Mitigation of Cyber Security Risk Threats During the Covid-19 Pandemic

Author Notification
09 October 2023
Final Revised
29 October 2023
Published
31 October 2023

Kemian Dai[1], Ichell Laurant Kawaki[2], Lintang Dwi Sakti[3]

International Islamic University Malaysia[1], Semarang University[2,3]
Jln Gombak, 53100 Kuala Lumpur, Selangor[1], Jl. Soekarno Hatta, RT.7/RW.7, Tlogosari Kulon, Kec. Pedurungan, Semarang City, Central Java 50196[2,3]
Malaysia[1], Indonesia[2,3]
e-mail: kkrmiandain132@gmail.com[1] , C111200034@student.usm.ac.id[2] , C111200037@student.usm.ac.id[3]

To cite this document:
Dai, K., Kawaki, I. L. ., & Sakti, L. D. . (2023). Mitigation of Cyber Security Risk Threats During the Covid-19 Pandemic. International Journal of Cyber and IT Service Management, 3(2), 107–119. *Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/135*

DOI:
https://doi.org/10.34306/ijcitsm.v3i2.135

Abstract

Cyber security mitigation is becoming an increasingly urgent aspect in today's digital era, in response to the threat of theft and disruption to information systems, software and hardware. The Covid-19 pandemic has exacerbated this situation by increasing the chances of success of cyberattacks, as the number and scope of such attacks increases. The impact of increasing levels of cyberattacks is the wider disruption to various sectors. This study aims to investigate cybersecurity issues that arose during the Covid-19 pandemic. Researchers analyzed the current conditions as well as cybercrime acts and various types of cyberattacks carried out during this period. In addition, this research also proposes a practical approach to mitigating the risk of cyber attacks that can be implemented by organizations. It is important for organizations to strengthen the protection of their data and critical assets by implementing a comprehensive cybersecurity approach. The results of this study present various techniques for detecting and avoiding cybercrime threats, even after the pandemic is over. By implementing this approach, damage caused by cyber attacks can be minimized, maintaining the integrity of an organization's data and systems. For future research, it is necessary to carry out further development in the field of cyber security by integrating the latest technologies such as artificial intelligence, blockchain, Internet of Things, and other technologies. In this way, efforts to mitigate cyber attacks can continue to be improved, maintaining the integrity and security of information systems in this ever-growing digital era. This research makes an important contribution to understanding and addressing cyber security issues during the pandemic and provides a foundation for further development in the future.

Keywords*: Cybersecurity, Cyberattacks, Covid-19 Pandemic, Mitigation, Technology*

1. Introduction

Almost the whole world is currently being hit by one of the biggest disease outbreaks of this century [1]. The Covid-19 outbreak which was declared a pandemic by the World Health Organization or WHO has affected the lives of individuals, organizations and the wider community [2]. The corona virus outbreak has had and is still impacting all industries, including the use of information and communication technology [3]. As a result of this crisis, many employees now rely on cell phones, laptops and internet access to work remotely from home. In addition, most of the business is now conducted online to reduce physical interaction. The health sector is not left behind with the increase in teleconsultation and remote management. Most schools have gone digital to ensure learning is uninterrupted. All of these conditions have led to a sudden increase in the use of internet technology and indirectly increased cybercrime.

Security is not just a “set and forget” type of problem, effective security involves thorough analysis, implementation, updating and monitoring. Cybercriminals have exploited the opportunity to attack individuals and organizations to commit numerous crimes using a variety of techniques. This research provides an overview of various computer security threats that were made during the COVID-19 pandemic and provides analysis and solutions related to computer security [4]. Solutions are made with several techniques to detect and avoid this threat even after the pandemic is recommended so that the damage caused by cyber computer crimes can be reduced [5].

The COVID-19 pandemic has created uncertainty, anxiety and drastic changes regarding our lifestyle. Organizations must adapt to the demand for remote work with speed and scale. Many were forced to change their physical offices and frantically created policies to allow employees to work from home without the necessary training or properly prepared setup [6]. Most of these companies and institutions had no plans in place to facilitate this drastic and sudden change in a short period of time [7]. In fact, only 38% of businesses have a cybersecurity policy [8]. By moving to an online environment, organizations and enterprises around the world have implemented work-from-home (WFH) business models that increase attack vectors and risks to internal data [9]. It is worth noting that WFH has become the new normal for people across the world [10]. In most scenarios, this implies a requirement for employees to use their own personal devices and home networks, most of which are insecure by nature and lack the necessary industry security standards [11]. There are many factors that threaten computer network security, which can be divided into subjective factors and objective factors [12]. For institutions that already provide business tools for their employees, this is usually guaranteed with minimal or no administrative rights. Instead, the common arrangement where staff are given temporary rights to install required software is problematic. Hence, businesses need to provide more realistic solutions and give employees more rights, which indirectly implies more potential security issues. Cybersecurity during the coronavirus disease 2019 (Covid-19) pandemic is a matter of true concern due to the emergence of cyber threats and security incidents targeting vulnerable people and systems globally [13]. This research focuses on cyber security mitigation that emerged in various environments during the pandemic. Therefore, it is very challenging for organizations to develop cyber security mitigation measures.

2. Research Method

This research has the main objective of investigating cybersecurity issues that have arisen during the Covid-19 pandemic and developing effective mitigation strategies in response to these threats. In the following explanation, we will detail the steps of the research method used in this study.

The first step in this research method is the identification of cybersecurity threats that may be faced by organizations during the Covid-19 pandemic. It includes in-depth analysis of various types of threats, such as phishing attacks, malware, ransomware, DDoS attacks and other cybersecurity threats that can compromise information systems, software and hardware.

