Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Journal of King Saud University – Computer and Information Sciences 34 (2022) 8176–8206

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A deeper look into cybersecurity issues in the wake of Covid-19: A survey

Moatsum Alawida [a,*], Abiodun Esther Omolara [b], Oludare Isaac Abiodun [b,*], Murad Al-Rajab [a]

[a] Department of Computer Sciences, Abu Dhabi University, Abu Dhabi 59911, United Arab Emirates
[b] Department of Computer Science, University of Abuja, Gwagwalada, Nigeria

ARTICLE INFO

Article history:
Received 27 April 2022
Revised 3 July 2022
Accepted 2 August 2022
Available online 11 August 2022

Keywords:
Cybersecurity
COVID-19 and organization cybersecurity challenges
Trending insight of cyber-attack
Internet security
Business security
Economic disruption
Cyberspace future

ABSTRACT

This study analyzed the Coronavirus (COVID-19) crisis from the angle of cyber-crime, highlighting the wide spectrum of cyberattacks that occurred around the world. The modus operandi of cyberattack campaigns was revealed by analyzing and considering cyberattacks in the context of major world events. Following what appeared to be substantial gaps between the initial breakout of the virus and the first COVID-19-related cyber-attack, the investigation indicates how attacks became significantly more frequent over time, to the point where three or four different cyber-attacks were reported on certain days. This study contributes in the direction of fifteen types of cyber-attacks which were identified as the most common pattern and its ensuing devastating events during the global COVID-19 crisis. The paper is unique because it covered the main types of cyber-attacks that most organizations are currently facing and how to address them. An intense look into the recent advances that cybercriminals leverage, the dynamism, calculated measures to tackle it, and never-explored perspectives are some of the integral parts which make this review different from other present reviewed papers on the COVID-19 pandemic. A qualitative methodology was used to provide a robust response to the objective used for the study. Using a multi-criteria decision-making problem-solving technique, many facets of cybersecurity that have been affected during the pandemic were then quantitatively ranked in ascending order of severity. The data was generated between March 2020 and December 2021, from a global survey through online contact and responses, especially from different organizations and business executives. The result show differences in cyber-attack techniques; as hacking attacks was the most frequent with a record of 330 out of 895 attacks, accounting for 37%. Next was Spam emails attack with 13%; emails with 13%; followed by malicious domains with 9%. Mobile apps followed with 8%, Phishing was 7%, Malware 7%, Browsing apps with 6%, DDoS has 6%, Website apps with 6%, and MSMM with 6%. BEC frequency was 4%, Ransomware with 2%, Botnet scored 2% and APT recorded 1%. The study recommends that it will continue to be necessary for governments and organizations to be resilient and innovative in cybersecurity decisions to overcome the current and future effects of the pandemic or similar crisis, which could be long-lasting. Hence, this study's findings will guide the creation, development, and implementation of more secure systems to safeguard people from cyber-attacks.

Contents

* Corresponding authors.
E-mail addresses: moatsum.alawida@adu.ac.ae (M. Alawida), oludare.abiodun@uniabuja.edu.ng (O.I. Abiodun).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2022.08.003
1319-1578/

1. Introduction

In times of crisis, an upsurge in cyber-attacks is usual. Take for instance, the global economic crisis in 2008 resulted in cyber-attacks as corporation capital declined and citizens became an easy target (Ng and Kwok, 2017; Thakur et al., 2016; Das, 2015; Watters et al., 2012). Cybercriminals take advantage of social flaws, and thus, the coronavirus pandemic, also known as COVID-19, is no exception. The picture of cybersecurity threats in 2020 has mirrored that of the previous economic downturn. With these eye-opening 2020 cybersecurity figures, one can observe the impact of COVID-19 on individuals, businesses, and the entire world, even in its early phases. The COVID-19 outbreak began to make international headlines in January 2020. COVID-19 was declared a worldwide pandemic by the World Health Organization (WHO) on March 11, 2020. That week, everything changed in the world. Bustling streets were deserted, hospital beds were overflowing, and shops were shuttered. COVID-19 has already been dubbed the world's biggest cybersecurity threat. The healthcare and banking industries were the most vulnerable to cyber-attacks. As a result of the COVID-19, email phishing threats were the most common source of data breaches while working from home because of the national lockdown.

