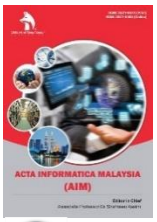
ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2521-0874 (Print)
ISSN: 2521-0505 (Online)
CODEN: AIMCCO

Acta Informatica Malaysia (AIM)

DOI: http://doi.org/10.26480/aim.01.2023.19.23



CrossMark

REVIEW ARTICLE

A REVIEW ON THE IMPACT OF CYBERSECURITY CRIMES IN FINANCIAL INSTITUTIONS DURING THE TIME OF COVID-19

Abthal Abdajabar, Nur Arzilawati Md Yunus

Faculty of Business and Technology, University of Cyberjaya, 63000 Cyberjaya, Selangor, Malaysia.
****Corresponding Author Email: abthal.abdajabar@gmail.com***

ARTICLE DETAILS

Article History:

Received 21 October 2022
Revised 01 November 2022
Accepted 06 December 2022
Available online 15 December 2022

ABSTRACT

The COVID-19 pandemic significantly impacts every aspect of our life, including how we connect with others in our professional and personal lives and how we structure our work in general. Quarantines and the deployment of social isolation measures caused an astronomical rise in cybersecurity offences in this region. As a result, using the risky Internet network to run every aspect of daily life necessitates complete and direct reliance on it, which increases the risk of cyberattacks, which increased in the financial sector during COVID-19. This paper analysed the cyber security crimes during the pandemic of COVID-19, highliting the different types of cybercrime that occurred worldwide. The mechanism of cybersecurity crimes campaigns was demonstrated by analysing and evaluating cyberattacks in the framework of worldwide events. The systematic review methodology was used in this paper to summarise, compare, and critically analyse the findings of about 60 researchers, articles, and numerous reports from government organisations, security companies, as well as the academic journals that looked into cybercrimes during COVID-19 or suggested solutions to combat them. The influence of the COVID pandemic on cybersecurity is also discussed in this study, with an emphasis on the financial sector and how cybercrimes increased compared to the period prior to the pandemic to a stage where four to five separate cyberattacks on particular days were reported.

KEYWORDS

COVID-19, Cybersecurity, Financial institutions, Cyberattacks.

1. INTRODUCTION

The COVID-19 epidemic has profoundly affected all aspects of our life, including how we conduct social and professional contacts and how our work is generally organised. Quarantines and the implementation of social segregation measures led to an extraordinary increase in crime in this area (WHO, 2020). Many workers had to quickly adjust to using online platforms, mobile applications, and new forms of communication in their daily work (WHO, 2020). People have to adapt to new lifestyle patterns brought on by these situations. As a result, operating every element of life requires complete and direct reliance on the usage of the dangerous Internet network (Khweiled et al., 2021). Numerous institutions, whether large or small, depend extensively on the use of information technology in their everyday operations, necessitating efficient information security methods to prevent hackers from stealing or attacking (Khweiled et al., 2021).

In the past several years, the global banking system has seen considerable changes in terms of processes, transactions, and operations, which technological advancements and recent trends have impacted. However, All financial institutions rely on external platforms to provide various digital services. In order to protect their customers, banks should evaluate cyber-attacks, the tactics they have put in place, and the level of knowledge both they and their customers have regarding cyber threats and security (Alaawi and Bassam,.2020). This paper describes COVID-19 impact towards Cybersecurity from a cyber-crime perspective. It highlights the range of cyber-attacks experienced globally during the pandemic, focusing on the impact on the financial institution and how cyber crimes rose compared to the time before the pandemic. This paper also presents a comparison of the results and surveys from earlier studies. This paper examines the studies, reports, and studies by government organisations, security companies, and the literature that looked into cybersecurity crimes during COVID-19 or suggested defences against them.