After threat identification, we proceed by conducting a comprehensive risk analysis. We evaluate the level of risk associated with each threat, considering potential system vulnerabilities, data that may be targeted, and the financial and operational impact on the organization. This risk analysis is the basis for developing mitigation strategies.

Data collection is the next step in our research method. We collect data related to cyber attacks that occurred during the Covid-19 pandemic, including the type of attack, the origin of the attack, the target of the attack, the method used by the attacker, and the impact caused by the attack.

Based on the results of risk analysis and collected data, we develop mitigation strategies that are tailored to the needs and characteristics of the organization. This strategy includes concrete steps to reduce the risk of cyberattacks, such as implementing security software, changing security policies, and other relevant countermeasures.

Next, we implemented security measures that had been designed as part of the mitigation strategy. Implementation of these measures includes the use of the latest technologies, such as artificial intelligence, blockchain, or the Internet of Things, according to the needs and resources of the organization.

To ensure the effectiveness of mitigation strategies, we conduct regular testing and evaluation. This can include simulating cyber attacks to measure the security system's ability to protect the organization from threats. The results of this evaluation help us identify areas that require improvement and refinement in mitigation strategies. During this research, we also developed practical guidelines that other organizations can use to reduce the risk of cyberattacks during a pandemic or similar situation. This guide covers steps to follow, resources needed, and actions to take against cybersecurity threats.

The results of this research are documented in a research report that presents research findings, successful mitigation strategies, and recommendations for other organizations potentially facing similar threats. This report will be an important guide in understanding and addressing cybersecurity issues during the pandemic.

Additionally, we share these research findings with the cybersecurity community through scientific publications, conferences or webinars. It aims to contribute to a common understanding and solution to cyber security threats during the Covid-19 pandemic.

As a final step, we are planning further development in the field of cybersecurity by integrating the latest technologies such as artificial intelligence, blockchain, Internet of Things and other technologies. This will enable us to continuously improve our cyber-attack mitigation efforts, maintaining the integrity and security of information systems in the ever-evolving digital era. This research method is an important contribution to understanding and addressing cybersecurity issues during the Covid-19 pandemic and provides a basis for further development in the future.

2.1 Literature Review

With the widespread adoption of digital technology, many aspects of society have moved online, from shopping and social interactions to business, industry, and unfortunately, also crime [14]. Due to its profitable nature and low level of risk as cybercriminals can launch attacks from anywhere around the world, it is clear that cybercrime is here to stay [15].

Cybercrime, as a traditional crime, is often described with the crime triangle, which specifies that for cybercrime to occur, three factors must be present: victim, motive and opportunity [16]. The victim is the target of the attack, the motive is the aspect that drives the criminal to carry out the attack, and the opportunity is the opportunity to commit the crime, for example, it can be an inherent vulnerability in an unprotected system or device [17].

It is clear then that attackers are seeking to take advantage of the disruption caused by the pandemic, especially considering that disruption continues [18]. This guidance is critical to mitigating the growing threat, but to solidify the basics, there first needs to be a core understanding of the cyberattack being launched [19]. Even under normal circumstances, online crimes such as fraud provide better results with the least risk to attackers. Given these facts, more and more people are unemployed, spending more time at home and using the Internet for work and socializing [20].

In addition, the government has provided incentives to help people financially as well as other businesses to try to attract or retain customers. As the world anticipates the potential of drugs to control the spread of Covid-19, all information related to Covid-19 will attract public attention. Scammers take advantage of this method to send malicious [phi, smi, vi] shing3 attacks on victims posing as governments, tax authorities. With a link to claim assistance related to Covid-19.

This scam is much more effective now during a pandemic as most of the vulnerable people are more anxious and expect Covid-19 related emails, texts, calls from the authorities. As cybercriminals become more aware of the situation, it is much easier for them to create fake messages or websites that imitate the appearance of relevant and familiar authorities, including words that use urgency to exploit the fear factor felt globally due to the importance of addressing. emergencies and needs. Therefore, cybercriminals can increase the effectiveness of their phishing attacks. These attacks can come in many forms, such as internal and external updates, personal gain, and charity. It's worth mentioning that criminals can use the original material available as bait to encourage people to take risky actions such as clicking on links or opening attachments. It is important for users to look at the sender of the email and check for any links contained in it before acting. Cybercriminals often use impersonation techniques that impersonate the World Health Organization (WHO), United Nations (UN) or popular companies while the people are WFH, Zoom, to trick users into clicking links or opening infected documents [21].

As a result of the pandemic, we have seen complete lockdowns in almost all parts of the world. The shift to a new way of working where employees work from home primarily using their home systems secured by their employer has created a level of concern within the sector. Thanks to these mass quarantine arrangements, new challenges relating to the resilience of technological solutions for large parts of the ecosystem become important; in particular, the resilience of current technologies within the employer's existing cyberinfrastructure [22].

2.1.1 Cyber Attacks During the Covid-19 Pandemic

Cyberattacks during the pandemic can be categorized into three categories: fraud and phishing, malware, and distributed denial of service (DDoS). Specific examples of cyber attacks during the pandemic [23]. In March 2020, the Brno University Hospital as one of the COVID-19 testing laboratories in the Czech Republic was hit by a cyber attack in the form of ransomware and forced the entire IT network to be closed [24]. In June 2020 in Germany there was a phishing email attack on senior executives at companies supplying individuals with personal protective equipment (PPE) [16]. Phishing links have been designed to direct executives to fake Microsoft login pages to steal their credentials. Cybercriminals and Advanced Persistent Threats (APT) groups are launching cyberattacks on vulnerable people and organizations through Covid-19 related scams and phishing. They exploit the pandemic for various motivations, for example for commercial gain or to collect information related to the Covid-19 vaccine by applying various techniques such as phishing or ransomware and other malware. Examples of APT activity during the pandemic include Hades, Patchwork (aka Dropping Elephant, APT-C-09), TA5058, and APT299.

