers office supplies. Instead, they permitted employees to connect from their sometimes inadequately protected home devices to the corporate IT infrastructure and do business [3]. IT managers at the office oversee protecting the Internet channel. However, setting up one's own routers and networks when working from home increases security hazards. As a result, between March and April 2020, assaults on unprotected RDP ports—the most widely used remote connection protocol on Windows computers—increased tenfold in Russia and seven times in the US [5].

Employees may modify documents and take part in meetings in person while they were at work. The demand for videoconferencing software and communication tools has skyrocketed in the realm of remote work [4]. Cybercriminals have expressed interest due to the increase in demand. Even reputable videoconferencing software has security flaws. For instance, a flaw in the Microsoft Teams business messaging service that had given an attacker access to all accounts inside a company was found and fixed in March 2020 [1]. The creators of Zoom for macOS made bug fixes at about the same time that prevented others from controlling a user's device [1].

Employees frequently collaborate on documents and share files using personal accounts on free platforms like Google Docs. These services typically lack centralized rights management, which would allow them to safeguard private information.

Mitigating Cyber Risk

Two immediate priorities have been presented to chief information security officers (CISOs) and their teams during the COVID-19 pandemic. One is securing work-from-home agreements on a never-before-seen scale now that businesses have instructed staff to cease traveling and congregating, and many government leaders have suggested or commanded their people to stay at home as much as possible [10]. The other is preserving the privacy, integrity, and accessibility of consumer-facing network traffic as volumes grow, in part because of consumers spending more time at home [6].

Employees who work from home still need to use good judgment to ensure information security even with tighter technological protections [16]. The extra stress that many people experience may increase their susceptibility to social engineering attempts. Some workers might decide to engage in behaviors that expose them to additional risks, such as visiting harmful websites that office networks restrict when they discover that their activity isn't being watched as closely as it is in the office [4]. Creating a "human

firewall" will make it easier to make sure that remote workers contribute to maintaining the security of the company.

New phishing scams with COVID-19 themes prey on fear, capture helpless people, and cause disruption in the workplace [12]. Therefore, those who telecommute should as soon as possible learn about their digital security and cyber security bombing since the cost of global cybercrime damage could double this year. Organizations generally wouldn't have a complete set of tools available for employees who operate from home [11]. If you don't already have a home office, try your best to create a room that is just used for business that is specially decorated and equipped. When people begin working from home, their profitability may temporarily decline if their home office is not properly set up.

There are two types of working from home: changeless or all-day work from home and present-moment or intermittent work from home. With COVID-19, it is uncertain how many people will be at home, adding to the problems. There is little doubt that these are distressing times. The pandemic is being fought against by friends and relatives. However, the more effort you put into talking with friends, the higher chance you have of avoiding feelings of distance, which can lead to despondency. Today, it is incredibly simple to feel anxious or depressed. By maintaining the spirits, it is necessary to establish norms or some similarities.

B. User Survey

I will collect data from employees who work from home pertaining to IT security measures put in place by their companies/agencies and collect data on any trends of any COVID-19-related phishing mail/spam mail/fraudulent emails. The purpose of my survey is to understand the different ways in which the COVID-19 pandemic has affected the rise in cybersecurity threats in organizations and remote workers. I will analyze this survey along with other sources of information to find any patterns and make conclusions related to my thesis.

III. Results

This section will cover the cumulative results obtained from my research methodology outlined in Section II.

A. Work-from-home transition

Many nations aggressively encouraged or regulated minimizing physical presence at work as the COVID-19 pandemic spread over the world and social distance was necessary to limit contagion. As a result, many companies adopted digital technology to continue running, allowing staff to work remotely while utilizing resources like videoconferencing, cloud services, and virtual private networks. Businesses best positioned to make a relatively seamless transition to working from home and best able to maintain output levels were those that could quickly adapt or exploit pre-existing telework capabilities.

Work-from-home opportunities have persisted long after the pandemic scare has faded. The relative success of working from home is one of the disaster's few silver linings, according to HR directors of large companies [15]. Working from home is advantageous for both managers and employees, even on regular days. Organizations have spent the past few weeks putting out fires as they built up the IT infrastructure, which has been the biggest obstacle to implementing virtual workspaces. Organizations are planning to redesign workplace seating in accordance with social segregation norms, use move-based work, have meetings virtually, improve cleaning protocol with visit sanitization and the placement of hand sanitizers, and reintroduce access cards in favor of biometrics.