Many types of cyber-attack took place day and night during the peak period of the global COVID-19 crisis. Hackers were busy launching and trying their hands on different variants of cyber-attacks such as phishing, malware, distributed-denial-of-service (DDoS), denial-of-service (DoS), advanced persistent threat (APT), malicious social media messaging (MSMM), business email compromise (BEC), botnet, ransomware amongst many others. In the case of the phishing attack, hackers used harmful links hidden in carefully designed emails to target company employees. Unfortunately, when employees click on such links, they ignorantly download keylogging software onto their computers or devices, giving hostile actors access to their credentials. Hackers can then gain unrestricted access to critical business assets and data of the victim's organization by impersonating a genuine employee.

In the year 2020, there was about 1001 frequency of data breaches in the United States. As a result, over 155.8 million people were affected by data breaches in the same year. According to the Identity Theft Resource Center's (ITRC) data breach study, there were 1,291 data breaches between September 2020 and September 2021. Compared to the 1,108 data breaches reported in 2019, this statistic represents an 8 percent rise. The trend of compromise between 2016 and 2021 is highlighted in Table 1.

In the year 2020, in the wake of the COVID-19 crisis, there were about 1,872 breaches, compared to 1,108 in 2019. However, in the first quarter of 2022, data compromises caused by physical attacks such as document or device theft and skimming devices fell to single digits (3), totaling 404. In the aftermath of the COVID-19 pandemic, cyber security concerns have arisen from various quarters. In the past two years, the COVID-19 pandemic has been making headlines worldwide. The medical community, as well as governments and citizens around the world, are pooling their resources to stop the spread of the disease. Unfortunately, as healthcare organizations beef up their resources to battle the COVID-19 outbreak, they have become targets of cyber-attacks (McKinsey and Company, 2020, TCS Worldwide, 2020; Orange Cyber Defense, 2020).

In this context, on April 8, 2020, the US Department of Homeland Security (DHS), the UK's National Cyber Security Centre (NCSC), and the Cybersecurity & Infrastructure Security Agency (CISA) issued a joint advisory describing how the COVID-19 pandemic was being exploited by cybercriminals and APT organizations (Deloitte, 2020). Concerns about phishing, malware and other attacks on communication networks were addressed in this advisory from organizations, such as Microsoft Teams and Zoom. As the world focuses on the health and economic concerns posed by COVID-19, cybercriminals around the world are undoubtedly taking advantage of the situation (Abiodun et al., 2022). Recent studies have shown that a plethora of businesses owned by mega organizations, small and medium scale enterprises were victims of cyber-attack with the rise of COVID-19, which also constituted to their collapse (Lallie et al., 2021).

(a) Motivation

In the wake of COVID-19, cyber-attackers aimed at disrupting and rendering company operations useless for malicious and remunerative purposes. There has been a significant increase in DDoS and DoS activities. Adversaries have been spotted attempting to disrupt business networks and propagate disinformation to weaken pandemic responses involving vaccine research, healthcare distribution, and treatment delivery. Hackers seeking financial gain, as evidenced by the rise in Bitcoin-to-United States Dollar (USD) pricing, are likely the cause of the return to or re-prioritize ransom denial of service (RDoS) and DDoS extortion operations in huge numbers. Threat actor groups with sophisticated tools meant to disrupt or take down enterprise networks are frequently the source of this.

Nowadays, people use Internet platforms to purchase transportation tickets for air, bus, train, and taxi booking. Likewise, the Internet serves as a space for making food orders, recharging mobile phones, paying utility bills with credit/debit cards, and many e-commerce activities. Unfortunately, cybercriminals are attacking these sites to collect personal information for financial rewards. Therefore, the international research community, national research community and stakeholders in ICT must come together to tackle cyber-attack issues to curtail the losses emanating as the end product of the attacks, ranging from financial losses and damages to devices and network infrastructure collapse.

Table 1
The trend of compromise between 2016 and 2021.