2. AN OVERVIEW OF THE IMPACT OF CYBERSECURITY

The United Nations and the World Health Organization warned that the COVID-19 pandemic was preceded by a similarly dangerous outbreak of frauds and deceptions (WHO). The term "infodemic" was coined to describe the misuse of online data. Additionally, the pandemic paved the way for the COVID-19 scamdemic, which led to an increase in a wide range of cyberattacks and cybersecurity problems. Phishing attacks were by far the most common during the scamdemic (Lallie et al., 2021). The phishing attempts that took place during the outbreak also included distinctive features designed to take advantage of COVID19's quirks and boost their probability of winning. The high quantity of phishing assaults, combined with their novel qualities, drew researchers attention and many studies (He et al., 2021). Due to the unusual effects caused by COVID-19, a great wave of research was conducted to contrast the numerous covid-induced cybersecurity problems. Several studies focused on cybercrime and cyberattack challenges that emerged during the pandemic are included in this new wave of analysis, especially in financial institutions; a few review publications supplemented original research in this area.

Here, in brief, we examine previous studies examining the connection between cyberattacks and COVID-19 focused on the financial institution and point out how they differ from our current study. The

Quick Response Code	Access this article online	
	Website: www.actainformaticamalaysia.com	**DOI:** 10.26480/aim.01.2023.19.23

Cite The Article: Abthal Abdajabar, Nur Arzilawati Md Yunus (2023). A Review on the Impact of Cybersecurity Crimes in Financial Institutions During the Time of Covid-19. *Acta Informatica Malaysia, 7(1): 19-23.*

global banking system has undergone significant shifts in terms of processes, money transfers, and operations over the past several years, as a result of technological advancements and current trends. Nevertheless, systemic operations and the advancement of information technology both have specific problems. All the financial institutions rely on external platforms to provide a variety of digital services. Consequently, they are at the risk of forces beyond their control. This has made hackers and criminals more cognizant of the risks and vulnerabilities in technology that might allow them to breach banking networks and steal sensitive data and funds. Due to the quick advancement of technology, cyber threats and attacks are difficult. In order to protect their customers, banks should evaluate cyber-attacks, the tactics they have put in place, and the level of knowledge both they and their customers have regarding cyber-threats and security (Alaawi and bassam, 2020).

2.1 Cyber Crimes Types

In this analysis, we look into the most common crime patterns that emerged during the COVID19 epidemic. After introducing the backdrop of COVID19 and highlighting the most notable anomalies of covidrelated cyber attacks, we provide a comprehensive literature analysis of the many studies that have looked into this topic.

2.1.1 Hacking

Scammers out for financial gain went on a hacking spree targeting users of mobile devices, desktop computers, and other devices connected to the internet. The result is the theft of confidential information like login credentials, financial data, and more. In some cases, hackers actually withdrew money from victims' accounts using the information they obtained. Similar to how bank loan scams proliferated quickly during the height of the COVID-19 situation, many of these schemes concentrated on stealing people's personal and financial information using online purchasing. As many stores were forced to close due to the pandemic, cybercriminals took advantage of the situation and increased cases of fraud by 42% compared to 2019. SMS alerts advising customers of one bank to reschedule a shipment delivery were reported by some of those customers.

2.1.2 Phishing

The simplest way for hackers to infect a smartphone with malware is still through phishing. Phishing tactics lure victims into opening emails or clicking on links that appear to be from reliable sources or legitimate companies. Attackers made the best of the circumstance by targeting a large number of people with phishing emails during the statewide lockdown brought on by the prevalent Coronavirus. False websites that can gather user information are part of phishing. Most people now rely on internet tools to deal with the situation, making them open to phishing attempts. A total of 4,67,825 phishing emails, or less than 2% of all phishing emails, were sent in March 2020, with 9,163 of those emails pertaining to COVID-19 (Naidoo, 2020).

2.1.3 Ransomware

Criminals create ransomware to prohibit users from using their systems unless a ransom is paid. In essence, ransomware, a type of cyber assault, locks a company out of its own IT infrastructure, which includes computers, networks, and other systems. Then, access to the environment and the data it houses are demanded as ransom. The information is occasionally sold to other internet criminals or made publicly available by the hackers, who seldom ever provide access back. Throughout the pandemic, ransomware assaults escalated as more individuals operated remotely (Chigada and Madzinga, 2021).