B. Online Shopping Increase

With the COVID-19 pandemic-related retail closures, online buying is more common than ever. The combination of less money spent on eating out and more time spent at home led to an increase in e-commerce. Businesses that did not previously offer online sales are creating websites to maintain the status quo and remain in operation. Even though it may seem ideal to be able to choose the items you want to buy without having to make the effort to go to the store, this increased convenience is not without possible drawbacks for customers. As the number of online shops grows, more consumers' personal information is in their possession [11]. Given the uncertainty caused by the COVID-19 epidemic,

people are particularly susceptible to misleading and fraudulent marketing tactics.

Prior to the coronavirus disease COVID-19 pandemic, online purchasing was progressively rising. With stay-at-home orders already prevalent across the nation, a significant rise in online purchases of groceries, clothing, and household goods might be anticipated. Even though consumer behavior is complicated, and that the pandemic changed the demand for some products, the difficulty to buy in person and the huge proportion of American households with an internet connection would suggest a significant growth opportunity for online merchants.

The biggest threat to consumers during the COVID-19 epidemic comes from vendors that use customers' fear and uncertainty as a tool for manipulation and pressure. Due to the exceptional conditions, people are more likely to believe advertisements and marketing initiatives than they otherwise would [17]. For instance, consumers are much more willing to believe the information in emails about at-home coronavirus testing kits or donating to families affected by the pandemic than they were before the outbreak [13]. Consumers' susceptibility is being exploited by e-commerce. While it may be entirely lawful in some circumstances and perhaps expected that there will be more people using the internet because most Americans are stuck at home, it is illegal to use this additional traffic to deceive and hurt consumers.

C. User Survey Results

I conducted a survey to analyze how the COVID-19 pandemic has affected cybersecurity. My survey consisted of seven (7) questions, completed by 100 respondents. Participants of my survey are anonymous and consisted of people of different ages and occupations. The findings of my survey are as follows:

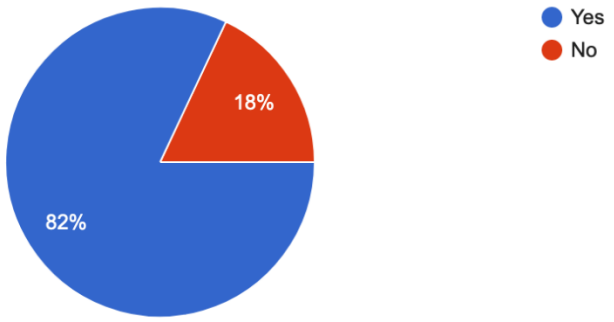

Figure 1: Do you primarily work from home?

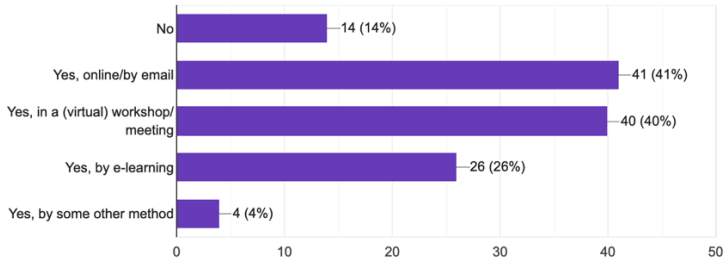

Figure 2: Has your employer provided mandatory training/awareness raising on working securely from home?

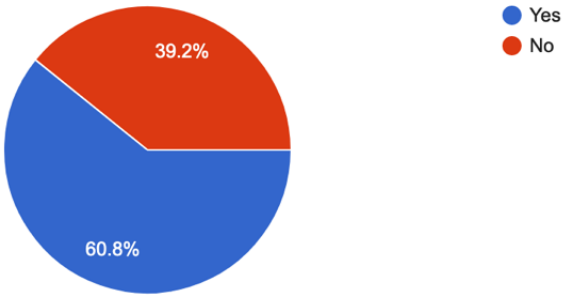

Figure 3: Have you received any COVID-19 themed phishing scam while working from home?