S/n	Year	Compromises
1	2021	1,862
2	2020	1,872
3	2019	1,108
4	2018	1,175
5	2017	1,506
6	2016	1,088

(b) Search keyword

In this study, search keywords, including bibliographic databases, are explored. Overall, 300 papers were used in our study. The number of articles processed is summarized in Table 2.

(c) Paper organization

This paper discusses the existing open problems and challenges in cybersecurity during the global COVID-19 crisis. It is divided into several sections: Section 1, covers the introduction, motivation, and search keyword. Section 2, covers contributions and related work - combining previous and current studies, each with its subsections. The methodology is discussed in Section 3, which introduces the main analysis used for the data. It also provides details of how the survey was carried out systematically using a flow chart description. Section 4 showcases the result from the survey, analysis, and interpretation of results, each with their corresponding subsections. Section 5 is the discussion of the result with a presentation of a summary of implications, future research issues, and implications. Section 6 focused on solutions to the current cybersecurity challenges, recommendations and research findings. It also identified research gaps, current trends, future perspectives, directions, and suggestions. Finally, Section 7 concludes this survey and provides highlights of future work.

(d) Contributions

This study explores variants of cybersecurity problems, issues, and challenges encountered at the wake of the COVID-19 pandemic. However, certain types of cybersecurity problems were identified, which were predominant during the COVID-19 pandemic. Fifteen (15) types of cyber-attacks were identified as the most common. Some of the cyber-attack types are; malware, phishing, ransomware, distributed denial-of-service (DDoS), browsing apps, malicious domains, denial-of-service (DoS), mobile apps, and malicious websites. Others are spam emails, malicious social media messaging, business email compromise, APT, botnet attacks and hacking. Then policy conclusions were generated based on data from a comprehensive worldwide study conducted from March 2020 to December 2021. The main contributions of this research, as well as the distinctiveness of its methodology, are summarized in Fig. 1.

The frequency of cyber-attacks has risen dramatically in recent years and has progressively become more dangerous in the wake of COVID-19 as almost every-one has become a target to cybercriminals. Many people have suffered as a result of a lack of personal safety procedures when using the Internet. Cyber attackers now have simple access to some people's data due to the lockdown as a result of the COVID-19 epidemic. During this time, many banking sectors, governmental and non-governmental organizations have been targeted by attackers. Hence, this paper focuses on several security measures that can be taken to protect personal and organizational information from cybercriminals. Thus, Fig. 1 highlights the different angles depicting the main contributions of this paper, which uniquely covered the many incidences of cyber-attack cases in the wake of the COVID-19 pandemic. These main contributions are further discussed as follows;

Table 2
Data collection and systematization.

Item	Description
Research strings	String 1: "Cybersecurity and Coronavírus" or "COVID-19 pandemic" or "corona crisis" "corona" disease" "network security" "disease management" or "Internet security" "family* firm*" or "business crisis*" String 2: "Coronavírus" or "COVID-19" and "DDoS*" or "Phishing" or "ransomware" or "APT" or "eavesdropping*" or " Botnet" or "Malware" or "Scamming" or "Scam" or "Scan*" String 3: "COVID-19" or "coronavirus" and "Intrusion" or "Cyber-attack" or "Cybercriminals" or "Loss" or "Losses" String 4: "Coronavírus" or "COVID-19" and "business disruption" or "network disruption" or "financial impact" or "financial crisis" or "economic crisis" or "economic impact" or "socio-economic crisis" or "socio-economic impact".
Online databases	→IEEE (Institute of Electrical and Electronics Engineers) Xplore, →Emerald insight, →Science Direct, →Directory of Open Access Journals (DOAJ), →ACM Digital Library, →PubMed, →Scopus, →Compendex →Elsevier, →Education Resources Information Center (ERIC), →Springer, →Taylor and Francis, →World of Science (WoS), →EBSCO Host, →Journal Storage (JSTOR), →Google Scholar, →Willey, →Others include a resources list from COVID-19 research: journals, websites, and bibliographies
Period	March 2020 to December 2021
Area of research	Cyber-attacks and COVID-19 crisis
Language	English
Documents	Article and Review and Editorial
Date of search	December 2021