Scams and Phishing: The most common and effective attacks during this pandemic have been through various types of scams and phishing. In fact, phishing attacks have a success rate of 30% or higher. It is troubling that attackers only need a small percentage of clicks to gain financial or other interests. Therefore, sending millions of emails to victims who wish to apply for government-provided financial assistance, will result in fast and huge rewards. There are various phishing attacks (email, SMS, voice) targeting vulnerable people and systems using coronavirus or COVID-19 as a headline to lure people. There was a 600% increase in phishing email attacks related to the coronavirus in Q1 2020 [25]. Cybercriminals are also using more sophisticated techniques to lure victims such as using the HTTPS encryption protocol on their websites. In fact, about 75% of phishing sites are equipped with SSL [26]. Additionally, webmail and Software-as-a-Service (SaaS) users are the most targeted phishing sectors.

Malware includes computer viruses, worms, Trojan horses, spyware, and ransomware. During the pandemic, cybercriminals and APT groups have taken advantage of targeting vulnerable people and systems by spreading various types of malware via emails and websites [23]. In fact, 94% of computers damaged by malware have been infected by email [20].

3. Findings

The results of this research reveal a number of significant findings in efforts to mitigate cyber security threats during the Covid-19 pandemic. First of all, our research confirms that threats to cybersecurity have increased significantly with the spread of the pandemic. There has been a sharp increase in the number and scope of cyberattacks, including phishing attacks targeting vulnerable users that are on the rise.

Furthermore, we were able to identify various types of cyberattacks that have been carried out during this pandemic. Phishing attacks remain one of the most common types of attacks, but ransomware attacks are also showing notable increases. These attacks are often targeted at the healthcare and public service sectors, threatening the integrity of patient data and critical services.

The importance of a comprehensive approach to cybersecurity is also emphasized in our research results. Organizations need to engage technical, policy and training elements to improve the protection of their data and critical assets. By implementing techniques such as regular software updates, use of advanced threat detection tools, and training employees on good security practices, the risk of cyberattacks can be minimized.

Another finding is that efforts to detect and avoid cybersecurity threats should not stop after the pandemic is over. We recommend using the latest technologies such as artificial intelligence, blockchain, and the Internet of Things to strengthen defenses against increasingly sophisticated cybersecurity threats.

This research provides a solid foundation for further development in the field of cybersecurity. We hope that our findings and recommendations will assist cybersecurity organizations and communities in their efforts to confront cybersecurity threats during and after the Covid-19 pandemic. In conclusion, this research makes an important contribution to understanding and handling cybersecurity issues during a pandemic and provides a basis for further development in the future in maintaining the integrity and security of information systems in the ever-evolving digital era.

3.1 Cyber Attack

Cybercrime incidents that have arisen from the Covid-19 pandemic pose a serious threat to the global safety and economy of the world's population, therefore understanding their mechanisms, as well as the spread and reach of these threats is essential. Many solutions have been proposed in the literature to analyze how events unfold ranging from formal definitions to systemic approaches that examine the nature of threats. Although this approach allows categorization of attacks, it often lacks the ability to map larger, distributed events such as those presented in this manuscript, where many events stem from pandemics, but are unrelated. For this purpose, temporal visualization was chosen, allowing to chart events without compromising the narrative. Additionally, this type of visualization is used throughout the cybersecurity domain to represent the resulting cyberattack.

Table 1. Examples of Cyber Attacks during the Pandemic

No	Attack Type	Country	Reference Information
1	Phishing	Amerika	Discusses the phenomenon of increasing phishing attacks that exploit the issue of COVID-19 or coronavirus. These phishing attacks include sending fake emails, fake websites, and fake text messages that try to trick individuals into clicking on malicious links, entering personal information, or downloading related malware [27].
2	Phishing, Malware, Financial Fraud	Filipina	Discusses how COVID-19 related email attacks have evolved and changed as the pandemic has spread. This email attack includes various tactics such as phishing and spreading malware by taking advantage of current issues around the COVID-19 pandemic. This attack seeks to exploit the public's fear and interest in news and information related to COVID-19 [28].
3	Hacking	Czech	Containing that this blog discloses new threat discoveries indicating that commercial surveillance software operators have seized on the COVID-19 pandemic as an opportunity to increase their spying activities. They have used a variety of methods to collect personal data and sensitive information from unsuspecting users, often using apparently useful masquerading software [29].
4	Phishing, Malware	Cina	It states that the threat group APT32 from Vietnam has carried out cyber attacks against the government of Wuhan and the Chinese Ministry of Emergency Management in espionage efforts

			related to COVID-19. This attack is part of a broader espionage activity aimed at acquiring information related to the COVID-19 pandemic and may also be related to political and security interests. Cyber threats like this show the importance of cyber security in protecting sensitive and important data related to global health crises such as the COVID-19 pandemic. The article describes APT32's efforts in carrying out these espionage operations and the critical role cybersecurity plays in countering such threats [30].