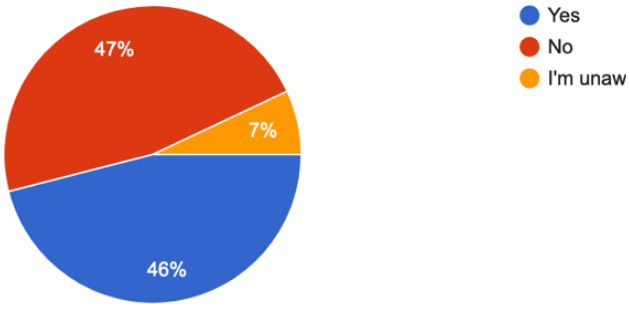

Figure 4: Do you fall for phishing scams while working from home?

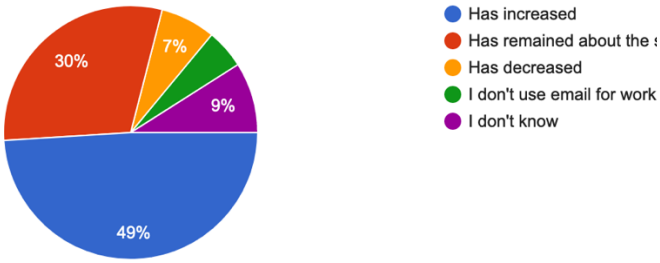

Figure 5: How has the number of phishing mails/spam mails/ fraudulent emails you receive at work changed since the COVID-19 crisis?

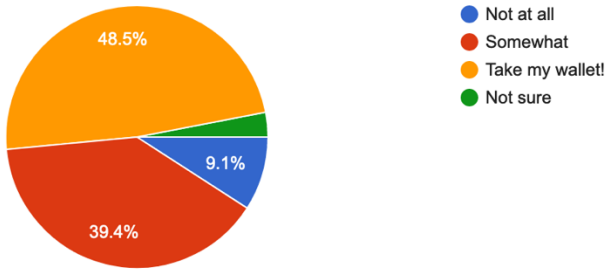

Figure 6: Overall, how has COVID-19 impacted your online shopping/buying behavior?

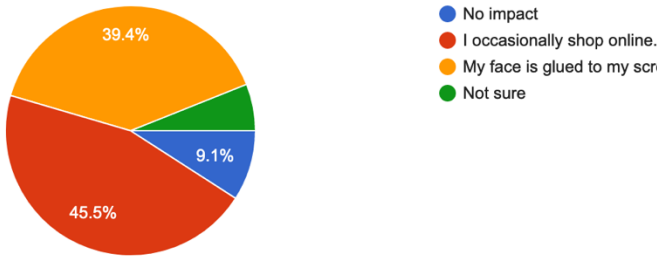

Figure 7: How much do you rely on IoT devices since the pandemic?

IV. Analysis of Results

A. Remote Training for Employees

My research focused on the topic of the impact the COVID-19 pandemic has had on cybersecurity. One of the most prominent topics that have been discussed in this report is the importance of cyber training for employees working from home. Due to the growing popularity of remote work, both businesses and people are choosing to work from home [13]. This has led to increased productivity, adaptability, and efficiency at work coupled with the availability of technology, but it also presents certain cybersecurity problems. In today's business world, cybersecurity is paramount, especially for remote workers [17].

Employees that receive cybersecurity training are better able to identify, protect against, detect, and respond to security threats, which increases their level of cyber resilience. Employees are less likely to fall victim to traps if they are trained to recognize common attacks and avoid common security risks. Lessons on cybersecurity will also give students a solid understanding of the company's data security strategy, enabling them to react quickly and decisively should emergencies happen. The organization will be better able to prevent, mitigate, and respond quickly to cyber-attacks by offering this crucial training, increasing the enterprise's overall cyber resilience.

Cybercriminals aren't afraid to emphasize their advantage since they know that remote workers are less likely to have gotten the training that enables them to recognize sophisticated signals. According to the results of my poll, phishing communications are proliferating and growing more alluring to employees, which has a significant impact on clickthrough rates while escalating the danger for firms.

B. Online Consumer Presence

Because of governmental restrictions and customer concern over the potential health danger involved with in-store purchasing, the COVID-19 pandemic led to an upsurge in online shopping. Everyone's shopping habits have changed as a result. Whether you preferred in-person browsing or internet buying, the pandemic changed habits in a variety of clear and

less obvious ways. As customers got used to standing in line, curbside pickup and internet buying also became commonplace. Although new variations keep appearing [13], COVID-19 is still here nearly four years later. Consumers appear to be content with their online experience and are purchasing online more than before the outbreak, even though restrictions are being relaxed and stores are reopening in some countries.