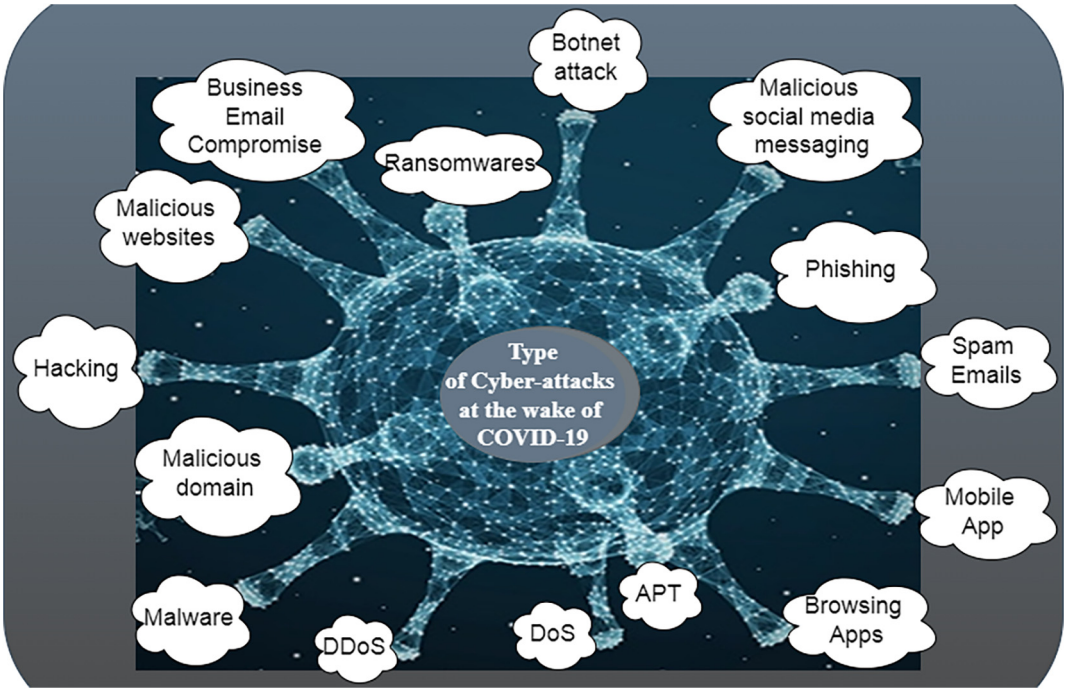

Fig. 1. Main Cyber Security Threats in the wake of COVID-19.

1.1. Hacking

Malicious scammers went on a rampage to hack people connected to digital networks such as computers, laptops, tablets, and phones. Thereby stealing sensitive data such as passwords, usernames, bank information, and other personal details. Some hackers used the stolen data to withdraw money from people's accounts. Likewise, bank loan scams spread rapidly at the peak of the COVID-19 crisis, as many of the scams focused on defrauding people of their money and personal information through online shopping. As a result of the pandemic, fraud cases was 42 percent greater than the previous year, 2019, as cybercrooks took advantage of the fact that many physical stores had to close. Some bank clients reported receiving SMS messages instructing them to go online and reschedule a package delivery. At the same time, others filled out their banking information which subsequently led to

their accounts being hacked. In other news, two Indonesian hackers were apprehended for a $60 million scam, according to CBS News, on the 16th of April 2021. Following a tip from US authorities, the two suspects were apprehended in Surabaya, Indonesia's second-largest city (cbsnews, 2021).

The scam had been going on for an unknown amount of time, according to the Indonesian police. "Around 30,000 Americans have been duped, and the government has lost up to $60 million," claimed East Java police head Nico Afinta (cbsnews, 2021). In the United States, thousands of targeted victims have provided personal data to the fraudulent website. These personal details include social security numbers, with the expectation of receiving $2,000 as part of an unemployment relief program to scam the government. Hence, an urgent need for more research on how to counter hackers, especially during a crisis.

1.2. Phishing

Phishing is a method of social engineering exploits frequently used to obtain sensitive information from users, such as online banking login credentials, company login credentials, credit card details, login credentials, or username/passwords. Thus, cybercriminals steal confidential information by sending fraudulent messages to their target. The aim is to get people to expose their financial details, system credentials, and other sensitive data.