It is also important to note that cyberattacks may first be featured on this domain, before being highlighted by mainstream media outlets. With regard to the inclusion of news reports in attack tables and subsequent timelines, it must be acknowledged that these attacks are presented through a journalistic lens, and as such may have been written in an attempt to make headlines. Nevertheless, these reported cyberattacks still pose a real threat to the general public during the Covid-19 pandemic. The Timeline attempts to provide an overview of attacks that have occurred.

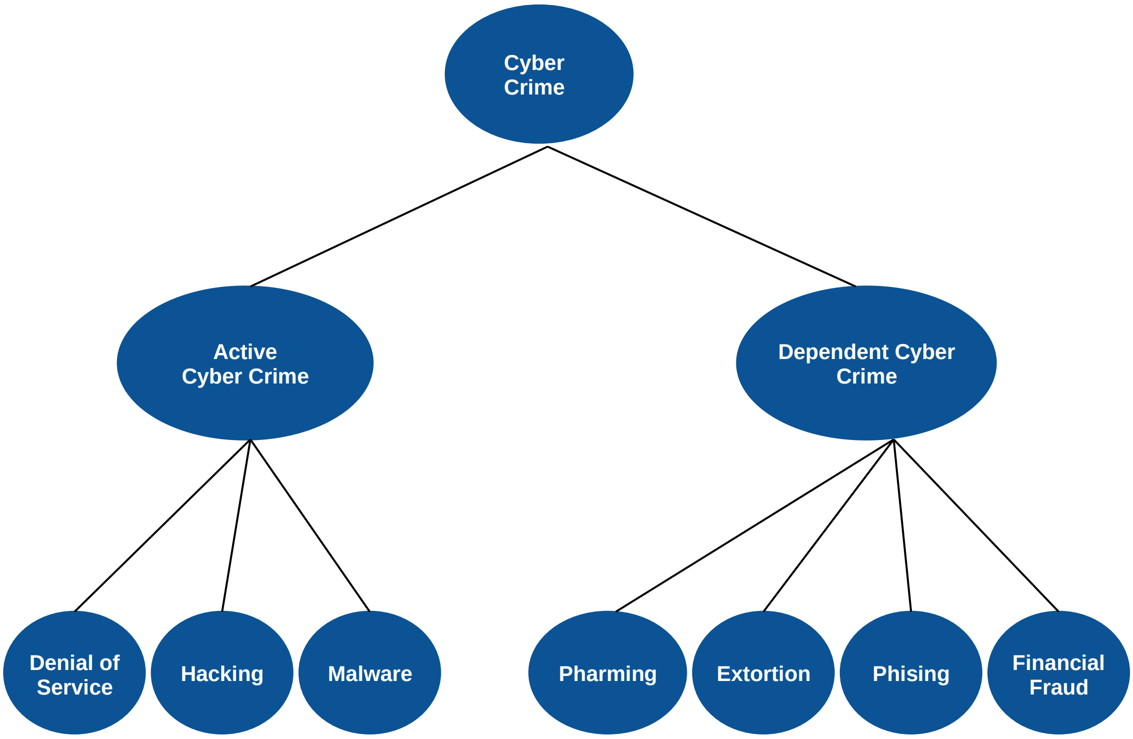

Figure 1. Dependent and Active Cyber Crime

This definition includes cybersecurity by default and has inspired many international definitions of cybercrime. Cyber-dependent crimes are offenses, "which can only be committed using computers, computer networks, or other forms of information and communication technology. These categories as well as examples of their subcategories can be seen in Figure 1. Some of the elements described by the CPS are often interrelated in cyberattacks.For example, phishing emails or text messages, for example SMS or WhatsApp can be used to lure victims to fraudulent websites.These websites can then collect personal data that is used to commit financial fraud, or may install malware, more specifically, ransomware that are then used to carry out extortion.Similarly Denial of Service (DoS) attacks are increasingly being used by cybercriminals to divert business during hacking attempts.In the following, it is worth considering these types of attacks and reflecting on how they are launched, including human factors or technical aspects (e.g. , vulnerabilities) that they are trying to exploit.

Phishing, or Social Engineering more broadly, includes attempts by unauthorized parties to convince individuals to take action, for example, sharing information or visiting a website under the pretense that they are engaging with a legitimate party. Quite often email messages are used, sometimes SMS or WhatsApp messages are used often referred to as smishing. Pharming is similar to phishing, but instead of tricking users into visiting malicious sites, attackers rely on compromising systems, such as users' devices or DNS servers to direct individuals to illegitimate sites. This type of attack is less common in general, as it requires more access or technical skills. Financial fraud generally involves defrauding individuals or organizations by using technology for financial gain for attackers or criminals.

Extortion refers to the act of coercing, threatening, or forcing an individual to perform some action, most commonly, spending money. Hacking, Malware, and Denial of Service (DoS) attacks are forms of crime often favored by more technical attackers. Hacking involves compromising confidentiality or system integrity, and requires reasonable skill; the technique may involve exploiting a system's vulnerabilities to compromise the system.

Malware refers to malicious software and can be used to disrupt services, extract data and various other attacks. Ransomware is one of the most common types of malware today, and combines malware with attempted extortion. DoS attacks the availability of a target system and works by flooding key services with unauthorized requests. The goal here is to use the bandwidth used for legitimate server requests, and ultimately force the server offline.

These types of attacks provide the basis for our analysis in timeline and how we approach our discussion in the next section of this research. Table 1 explains a number of cyber attacks. Cyberattacks have been organized by attack date. If the date of attack is not provided in the reference, then the date of the article has been used. The target countries of each cyberattack have been listed, along with a brief description of the methods involved.