2.1.4 Malware

Malware refers to programs or code designed to damage computers by encrypting information, corrupting hardware, preventing software from operating properly, stealing data, or gaining unauthorized access to a computer. The pinnacle of COVID-19 came when malware was collecting data. In other words, it has turned into a time when hackers are using more data-harvesting tools including spyware, banking Trojans, info stealers, and Remote Access Trojan. Threat actors enter systems employing COVID-19-related content as an allure to breach networks, steal information, fraudulently move money online, and build botnets (Mukhopadhyay and Prajwal, 2021).

2.2 Cyber Threats to The Financial System in The World

The global world faces an increasing number of cyber risks to the financial system. In February 2017, hackers attempted to steal $1 billion from the central bank of Bangladesh by exploiting weaknesses in SWIFT, the primary electronic payment messaging system of the global banking system. Despite the fact that most transactions were banned, $101 million went. The crime served as a wake-up message to the banking industry that systemic cyber dangers had been grossly underestimated. Despite the growing reliance of the global financial system on digital infrastructure, it is not apparent who is in charge of guarding the system against cyber attacks. Due in part to how rapidly the environment is changing, this has happened. Without targeted action, as innovation, competition, and the pandemic expand, the digital revolution will only increase the vulnerability of the world financial system. Though many threat actors are merely seeking to make a buck, those who learn the ropes of theft get insight into the inner workings of the financial sector and are thus more equipped to launch disruptive or even destructive strikes in the future. There were many data breaches in the financial institutions all around the world, the cyber security issue comes in different type of crime. The compression of most cybersecurity crimes in the world is highlighted in Table 1.

Table 1: The Most Cybersecurity Crimes in The World

Authors	Year	Country	Cybersecurity/ crimes
Cybersecurity in the EU	2020	European Union	Cyber War, Cyber espionage, Cyber crime, Phishing, Online Fraud.
Computing, et al.,	2015	India	Phishing, cyberattacts, Spam email, Fical fraud
Malik and Islam,	2019	Pakistan	Cyber crimes, fraud
Smikle	2022	Jamaica	e-fraud, identity theft, credit card forging, Phishing
Butler Bank of England	2017	UK	Cyber crimes, extortion, blackmail, and fraud
SEC	2018	USA	cyber-risk, cyber crimes, Phishing.

In European Union countries, a successful cyber-attack on the banking industry might have disastrous implications, causing financial crises. The European Central Bank's (ECB) Executive Board member Benoît Coeuré noted in November 2018 that "the next financial crisis may start as a cyber-incident. in March, the Finance Ministers and Central Bank Governors underlined that the malicious use of ICT could disrupt national and international financial systems, weaken security and confidence, and jeopardise financial stability (Cœuré., 2018). The provision of liquidity by central banks and the execution of monetary policy may be threatened by the failure of wholesale payment networks. At the micro level, a major cyber attack could lead to the theft or loss of money and proprietary information, the alteration or loss of private company or client data, and the suspension of financial institution services.

Indirect expenses from a successful cyber-attack may include deteriorated customer relations, tarnished reputation, probable legal trouble, and regulatory repercussions (Bak, 2017). In India, the number of cybercrimes is increasing significantly. Cyber attacks frequently commit offences like social media, credit card fraud, phishing, virus, malware, denial of service, gambling, hacktivism, personal data breach, corporate data breach, and virtual currency. The majority of victims from different types of Indian banks suffer from financial loss and data loss. Since the internet is a vast source of information and a means of communication for people worldwide, using it safely requires taking some precautions (Computing, 2015). The effects of cybercrime occurrences on organisational performance are explored in Pakistan by employing a survey design on 302 employees in the country's banking sector.

This further explores the moderating effects of information security awareness. The study demonstrates that cybercrime occurrences negatively affect corporate performance, while information security awareness mitigates this effect.While Jamaica is still dealing with financial crimes, particularly in cyberspace, such as e-fraud, identity theft, credit card forgery, money laundering, and terrorist operations. Spoofing, spamming, virus spread, spear phishing, buffer overflow, and denial if service are just a few of the cybersecurity weaknesses that organisations in Jamaica are still vulnerable to. Because the illegal use of cyberspace could have a considerable influence on Jamaica's financial sector, cybersecurity is seen as a national policy issue (Smikle, 2022). Cyberattacks were listed as the second-most often reported source of risk to the UK financial system in the Bank of England's 2018 Systemic Risk Survey (Bank of England, 2018).