Phishing is still the easiest method for hackers to infect a device with malware. Phishing schemes entice victims to open emails or click on links that look to come from a credible company or respectable source. The link may take one to a bogus website that asks people for personal information or to a website that directly infects user computers with malware. Therefore, if one is unsure about a link, do not click the link. During the nationwide lockdown caused by the widespread Coronavirus, hackers took advantage of the situation by sending phishing emails to many people.

Phishing emails contain phony web pages that can acquire a user's personal information. Since most people now rely on online channels to cope with the pandemic, they have become exposed to phishing attempts. In March 2020, out of 4,67,825 phishing emails, 9,116 were related to COVID-19, accounting for less than 2 % of all phishing emails (Naidoo, 2020). Nevertheless, the reported amount of suspected email attacks provides insight into the United Kingdom (UK) cyber-crime incidence problem faced during the epidemic, where a sizeable number of phishing and smishing attacks occurred.

Smishing is a type of scam that involves sending text messages that appear to be from legitimate and trusted organizations to trick people into divulging personal information like credit card numbers, usernames and passwords. More than 160,000 suspicious emails attacks had been reported to the National Cyber Security Centre (NCSC) by the beginning of May, precisely 7th 2020 (NCSC, 2020; Lallie et al., 2021), and by the end of May, precisely on the 29th, 2020, about £4.6 million had been lost to COVID-19-related scams, with around 11,206 victims of phishing and/or smishing campaigns (Sky News, 2020). In response, the NCSC and Her Majesty's Revenue and Customs (HMRC) brought down 471 fraudulent online shops (Tidy, 2020) and 292 counterfeit websites (Hill, 2020). Vishing and Smishing are two types of cyber-fraud that criminals deploy to deceive people into giving up money or personal information. In the case of vishing, it is by voice, while, in the case of smishing, it is by SMS deception.

1.3. Ransomware

Ransomware is a sort of malicious software that criminals design to prevent users from accessing their computers unless they pay money. Ransomware attacks skyrocketed as the number of people working remotely rose during the pandemic (Chigada and Madzinga, 2021). Ransomware is becoming increasingly sophisticated. Other technologies are now being added to ransomware's armoury, in addition to encryption. The financial sector, in particular, is a common target for ransomware attacks. The ransomware has also grown in scope and intensity, causing damage to corporations, organizations, healthcare providers, and government departments while many countries struggle to respond to the COVID-19 crisis. As ransomware continues to be one of the most severe worldwide cyber threats to healthcare, security staff must be cautious and informed of the methods, techniques, and procedures that criminals will employ to earn a profit. According to cybersecurity experts, in October 2020, ransomware gangs are starting to use DDoS attacks on victims' networks or websites as a supplemental tool to pressure them to pay a ransom. RagnarLocker and SunCrypt were the two operations adopting this novel method at the time. Ransomware gangs now have new attack surfaces to try to exploit and apply debilitating strategies to force enterprises to pay ransom demands as the threat landscape has changed.

Healthcare providers are usually targeted by cybercriminals looking to make the most money in the shortest amount of time. The Avaddon ransomware gang has recently joined the practice of utilizing DDoS assaults to extort money from victims. After launching spam campaigns that targeted people all around the world, the Avaddon ransomware commenced operations in June 2020. The ransomware gang tried their hand at double extortion when they sent an unidentified victim organization a menacing ransom note with a deadline of 240 h to cooperate. Failure to do so would expose the company's database, which includes customer and employee personal details, as well as financial paperwork. According to the ransom message, the victim's website was under a non-stop DDoS attack until Avaddon was contacted. Therefore, there is an urgent need for more research on how to counter ransomware attacks, especially during a crisis.