Figure 2 provides a summary of countries targeted by cyberattacks early during the pandemic, organized by date of attack. As shown, China and the US accounted for 39% of the reported attacks. To further increase the chances of successful phishing attacks, cybercriminals have been identified as registering a large number of website domains containing the words 'covid' and 'coronavirus'. Such a domain is likely to be trustworthy, and therefore accessible, especially when paired with prominent words such as WHO or Centers for Disease Control and Prevention or keywords, for example, Corona-virusapps.com, anticovid19-pharmacy.com, which has been highlighted as used. Communication platforms, such as Zoom, Microsoft and Google, have also been impersonated, both via email and domain names.

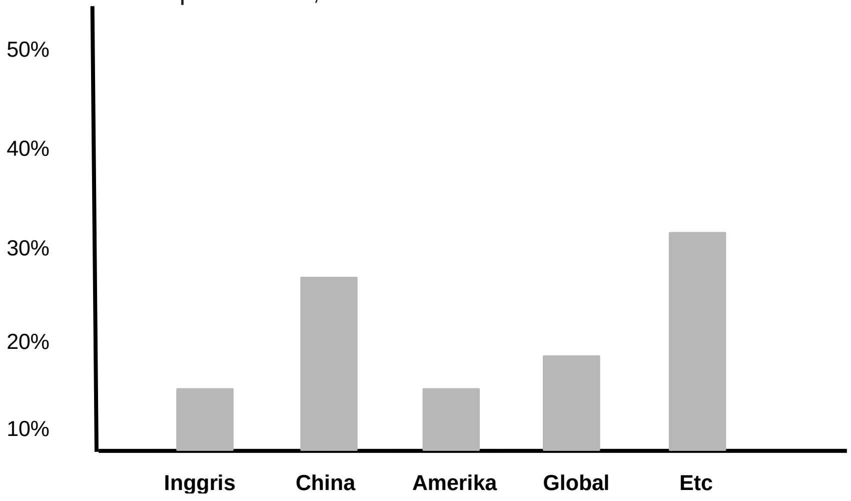

Figure 2. Distribution of Cyber Attacks Across Countries

This is noteworthy given the fact that it is the primary technology used by millions of people around the world to communicate, whether for work or pleasure. These facts, combined with convincing psychological manipulation emails, text messages and links, provide several important avenues for criminals to attack. Pharming attacks are much less common but occur in 13% of cases. As can be seen in Table 1, these attacks often occur together with other attacks

Covid-19 inspired scams have taken advantage of government/scientific announcements to exploit user anxiety and seek financial gain. From the analysis results, fraud is usually carried out through phishing and email attacks can also see this in our order above. In one case, criminals disguised themselves in emails and politely asked for donations to develop a vaccine, as well as any payments made in Bitcoin[30]. Commonly used phishing techniques, but on this occasion included requests for money: “Funding for the above project costs quite a bit and we are kindly asking for your good will to donate, nothing is too small”.

The important point about this particular attack is that it also asks the recipient to share the message with as many people as possible. This is worrying because people are more likely to trust emails that they believe have been checked by someone close to them.

There are various other attempts at fraud, most of which are based on threats or appeals. For example, our analysis identified investment offers in companies that claim to prevent, detect, or cure Covid-19, and investments in trading schemes/options that allow users to take advantage of possible Covid-19 driven economic downturns. Blackmail attacks were witnessed in our analysis but were less prevalent (occurring in only 13% of cases) than the others above. The most prominent case of this attack is an extortion email that threatens to infect recipients and their family members with Covid-19 unless Bitcoin payments are made. To increase the trustworthiness of the message, it includes the individual's name and one of their passwords (possibly gleaned from a previous password breach). After demanding money, the message went on to read: "If I don't get payment, I will infect every member of your family with the coronavirus." It attempts to use fear to motivate individuals to pay, and uses ciphers (i.e., items that are private) to build trust in criminal messages.

Malware related to Covid-19 has become more prominent during the pandemic and is affecting individuals and organizations around the world. Remaining malware attacks are variants of existing malware, in particular, are important threats and an example is COVIDLock, an Android application disguised as a heat map that acts as ransomware; basically locks the user's screen unless a ransom is paid.

At the organizational level, ransomware has had a significant impact on healthcare services—arguably the most fragile component of a country's critical national infrastructure today. Attacks have been reported in the United States, France, Spain and the Czech Republic, and use ransomware such as Netwalker. Such attacks fit a criminal modus operandi if we assume that criminals will target areas they believe will be leveraged to capitalize on their attacks; that is, healthcare organizations may be more inclined to pay a ransom to avoid the loss of a patient's life. Interestingly, since there have been promises from leading cybercrime gangs that they will not (or stop) targeting health services. In one report, it stressed that it would not normally target hospitals, or that it would temporarily halt all activities on health services until the virus stabilized.

Another well-known example of malware during the pandemic: Corona Live 1.1, an application that leverages the official COVID-19 tracker released by John Hopkins University and accesses device photos, videos, location data, and cameras [38]. As the pandemic continues, there will likely be more types of malware, targeting different types of harm, for example, physical, financial, psychological, reputational (for businesses) and social.

Advanced Persistent Threat (APT) —some of which may be aligned with the state identified as targets of pharmaceutical companies, medical research organizations and universities involved in the Covid-19 response. The goal is not always to disrupt their activities (as is the case with ransomware), but to steal sensitive research data or intellectual property (e.g. about vaccines, treatments).