As a result, the Bank responded to a perceived systemic risk with a macroprudential policy. This has included using the CBEST test methodology to gauge the susceptibility of systemically important enterprises. According to a UK Finance and KPMG analysis from April 2018, when crime, extortion, blackmail, and fraud move online, cybercrime has a global impact reaching $450 billion a year. On the contrary, the SEC in the United States published guidelines on the disclosure of cyber risk for listed organizations in 2011, which was updated in 2018 to include further information on how and when businesses should alert investors (SEC, 2011; SEC, 2018). Nevertheless, it is possible to offer a structure for reporting cyber attacks, which might adequately meet the data gaps that now exist. Cyber risk is a significant concern for the financial sector in all nations. But some countries are more exposed to cyber attacks than others.

The International Telecommunications Unit (ITU), which is a part of the United Nations, gives the world a global cybersecurity index. Their index is based on a number of things, like legal, technical, and organisational arrangements, as well as building capacity and working together (ITU, 2017). Also, The map illustrates that practically all nations are represented. In nations like the Baltic states and Bangladesh that had been the target of cyberattacks, the rating is highest (Bouveret, 2018).

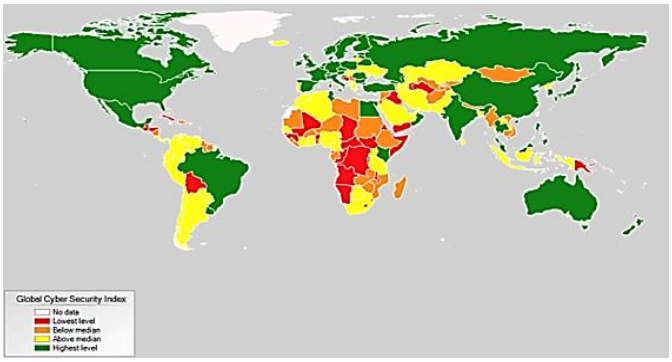


Figure 1: Cybersecurity around the world. Source: ITU (2017).

3. METHODOLOGY

A rapid systematic review is a process of generating a summary of knowledge in which its content is produced in a timely manner (Tricco et al., 2015). We, identifing the articles to fulfil the aims of the review, a literature search was conducted on the impact of cybersecurity. All searches were filtered to limit to the English language, articles published between 2018-2022, full text, articles that had abstracts, published articles or articles in the press, or review articles (these were used to inform but not for the final analysis), and no specific species. After the Cyber threats to the financial system in the world, analysing the highlighted the cybersecurity crimes in financial institutions in the world.

First, we defined the essential terms of the research, following the overview of the impact of cybersecurity, highlighting the common types of cyber crimes. Then, we discussed the impact of Covid-19 on cybersecurity by summarising the literature and concluded from an existing summary of several survey studies between the year 2020-2022. finally, compares the current study that impacts financial institutions in specific.

4. THE IMPACT OF COVID 19 ON CYBERSECURITY

Cybersecurity guards against unwanted access to and attacks on systems, networks, software, and data. Cybersecurity is a challenging research field due to the constantly changing nature of assaults. Understanding a few essential concepts, such as an attack, adversarial, risk, threat agent, threats, vulnerability, security policy and countermeasures, is crucial to understanding information flow in cybersecurity (Stallings and Brown, 2016). The COVID-19 epidemic has revealed how dependent society is on information technology and the importance of having a solid cybersecurity system to safeguard our technologies and the distant workers who rely on them. The COVID-19 outbreak has resulted in numerous cyber security crimes, which pose a significant risk to people's security and economic growth. That is why it is so essential to comprehend their mechanisms, spread, and impact. primarily when the pandemic produces several seemingly unrelated episodes.