1.4. Botnet attack

Botnet or a bot is a device like a computer, server, or phone infected with malware such as malicious programs, software, virus, and worms that perform destructive actions without the user's knowledge. Botnets are infected device networks that work collectively under an attacker's command. Botnets are utilized to carry out phishing scams, spam campaigns, and distributed denial of service (DDoS) attacks. Most botnets use distributed denial-of-service to send as many requests as possible to a single Internet computer or resource, overloading it and subsequently preventing it from serving genuine requests. Cybercriminals are swiftly enlisting Internet of Things (IoT) devices (Abiodun et al., 2021a; Abiodun et al., 2021b) into their botnet forces, according to the current threat intelligence discoveries from A10 Networks' cybersecurity researchers, boosted by Mozi malware spreading throughout the world. Attackers are increasingly focusing on low-volume, high-frequency attacks that can have a big impact and, in between, avoid being traced, detected or defended by measures put in place by targets.

Thus, in the wake of COVID-19, there are cases of botnet threats like emotet attacks. Emotet is a type of computer malware originally designed as a banking Trojan. Many botnets, such as emotet, are polymorphic in nature. Emotet polymorphism means that the malware's code changes every time it is activated. Usually, most antivirus programs search the computer for existing malware codes. However, a code change may make it more difficult to detect the infection, thus, allowing it to go undetected. Emotet grew in size over time and was responsible for millions of costly cyberattacks worldwide. Emotet's capacity to acquire access to one's computer got increasingly sneaky, allowing new viruses to infiltrate

the target system. Malspam, or spam emails with malware, is the most common way for it to disseminate, hence, the term. Summarily, emotet is a Trojan horse that is disseminated mostly through spam emails, that is, *malspam*. Malicious scripts, macro-enabled data, files, documents, and malicious links are all possible ways for the infection to spread. To persuade users, its messages frequently contain familiar branding to look like a legitimate email, imitating the email structure of well-known, trusted and popular companies such as DHL or PayPal to convince users.

Emotet was a cybercrime service that was both professional and long-lasting. Emotet, once labelled "the world's most destructive malware," has resurfaced and is being deployed on Windows systems infected with TrickBot malware during the peak of COVID-19. The emotet Malware infected over 1.6 million computers worldwide, causing damages worth hundreds of millions of dollars. In January 28, 2021, the United States of America Justice Department declared its participation in a worldwide operation encompassing the US, France, Canada, the Netherlands, Germany, and the United Kingdom to disrupt and shut down the infrastructure of the emotet malware and botnet. Officials from Ukraine, Sweden, and Lithuania also participated in this huge cyber operation on emotet. "Regrettably, the emotet malware and botnet infected hundreds of thousands of computers across the United States, such as key infrastructure, and caused millions of dollars in damage to victims around the world". Emotet can transmit further malware to targeted computers, such as ransomware or spyware that steals financial credentials, once it has infected them. Hence, there is an urgent need for more research on how to counter botnets, especially during a crisis.

1.5. APT

Cyber attackers and APT groups took advantage of vulnerable persons and systems during the national lockdown amidst the COVID-19 outbreak. An attack or state-sponsored group known as an APT happens when an unauthorized user uses advanced and sophisticated ways to obtain access to a system or network. APT usually deploy techniques such as ransomware, phishing, malware, and data breaches to launch attacks on their targets (Mohamed et al., 2018). The group focuses typically on telecommunications, military and travel sectors, suggesting that it intends to conduct surveillance, tracking, or monitoring activities on specific individuals. Intention to gather proprietary or customer data for commercial or operational purposes in support of national priorities or to build additional entry points and vectors to aid future campaigns. Targeting government entities reveals a secondary goal of gathering geopolitical data to aid nation-state decision-making. In an incidence case of an APT threat, three members of North Korea's Reconnaissance General Bureau were charged for WannaCry, the Sony Pictures hack, and many other cybercrimes in February 19, 2021. Template injection, Malicious macros, RTF exploits and Malicious LNK files are part of the methods utilized by APT cyber-attackers at the peak of the COVID-19 pandemic. Data exfiltration attacks continue to soar (Taofeek et al., 2022), and organizations are forced to pay huge amounts of money as ransom. Thus, researchers need to focus further research on how to counter APT attacks.