While a detailed analysis of these attacks has not yet emerged, password spraying (a brute-force attack that applies commonly used passwords in trying to log into an account) and exploiting vulnerabilities in Virtual Private Networks (VPN) have been flagged.

3.2 Risk Mitigation

Mitigating and preventing cyber attacks is not a trivial task. There are practical approaches that can reduce the risk of cyberattacks during WFH. User Education: Security is only as strong as its weakest link. People are considered the weakest link in many security systems. Therefore, developing cyber security awareness among users through continuous training is important to reduce the risk of cyber attacks on an organization. A recent study shows that only 11% of businesses provide cybersecurity.

Virtual PrivateNetwork (VPN): A VPN is an encrypted communication channel between two points on the Internet to protect the data sent and received. Using VPNs to browse the Internet is the new normal. VPNs provide two aspects of security: confidentiality and integrity and allow organizations to extend security policies to remote workers.

Enable multi-factor authentication (MFA): MFA strengthens security by requiring a username and password plus a one-time code sent to the phone via SMS or an authentication app. MFA is an important factor in reducing guesswork and password theft such as brute force cyber attacks. An employee trying to access his company's network from home must provide a username and password and have a one-time code sent to his cell phone to verify his identity before being allowed to access the internal network.

Ensure all device firmware is up to date: Ensure that all devices and device/OS firmware is up to date with the latest security enhancements applied to isolate them against known vulnerabilities. Ensuring that the latest anti-malware software is enabled on all devices connected to the network: Cybercriminals target vulnerable people by spreading various types of malware. Since millions of new malware and its types are generated every year, regular and up-to-date anti-malware can reduce the risk of cyberattacks caused by malware.

Enable strong company online policies: Organizations have little or no time to prepare for WFH scenarios. A robust and comprehensive WFH policy is needed to protect data and prevent cyberattacks. A strong WFH policy includes avoiding holding sensitive work conversations in public, using only company-approved video and audio conferencing channels, etc.

The policy should also include a robust, proven recovery plan and backup strategy. It's also important to test these plans regularly as a recent study highlighted that 46% of businesses only test their recovery and backup plans once a year or less.

Segmentation and unbundling: Moving away from “all-in-one” single-purpose devices and networks. Divide the network into trusted zones: home office network (high level of trust), home and guest entertainment networks (low level of trust) and Internet zone (untrusted). In a smart home, IoT devices must be isolated in a separate Wi-Fi network. By isolating the IoT device on a separate network segment, any intrusion of the IoT device will not automatically grant access to the user's primary device such as a corporate laptop.

Physical office/home security: It is important to physically protect home office devices. Practical approaches include ensuring that work devices are not left unattended, using a lock screen or locking the laptop, always logging off devices after use, etc.

Security updates: It is important to ensure that all systems and endpoints are updated and patched regularly, for example to ensure that the latest anti-malware software is enabled on all devices and endpoints connected to the network. An important risk that needs to be examined is the security risk.

In addition to the general mitigation approaches discussed above, examples of healthcare-related security risk mitigation are outlined below. During the pandemic, healthcare organizations dealing with COVID-19 have become prime targets for persistent cyberattacks. Healthcare organizations must protect their valuable data and assets from cyberattacks by improving their defenses. Two critical components in detecting malicious behavior that can compromise network security and trust are intrusion detection systems (IDS) and security incident and event management (SIEM).

Typically, IDSs use anomaly detection, stateful protocol analysis (aka deep packet inspection), signature matching, or a combination of all three techniques (hybrid) to analyze incoming cyber attacks. Due to its ability to more accurately detect zero-day attacks, Artificial Intelligence-based anomaly detection IDS are gaining popularity for detecting cyberattacks. Additionally, it is important for healthcare organizations to take a comprehensive approach to cybersecurity and not look at security from a technological perspective alone, but within a process framework. Examples of comprehensive approaches to cybersecurity include the CERT Resilience Management Model (CERT-RMM), risk management, and incorporating cybersecurity into strategic planning and budgeting processes.

Organizations need to reprioritize their cybersecurity strategy and take action to enhance cyber defense. Instead of focusing too much on critical business processes that may require immediate attention, organizations should also prioritize cyber risks to ensure that they can lead a resilient business into the future, once the chaos of the pandemic has been resolved.

Organizations can consider several steps to build their cybersecurity and overcome the short-term and long-term challenges mentioned above. Companies should strengthen threat intelligence programs and integrate them with other critical activities, such as monitoring security incidents. Organizations must also ensure active vulnerability discovery and threat hunting. Additionally, it is important for organizations to maintain proactive communications with employees and third parties to raise awareness about cyberthreats and ensure prevention of such threats. Engage the workforce about the security implications of working from home by explaining and educating them about best practices regarding remote work, such as sharing files securely, connecting to corporate networks through VPNs, and using secure passwords. To facilitate these best practices, organizations should ensure secure remote access by reviewing the security posture of VPN governance and use of multi-factor authentication. Organizations should also update their security incident response playbook and generate after-action reports. Documenting response activities taken in this pandemic crisis, including gaps identified and areas for improvement can yield useful insights and lessons for future situations.

Finally, organizations should strengthen security in high-risk areas, for example by updating their security architecture and ensuring protection from insider threats and cyber testing. Additionally, organizations should consider accelerating the implementation and optimization of critical security solutions, such as multi-factor authentication or mobile device management, especially for high-risk connectivity applications or platforms. What if your system remains compromised? If the cyberattack is successful, regardless of all security measures taken, organizations must follow a step-by-step approach to recovering their critical business operations. First of all, the lock system needs to be isolated for protection. Second, organizations need to fully understand and contain the incident, and consequently, eliminate any malware. Thereafter, appropriate protective measures must be implemented to improve overall system posture, and identify and prioritize recovery of key business processes to deliver operations. Finally, the hospital must implement a prioritized recovery plan.