Almost every nation on Earth has declared a state of emergency due to the spread of the Coronavirus, forcing its citizens to stay indoors and conduct most of their daily activities online. However, throughout the COVID-19 crisis, virtually every financial sector saw ongoing cybersecurity threats. (Furnell et al., 2021). Also, during the time of the panadmic E-learning resources have been used in higher education in various nations, such as the United Arab Emirates (UAE). For instance, UNESCO provided a range of resources for distance learning to help various institutions and organisations adjust to finish their work during the Covid period (UNESCO, 2020). Among others, WebEx, Zoom, Google Classroom, Ultra Collaborative, Skye and Respondus are popular tools used to deliver lectures. Through social media sites like WhatsApp, Telegram, YouTube, Facebook and others that provide online services that were used to promote education during the COVID-19 pandemic crisis, academic and nonacademic professionals as well as students frequently contact with one another.

Moreover, Zoom transformed from a little company to one of the most well-known and often used video and audio conferencing systems practically overnight as a result of the swift rise in people working from home as a result of COVID-19. Its revenue increased 3.55 times from Q2 of 2019 to Q2 of 2020. Zoom experienced numerous security incidents as a result of its quick growth, a most remarkable of these being the selling of more than 500,000 registered users on a dark web forum. Credential spamming, a method for gaining access to accounts, is said to have been used to leverage usernames and passwords that were already revealed in prior breaches (Alawida et al., 2022).

4.1 Existing Work Survey Comparision

Table 2: The Summary of The Existing Surveys.

Study	Year	Cybersecurity relates	Relate/not Relate to Covid
Hijji & Alam	2021	social engineering-based cyber-attacks	During Covid
Lallie et al.	2021	cyber-crime perspective	During Covid
Valiyaveedu et al.	2021	focuses on Web phishing attacks	Not relate
He et al	2021	highlighted the increase in cyberattacks (e.g., phishing campaigns and ransomware attacks)	During Covid
Basit et al.	2021	Applications of artificial intelligence to detect phishing attacks	Not relate
Salloum et al.	2021	Review natural language processing techniques for detecting phishing emails	Not relate
Alkhalil et al.	2021	describes the complete process of a phishing attack.	Not relate
Hakak et a	2020	Malicious cyber activities, focus on Phising	During Covid
Korkmaz et al.	2020	Analyzes machine learning-based phishing detection systems.	Not relate
Choudhary et al.	2022	Classified cyber crimes committed during the pandemic across the world.	During Covid
Alawida, M et al.	2022	Covered the main types of cyber-attacks such as mobile app, Phishing, email attacks etc.	During Covid

The extraordinary effects of COVID-19 led to a stunning wave of study that was developed to contrast the several covid-induced problems. Numerous studies that focused on cybercrime, cyberattacks, and cybersecurity challenges that emerged during the pandemic are included in this new wave of study. A few survey publications supplemented the original study done in this direction. Here, we examine previous studies that looked at the connection between cyberattacks and COVID-19 in brief and point out how they differ from our current study. The table below gives a summary of the existing surveys, most of which are relevant to our work.

4.2 Cyber Security Crimes During COVID-19 Pandemic in Financial Institution

Numerous cybersecurity attacks on the banking industry took place during the COVID-19 crisis. Financial services cybercrime has an average cost of $5.85 million, making it one of the most expensive crimes across all businesses (ibm.com, 2020; Najaf et al., 2020; Bossler, 2021). It has compelled financial institutions such as insurance and bank firms to continue providing internet help to their customers. Once more, the vast majority of workers utilised an unsafe network while working from home. Once at work, employees are subject to specific security precautions that weren't there before and have now become standard procedures. When using an unsecured network, employees were more susceptible to cyber dangers. Attackers frequently use distributed denial of services (DDoS), phishing, and malware intrusions to target the banking sector. Hackers used stolen bank credit cards to access ATM transactions (Omolara et al., 2019). Customers depend more on internet banking, which puts them at risk from hackers (Babulak et al., 2020). The incidence of credit card fraud increased during the Covid-19 crisis (Zhu et al., 2021; Payne and Morgan, 2020).