Following the Covid-19 outbreak, many people who formerly shopped at their local stores have migrated to online retailers. Unfortunately, as online consumer activity has grown, so too have cybercriminals' efforts to prey on the gullible and ignorant, leading to significant losses for those who fall victim to these dishonest people [15]. However, even if online fraud and cybercrime are on the rise, you don't always need to steer clear of online buying. If you take the necessary steps and heed crucial Internet security advice, you can purchase safely online.

Online buying is, overall, a relatively safe pastime. Individuals themselves, as well as their internet and online buying behaviors, are what contribute to the danger. And it is precisely what online crooks rely on. They count on you not knowing how to identify phishing emails and how to avoid them [14]. They count on you to utilize simple passwords or the same login information across all your internet accounts. They count on you signing into private accounts over a public Wi-Fi network. In essence, they count on you, the customer, to disregard a few obvious, common-sense instructions.

C. Growth of IoT Devices

The concept of the Internet of Things (IoT), or networked "smart" gadgets, is not new. The number of creative and occasionally unexpected use cases we see the Internet of Things (IoT) being used to each year is astounding, and this is never truer than it is right now, when it is being used to assist manage the COVID-19 situation and advance healthcare.

The prolonged pandemic has put a burden on the world's public services, healthcare system, and economy. Lockdowns and working from home, it has also put us to the ultimate test. With application cases and innovation for healthcare, COVID-19 testing, building health, and remote device maintenance, IoT technology opens new options and can help us develop a new normal [16].

Wearable tech has a wide range of potential applications for combating the infection. The identification, monitoring, recovery, and management of coronavirus symptoms and effects are being done with the help of wearable technology, such as smart watches, smart bracelets, and smart patches [16]. During the pandemic, telemedicine transitioned from being mostly underutilized to a commonplace healthcare option because to smartphone applications and functioning. While engaging in social withdrawal, patients can still communicate with their healthcare professionals.

IoT has a lot of promise to speed up the pandemic's end, but there are still a lot of challenges that need to be overcome before it can be successful. IoT development is sometimes attributed to privacy concerns and a lack of cybersecurity discipline [12]. Many IoT devices are made without considering security, whether on purpose or not. Sensitive information may be exposed when those devices enter households and larger networks, making the networks they are connected to susceptible to cyberattacks. Governments all over the world are now focusing on regulating smart devices as a result.

V. Conclusion

Although it frequently appears on the agenda of executive committee meetings, given the escalating concerns posed by the pandemic, cybersecurity may require additional consideration. Businesses should be proactive in addressing the threats and develop strategies for preventing successful cyberattacks rather than reacting when they happen amid future waves of the coronavirus [5]. Even though prevention measures are crucial, cyberattack detection, response, and recovery capabilities are also required.

This pandemic has shown us that minimizing the hazards associated with cyberattacks requires careful planning. The damage of a cyberattack can be lessened by having the ability to respond rapidly to unforeseen circumstances. Businesses that have already profited from safe remote working options will be better equipped to handle the rising number of cyber threats [6]. Companies that were unprepared will need to prioritize activities to close their cybersecurity gaps with best practices while also swiftly assessing their susceptibility to cyber-attacks. Additionally, firms should make using corporate-

owned devices the norm when granting remote access to critical and secret data. Cyber risks should be evaluated when accessing corporate data from a personal device, and steps should be made to reduce exposure to cyber threats.

Cybercriminals have profited from this pandemic by focusing on weak individuals and systems. It is a predicament that is also unlikely to alter in the near future [2]. For a variety of reasons, healthcare organizations are one of the prime targets of cyberattacks during the pandemic [17]. As a result, it is essential that healthcare companies strengthen their defenses against cyberattacks, such as by implementing a thorough strategy for cybersecurity.

Strong ethics training and security education programs are the first steps in providing teleworkers with cybersecurity protection [4]. No matter where they work, users must be taught not to click on dubious links and to always guard their log-in information. It is crucial to have a top-notch cybersecurity system that can both remove infections and pinpoint their source in the case that cyber assaults are successful [3]. No matter where they work, all employees must be accountable for preventing social engineers and hackers from exploiting the organization. Executive and line managers, professionals, technicians, suppliers, consultants, receptionists, and anyone with a keyboard might all be targeted for abuse; however, teleworkers might be the most marginalized and exposed. I contend that it is now impossible to overlook the enormous problem of protecting against human-based cyber and social engineering vulnerabilities. Businesses will continue to WFH for the foreseeable future as the US starts to recover from the COVID-19 pandemic [9]. No matter where we telework, we must all be on guard against the epidemic of encrypted malicious traffic from hackers and social engineers because camouflaged phishing threats, malware, and ransomware are on the rise.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