Technology is advancing rapidly and with it comes an increase in cyberattacks and an increase in the frequency of malicious attacks. We suggest a unique solution where we use advanced technology of artificial intelligence to detect and prevent threats before they start to root themselves in the computer system.

The artificial intelligence program will act primarily to scan, verify, and raise alerts of suspicious packages coming into the system. We can think of this like an advanced defender or firewall program. A secondary task will also be to scan and review the files currently stored on the computer system and raise alerts for them.

The implementation of artificial intelligence collects data from servers that communicate with it to see common patterns or attacks on the system. Therefore, in two parts, the program will act to filter all files and data, whether they are harmful, disable, auto-delete or cut their access to the computer system unless otherwise agreed by the user. The artificial intelligence system will take advantage of its machine learning capabilities such that when a user rules out a potential threat as malicious, the program will learn the pattern and send the data to a server where it will store the pattern.

All other computer systems that use this program will be able to refer to the patterns stored on the server. Using patterns in the algorithm will make it easier to detect system vulnerabilities. Increasing the accuracy of the prediction algorithm will affect the accuracy of the system in predicting recommendations to users[46]. This will ensure that the system learns about these attacks and can prevent them efficiently before they start.

These solutions, as previously stated, rely on sophisticated and advanced technology to do the toughest jobs. While the system will be used passively and actively in runtime, use more resources than usual, and may cause frustration at first, this solution is built to exist effectively in the long term by growing stronger and smarter as time passes.

The more data it collects, the more certain the program automatically eliminates and interrupts attacks before they cause damage to computer systems. This, in its smallest form will be very effective on stand-alone devices but works better on servers as more data will be loaded. This is especially valuable for companies like Google that value the security of their data and that of users highly. It can also work very well for small and large businesses. In addition, the current COVID-19 pandemic, where attacks are more frequent, can speed up the program's machine learning process, making it very effective quickly.

This program has the potential to eliminate the problem of having to do a lot of manual user work with firewalls or security programs as if the program is confident enough, it will execute the directives automatically. The program can also detect fraud and phishing attempts when receiving email data. It will alert and warn users about potential scams and with reasons. The system also sidesteps the problem of having security bugs and backdoors in the software because it learns progressively and automatically “patches” itself. Lastly, it will also detect malware implanted into the system and attempt to eliminate it before it causes greater damage.

These solutions, as previously stated, rely on sophisticated and advanced technology to do the toughest jobs. While the system will be used passively and actively in runtime, use more resources than usual, and may cause frustration at first, this solution is built to exist effectively in the long term by growing stronger and smarter over time. passed. The more data it collects, the more confident the program is in automatically eliminating and disrupting attacks before they cause damage to a computer system. This, in its smallest form will be very effective on stand-alone devices but works better on servers as more data will be loaded. This is especially valuable for companies like Google that value the security of their data and that of users highly. It can also work very well for small and large businesses. In addition, the current COVID-19 pandemic, where attacks are more frequent, can speed up the program's machine learning process, making it very effective quickly.

This program has the potential to eliminate the problem of having to do a lot of manual user work with firewalls or security programs as if the program is confident enough, it will execute the directives automatically. The program can also detect fraud and phishing attempts when receiving email data. It will alert and warn users about potential scams and with reasons. The system also sidesteps the problem of having security bugs and backdoors in the software because it learns progressively and automatically “patches” itself. Lastly, it will also detect malware implanted into the system and attempt to eliminate it before it causes greater damage. Spreading awareness about the importance of cybersecurity should be a top priority. It is better to educate people about cyber security, common cyber threats and prevention. As they say, prevention is better than cure.

If given the task of spreading awareness about cybersecurity, we will use several methods. First, we must take advantage of social media advertising. Surprisingly, most internet users are not aware of the dangers of using the internet. Advertising on these platforms, such as Facebook and Instagram, has been known to subtly influence social media users. Therefore, by using this psychological aspect, we can increase awareness or instill conscious thinking about cyber security. It aims not to instill fear of cyberattacks but to combat them using simple but effective prevention methods. Additionally, when it comes to the company and business side, employees should attend seminars related to cyber security to become aware of the common tactics and methods of fraudsters. This will also help employees who are not in IT to detect hacking attempts or attacks on their workstations if they occur. In the long run, the cost of sending employees to seminars will be a small amount compared to the amount of money saved from recovering from attacks and fraud in the company's prospects.

4. Conclusion

The Covid-19 pandemic has created extraordinary and unique social and economic circumstances that are being exploited by cybercriminals. Analyzes of events such as announcements and media stories have shown what appears to be a loose correlation between announcements and related cyberattack campaigns that leverage the event as a hook and thereby increase the likelihood of success.

The Covid-19 pandemic, and the increased level of cyberattacks it has caused, has broader implications, beyond such targets. Changes to work practices and socialization mean people are now spending more and more time online. On top of that, unemployment rates are also rising, which means more people are sitting at home online—it's likely that some of these people are turning to cybercrime to support themselves. The research that has been carried out provides opportunities for further research.

This research has demonstrated what could be described as a loose direct and inverse view between events and cyberattacks. Further research needs to be prepared for this phenomenon and determine whether predictive models can be used to regulate this relationship. In the future, cyber security will be developed with the integration of the latest technologies, such as Artificial Intelligence, Blockchain, Internet of Things, and many more. As for the current situation, every user should start taking small steps to protect your personal data before it is compromised by unauthorized users.