In order to secure data in online transactions, it is urgently necessary to build a hybrid cypher and modern, safe encryption techniques (Omolara et al., 2014). Financial institutions and banks are a natural target for ransomware since attackers are aware that they have access to enormous sums of money. The need to maintain banking services and the likelihood that victims will pay the ransom have led to a rapid increase in the attractiveness of financial institutions among hackers and other bad guys of all stripes. Approximately $5.2 billion in Bitcoin (BTC) has purportedly been traced to FinCEN (Financial Crimes Enforcement Network), which thinks the transactions have something to do with paying ransoms.

4.3 Timeline of Cyber Security Crimes Related to COVID-19

The COVID-19 pandemic's cyber-crime events seriously threaten the safety and socioeconomic advancement of the entire world's population. It is crucial to comprehend their mechanics and how they spread, and how far they can travel. In an attempt to contain the spreading of the coronavirus, more people are working from home, going to online schools, and doing business online. Virtually every nation on the planet declared a state of emergency. However, practically all financial industries saw constant cybersecurity threats during the COVID-19 crisis. Table 3 shows numerous Cyber security crimes that occurred in financial institutions during the peak of the COVID-19 pandemic.

Table 3: Different Cyber Security Crimes Incident in Financial Institution during The Pandemic.

Event	Date	Target	Incident
Fake calls banking Trojan	April 11, 2022	South Korea	Cyberattacks, Data breach
CashMama data breach (Sharma, B.)	April 06, 2022	India	Data breach
Aon ransomware attack. Jenkinson, A. (2022).	February 25, 2022	United States	Ransomware
OCBC phishing scam Tham, D. (2022	December 23, 2021	Singapore	Phishing
Banks targeted by SharkBot banking Trojan Dorotík, L. (2021).	October 2021	UK and Italy	Malware
Chase Bank phishing attacks (Rane, S et al, 2022	May to August, 2021	United States	Phishing
Reserve Bank of New Zealand Data Breach Davtyan, A. (2022).	January 10, 2021	New Zealand	Cyberattcks, Data breach
PixStealer targets Brazilian banking applications. Wernik & Melnykov, 2021	September 29, 2021	Brazil	malware cyberattack, data breach
Oscorp malware returns as an Android botnet. (Lakshmanan, R. (2021)	July 27, 2021	Spain, Poland, Germany, Turkey, United States, Japan, Italy, Australia, France and India.	malware cyber attacks
Southeast Asian Banks Credit Card Breach (Sukumaran, T. (2020)	March 06, 2020	Malaysia, Singapore, Philippines, Vietnam, Indonesia and Thailand	Cyberattack, Data breach
AXA hit by ransomware Kim & Lee (2022)	May 16, 2021	Thailand, Malaysia, Hong Kong and the Philippines	Ransomware

On April 11, 2022, researchers reported on the banking trojan Fake calls, where the fake caller spoke to victims and pretended to be one of the bank employees. Fake calls imitate the mobile applications of well-known Korean banks. The Trojan tries to access the victim's contacts, speaker, webcam, location, and call handling while the attackers try to get the victim's payment details or personal data. Additionally, Fake calls feature a spyware toolbox (Kim and Son, 2022). Cashman, an Indian loan app, announced a data breach on the 6th of April, 2022, in which invasively acquired and stored client data was made public. Clients' private details and other sensitive information were exposed because CashMama's Amazon S3 bucket was left in open manner (Sharma, 2022). On March 17, 2022, a data breach in South Africa was reported. A cyber attack on the credit bureau TransUnion SA resulted in the theft of the personal information of about three million customers.