[1] *4 Coronavirus-Related Cyber Threats to Watch Out For*. (n.d.). Www.boozallen.com. https://www.boozallen.com/insights/covid-19/coronavirus-related-cyber-threats.html

[2] Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, *11*(3), 215824402110318. https://doi.org/10.1177/21582440211031879

[3] Bitaab, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., Kim, D., Bao, T., Wang, R., Shoshitaishvili, Y., Doupe, A., & Ahn, G.-J. (2020). *Scam Pandemic: How Attackers Exploit Public Fear through Phishing*. https://www.ftc.gov/system/files/documents/public_events/1582978/scam_pandemic_how_attackers_exploit_public_fear_through_phishing.pdf

[4] Boehm, J., Kaplan, J., Sorel, M., Sportsman, N., & Steen, T. (n.d.). *Cybersecurity tactics for the coronavirus pandemic*. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20tactics%20for%20the%20coronavirus%20pandemic/Cybersecurity-tactics-for-the-coronavirus-pandemic-vF.pdf

[5] Borkovich, D., & Skovira, R. (2020). WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. *Issues in Information Systems*, *21*(4). https://doi.org/10.48009/4_iis_2020_234-246

[6] *COVID-19 and working from home: balancing cyber security and productivity*. (n.d.). Deloitte Switzerland. Retrieved December 29, 2022, from https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html

[7] DQINDIA Online. (2020, November 11). *The impact of pandemic on IoT security*. DATAQUEST. https://www.dqindia.com/impact-pandemic-iot-security/

[8] Grustniy, L. (n.d.). *The great lockdown: How COVID-19 has affected cybersecurity*. Usa.kaspersky.com. Retrieved December 29, 2022, from https://usa.kaspersky.com/blog/pandemic-year-in-infosec/24451/amp/

[9] Innarelli, M. (2020, November 12). *Online Shopping Obsession: Consumer Security Risks Brought on By E-Commerce Spike Amidst COVID-19 Pandemic | Journal of High*

Technology Law. Sites.suffolk.edu. https://sites.suffolk.edu/jhtl/2020/11/12/online-shopping-obsession-consumer-security-risks-brought-on-by-e-commerce-spike-amidst-covid-19-pandemic/

[10] Kaspersky. (2021, February 19). *Tips to Safe Online Shopping*. Usa.kaspersky.com. https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping

[11] Kataria, S. (n.d.). *IoT Security in the COVID-19 Pandemic*. Blog.isa.org. https://blog.isa.org/iot-security-in-the-covid-19-pandemic

[12] Kaushik, M., & Guleria, N. (2020). The Impact of Pandemic COVID -19 in Workplace. *European Journal of Business and Management*, *12*(15). https://doi.org/10.7176/ejbm/12-15-02

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

[14] Nheu, W. (2022, May 17). *The importance of training remote employees on cybersecurity*. Cyber Resilience Blog. https://www.backupassist.com/blog/the-importance-of-training-remote-employees-on-cybersecurity

[15] Pranggono, B., & Arabo, A. (2020). COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

[16] Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021, February 16). *Cybersecurity and Countermeasures at the Time of Pandemic*. Journal of Advanced Transportation. https://www.hindawi.com/journals/jat/2021/6627264/

[17] TaylorWessing. (2022, February 21). *Surge in IoT during COVID-19 pandemic helps pave the way for new IoT laws*. Www.taylorwessing.com. https://www.taylorwessing.com/en/interface/2021/disruptive-tech-2021/surge-in-iot-during-covid-19-pandemic-helps-pave-the-way-for-new-iot-laws

Appendix

The survey questions were used to gain perspective on remote workers and the protocols their employers required as well as any experiences with COVID-related phishing scams. These are the questions that comprised my survey:

1. Do you primarily work from home?
2. Has your employer provided mandatory training/awareness raising on working securely from home? (Multiple answers)
3. Have you received any COVID-19-themed phishing scams while working from home?
4. Do you fall for phishing scams while working from home?
5. How has the number of phishing emails/spam emails/ fraudulent emails you receive at work changed since the COVID-19 crisis?
6. Overall, how has COVID-19 impacted your online shopping/buying behavior?
7. How much do you rely on IoT devices since pandemic?