References

[1] I. Chakraborty and P. Maity, "COVID-19 outbreak: Migration, effects on society, global environment and prevention," *Sci. Total Environ.*, vol. 728, p. 138882, 2020.

[2] L. Kuznetsova, "Covid-19: The world community expects the World Health Organization to play a stronger leadership and coordination role in pandemics control," *Front. Public Heal.*, vol. 8, p. 470, 2020.

[3] F. Alfiana *et al.*, "Apply the Search Engine Optimization (SEO) Method to determine Website Ranking on Search Engines," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 65–73, 2023.

[4] W. He, Z. J. Zhang, and W. Li, "Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic," *Int. J. Inf. Manage.*, vol. 57, p. 102287, 2021.

[5] K. Kano and E. Dolan, "Data Compression Analysis of Multimedia Video on Demand and DEMAND TV Broadcast Systems on the Network," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 48–53, 2023.

[6] S. W. Ross *et al.*, "Maximizing the calm before the storm: tiered surgical response plan for novel coronavirus (COVID-19)," *J. Am. Coll. Surg.*, vol. 230, no. 6, pp. 1080–1091, 2020.

[7] N. Donthu and A. Gustafsson, "Effects of COVID-19 on business and research," *Journal of business research*, vol. 117. Elsevier, pp. 284–289, 2020.

[8] L. K. Choi, K. B. Rii, and H. W. Park, "K-Means and J48 Algorithms to Categorize Student Research Abstracts," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 61–64, 2023.

[9] R. Klint, "Cybersecurity in home-office environments: An examination of security best practices post Covid." 2023.

[10] A. Eiji and S. Mehta, "Simulation-Based 5G Femtocell Network System Performance Analysis," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 74–78, 2023.

[11] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, 2020.

[12] D. Papatsaroucha, Y. Nikoloudakis, I. Kefaloukos, E. Pallis, and E. K. Markakis, "A survey on human and personality vulnerability assessment in cyber-security: Challenges, approaches, and open issues," *arXiv Prepr. arXiv2106.09986*, 2021.

[13] J. Chigada and R. Madzinga, "Cyberattacks and threats during COVID-19: A systematic literature review," *South African J. Inf. Manag.*, vol. 23, no. 1, pp. 1–11, 2021.

[14] C. Yegen, A. M. Kirik, and A. Çetinkaya, "Sustainability, Digital Security, and Cyber Hygiene During the Covid-19 Pandemic," in *New Normal in Digital Enterprises: Strategies for Sustainable Development*, Springer, 2023, pp. 91–105.

[15] B. Collier, R. Clayton, A. Hutchings, and D. Thomas, "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies," 2020.

[16] H. S. Lallie *et al.*, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” *Comput. Secur.*, vol. 105, p. 102248, 2021.

[17] S. R. Zahra, M. A. Chishti, A. I. Baba, and F. Wu, “Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system,” *Egypt. Informatics J.*, vol. 23, no. 2, pp. 197–214, 2022.

[18] D. Mustajab, A. Bauw, A. Rasyid, A. Irawan, M. A. Akbar, and M. A. Hamid, “Working from home phenomenon as an effort to prevent COVID-19 attacks and its impacts on work productivity,” *TIJAB (The Int. J. Appl. Business)*, vol. 4, no. 1, p. 13, 2020.

[19] M. Jbair, B. Ahmad, C. Maple, and R. Harrison, “Threat modelling for industrial cyber physical systems in the era of smart manufacturing,” *Comput. Ind.*, vol. 137, p. 103611, 2022.

[20] B. Pranggono and A. Arabo, “COVID-19 pandemic cybersecurity issues,” *Internet Technol. Lett.*, vol. 4, no. 2, p. e247, 2021.

[21] A. Minnaar, “‘Gone phishing’: the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals,” *Acta Criminol. African J. Criminol. Vict.*, vol. 33, no. 3, pp. 28–53, 2020.

[22] D. Gupta, S. Bhatt, M. Gupta, and A. S. Tosun, “Future smart connected communities to fight covid-19 outbreak,” *Internet of Things*, vol. 13, p. 100342, 2021.

[23] S. Hakak, W. Z. Khan, M. Imran, K.-K. R. Choo, and M. Shoaib, “Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies,” *Ieee Access*, vol. 8, pp. 124134–124144, 2020.

[24] J. Kolouch, T. Zahradnický, and A. Kučínský, “Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic,” *Masaryk Univ. J. Law Technol.*, vol. 15, no. 2, pp. 301–341, 2021.

[25] R. Goenka, M. Chawla, and N. Tiwari, “A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy,” *Int. J. Inf. Secur.*, pp. 1–30, 2023.

[26] R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Futur. internet*, vol. 12, no. 10, p. 168, 2020.

[27] A. F. Al-Qahtani and S. Cresci, “The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19,” *IET Inf. Secur.*, vol. 16, no. 5, pp. 324–345, 2022.

[28] M. Bitaab *et al.*, “Scam pandemic: How attackers exploit public fear through phishing,” in *2020 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, 2020, pp. 1–10.

[29] P. Tulkarm, “A Survey of Social Engineering Attacks: Detection and Prevention Tools,” *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 18, 2021.

[30] N. Katagiri, “Explaining Cyberspace Dynamics in the COVID Era,” *Glob. Stud. Q.*, vol. 2, no. 3, p. ksac022, 2022.