TransUnion declined to pay the ransom that the attackers requested. Aon, a leading worldwide insurance and reinsurance broker, experienced a ransomware attack in February 2022, which had a minor negative impact on a few of its services. According to reports, the attack had little to no effect on the business. Aon has not provided any other information regarding the incident (Jenkinson et al., 2022). A phishing fraud that targeted 790 OCBC bank clients in Singapore in December 2021 cost at least $13.7 million in losses. Attackers could access victims' bank accounts and drain them entirely of their funds when victims clicked on the supplied link and entered their login information (Tham, 2022). A new Android banking Trojan named SharkBot was found by Cleafy and ThreatFabric experts before the end of October 2021. The Trojan gains admin rights, collects keystrokes, accesses mobile banking and cryptocurrency apps to transfer money, and grants itself admin credentials after tricking targets into downloading malicious apps from Google Play Store (Dorotík, 2021).

Researchers from Cyren observed a 300% rise in phishing assaults directed against Chase Bank between May and August 2021. The XBALTI phishing kits imitated the Chase banking portal. The phishing kits, according to researchers, were extremely sophisticated and made to gather more information than email addresses and passwords (Rane et al., 2022). The Reserve Bank of New Zealand experienced a data breach in January 2021 as a result of unauthorised access to its data through one of the bank's third-party file-sharing services. A fresh wave of harmful Android apps targeting Brazilian banking software, such as the Pix payment system used by the Central Bank, was uncovered in September 2021 by Check Point Research experts. A never-before-seen feature known as PixStealer, found in one of the malicious software, allows for the money theft of victims utilising Pix transactions (Wernik and Melnikov, 2021).

A botnet effort known as UBEL was reportedly targeting users of banking applications in Australia, Germany, Spain, the United States, Japan, Turkey, Italy, France, Poland and India on July 27, 2021, according to Cleary researchers. A botnet made from the Android virus Oscorp was used in the campaign. Before, it was discovered that the malware was leveraging accessibility services to steal user passwords from European banking applications (Lakshmanan, 2021). UBEL has the ability to access confidential data and exfiltrate it back to a distant server, concealing its location and attaining persistence. Based on a study, It was revealed in March 2020 that more than 200,000 credit card numbers from reputable banks in Singapore, Malaysia, the Philippines, Vietnam, Indonesia, and Thailand had been stolen and posted online (Sukumaran, 2020).

According to security analysts, Singapore and Malaysia had 37,145 and 25,290 cards compromised, respectively, while the Philippines had 172,828 cards. In response, CIMB Group Holdings, one of the banks, stated that they were confident there had been no breach and that the information would have been found elsewhere (Sukumaran, 2020). The Philippines, Thailand, Malaysia, Hong Kong, and Axa, a French insurance company, were the targets of a ransomware attack, according to a statement released on May 20, 2021. The Abaddon ransomware organisation launched DDoS attacks the day before and claimed to have stolen 3 TB of private data from AXA's Asian operations (Kim and Lee, 2022).

5. CONCLUSION

In this paper, the goal of this systematic review is to determine the impact that Covid-19 has on cybersecurity from the perspective of cybercrime. It also highlights the variety of cyberattacks experienced globally during the pandemic, focusing on financial institutions and how cybercrime increased over the period prior to the pandemic. Therefore, this paper specifically focused on the financial sector's exposure to cybersecurity crimes committed during the COVID-19 epidemic. Numerous studies and reports relating to cybersecurity were systematically discussed and analysed. The debate summarised the literature, concluded based on a synthesis of various recent studies, and compared cyberattacks before and after Covid-19 to determine how they affected cybersecurity. Our analysis highlighted that the number of cybersecurity crimes in financial institutions had nearly doubled compared to the period before covid. Also, phishing attacks are the most common form of cybercrime. Finally, in order to address the growing cybersecurity risks that are becoming more prevalent every year, it will be helpful to draw lessons from the contrast between phishing and other cyberattacks during the COVID-19 pandemic.

REFERENCES

Alawida, M., Omolara, A.E., Abiodun, O.I., and Al-Rajab, M., 2022. A deeper look into cybersecurity issues in the wake of Covid-19: a survey. Journal of King Saud University-Computer and Information Sciences.

Bouveret, A., 2018. Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Calliess, C., and Baumgarten, A., 2020. Cybersecurity in the EU the example of the financial sector: a legal perspective. German Law Journal, 21 (6), Pp. 1149-1179.

Computing, C., 2015. International Journal of Advanced Research in Computer Science and Software Engineering. International Journal, 5 (6).

Davtyan, A., 2022. Cyber Vulnerability Of Japanese Banking/Financial System. The EUrASEANs: journal on global socio-economic dynamics, 1 (32), Pp. 53-59.

Dorotík, L., 2021. Analýza datových sad umožňujících detekci mobilního malwaru.

Gobeo, A., Fowler, C., and Buchanan, W.J., 2022. GDPR and Cyber Security for Business Information Systems. CRC Press.

Jenkinson, A., 2022. Ransomware and Cybercrime. CRC Press.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A., and Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139, Pp. 719-749.

Kashyap, A.K., and Wetherilt, A., 2019. Some principles for regulating cyber risk. AEA Papers and Proceedings, 109, Pp. 482-87.

Kim, J., and Lee, S.J., 2022. Darknet Traffic Detection and Classification Using Gradient Boosting Techniques. Journal of the Korea Institute of Information Security & Cryptology, 32 (2), Pp. 371-379.

Kim, J., Kim, J., Wi, S., Kim, Y., and Son, S., 2022. HearMeOut: detecting voice phishing activities in Android. In Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, Pp. 422-435.

Kopp, E., Kaffenberger, L., and Wilson, C., 2017. Cyber risk, market failures, and financial stability. International Monetary Fund.

Kost, E., 2022. Biggest Cyber Threats for Financial Services in 2022 | UpGuard. Third-Party Risk and Attack Surface Management Software | UpGuard. https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services#toc-0G7 (2016): "Fundamental elements of cybersecurity for the financial sector", October.

Lakshmanan, R., 2021. Ubel is the new Oscorp - android credential stealing malware active in the wild. The Hacker News. Retrieved November 2022, from https://thehackernews.com/2021/07/ubel-is-new-oscorp-android-credential.html#:~:

Lam, E., 2019. Hackers Steal $40 Million Worth of Bitcoin from Binance Exchange. The Bloomberg.

Malik, M.S., and Islam, U., 2019. Cybercrime: an emerging threat to the banking sector of Pakistan. Journal of Financial Crime.

Mallet, V., and Chilkoti, A., 2016. How cyber criminals targeted almost $1 bn in Bangladesh bank heist. Financial Times, Pp. 18.

Prenio, J., Yong, J., and Kleijmeer, R., 2019. Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions. FSI Insights, No. 21.

Rane, S., Devi, G., and Wagh, S., 2022. Cyber Threats: Fears for Industry. In Cyber Security Threats and Challenges Facing Human Life, Pp. 43-54. Chapman and Hall/CRC.

Silver-Greenberg, J., Goldstein, M., and Perlroth, N., 2014. Jpmorgan chase hack affects 76 million households. New York Times, 2.

Smikle, L., 2022. The impact of cybersecurity on the financial sector in Jamaica. Journal of Financial Crime.

Stallings, W., and Brown, L., 2016. Computer security concepts. Computer Security Principles and Practice, Pp. 10-17.

Tham, D., 2022. OCBC Phishing Scam: Youth admits to money laundering, first to be dealt with by Court. CNA. Retrieved April 2022, from https://www.channelnewsasia.com/singapore/ocbc-phishing-scams-money-laundering-leong-jun-xian-court-2635506

Tofan, D., Nikolakopoulos, T., and Darra, E., 2016. The cost of incidents affecting CIIS: systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). ENISA, Athens, Greece.

Treanor, J., 2016. Tesco Bank cyber-thieves stole£ 2.5 m from 9,000 people. The Guardian.

Vučinić, M., and Luburić, R., 2022. Fintech, risk-based thinking and cyber risk. Journal of Central Banking Theory and Practice, 11 (2), Pp. 27-53.

Wernik, I., and Melnykov, B., 2021. Pixstealer: A new wave of Android Banking trojans abusing accessibility services. Check Point Research. Retrieved November 2022, from https://research.checkpoint.com/2021/pixstealer-a-new-wave-of-android-banking-trojans-abusing-accessibility-services/