1.6. Malware

Malware is software or code meant to harm computers by encrypting files, damaging, disabling, stealing data, or gaining unauthorized access to a computer. Likewise, malware can replicate itself onto a system like a computer or computer network to cause harm or destroy data. It is one of the common cyber-threats that organizations and businesses face in recent times. The phrase refers to a variety of harmful software, including trojans, worms, and ransomware. COVID-19 peak crisis was Malware's data-gathering season. That is, it has become a period in which cybercriminals have increased their use of data harvesting software such as Remote Access Trojan, info stealers, spyware, and banking Trojans. Threat actors enter systems using COVID-19-related material as a lure to breach networks, steal data, fraudulently transfer money digitally, and construct botnets. During this Coronavirus crisis, cybercriminals are infecting users' gadgets with malware. Malware can open a backdoor in a user's gadgets, allowing cyber attackers to access all of the user's private details, such as username and password. This malware is being propagated using a few internet Corona tracing maps.

More disruptive Malware, such as DDoS and Ransomware were launched during the COVID-19 crisis. Cybercriminals are mercilessly increasingly utilizing disruptive malware against vital infrastructure and healthcare organizations because of the potential for financial gain. For example, multiple threat organizations that had been relatively idle for a few months launched a wave of ransomware attacks in the first two weeks of April 2020. According to law enforcement investigations, most attackers predicted the maximum amount of ransom they might demand from targeted firms pretty accurately. As a result, consumer victims reported total cybercrime-related losses of $4.2 billion in 2020, which was up to 69 percent from 2019, according to the FBI Internet Crime Complaint Center. Malware attacks contributed to some of these losses. Therefore, there is an urgent need for more research on addressing malware attacks even during this crisis period.

1.7. Malicious social media messaging

During the climax of the COVID-19 attack and the lockdown period, there was a lot of malicious social media messaging and misinformation. Malicious social media messaging and misinformation to people and fake news grew to an alarming proportion. Unverified information, a lack of understanding of dangers, and a plethora of conspiracy theories have all led to community fear and, in some circumstances, aided in the execution of cyberattacks. Nearly 30 % of countries participating in the worldwide cybercrime study reported that incorrect material about COVID-19 was being circulated. A country recorded 290 postings in a month, the bulk of which contained hidden spyware. According to reports, misinformation has also been related to the unlawful trafficking of fake medical supplies. Other incidents of disinformation also reported scams, including *'too great to be true'* offers like free food. Hence, there is an urgent need for research on how to address the issue of malicious social media messaging attacks that is fast growing as a means of cyber-attacks.

1.8. Business ***email compromise***

Business Email Compromise (BEC) threats are one of the most financially devastating types of cybercrime (Greathorn.com, 2021; Cross and Gillett, 2020; Cross and Kelly, 2016). They often use social engineering strategies and phishing emails to infiltrate organizations and fool unwary employees and executives into performing tasks that appear to come from a trustworthy sender, frequently posing as legitimate business activities. BEC attacks increased by 14 % in 2020 due to the massive cyber-attack surge prompted by the COVID-19 issue and worldwide lockdown measures. Profit will likely continue to drive this category forward; in 2020, hostile actors received compensation that was 30 % higher than the previous year, 2019. Hackers masquerading as the World Health Organization (WHO) send messages to people's emails that an attached file explains how to stop the sickness from spreading. They say that "*one small measure can cure you*." However, according

to Proofpoint, the email attachment contains no relevant information and instead infects Personal computers (PCs) with malicious software known as AgentTesla Keylogger. AgentTesla Keylogger could record every keystroke and sends it to the attackers, allowing them to track their victims' online activities.

In a recent BEC report by "Cybersecurity Insiders" found in Greathorn.com (2021) and Cross and Gillett (2020): (i) the most popular type of BEC attack is a spoofed email accounting for 71 %, followed by spear-phishing, which was 69 %. Furthermore, (ii) more than half of links received via email lead to a malicious site (iii) 57 % of malicious links in phishing emails intend to steal credentials. (iv) the finance sector has a target on its back, according to 34 % of respondents. (v) in the last 12 months, 3 % of firms have had a security event, with BEC/phishing attacks accounting for more than 50 % of those occurrences, according to 35 %. Regrettably, the rate of financial crime (Omolara et al., 2018a; Omolara et al., 2018b), has increased in recent times (Achim et al., 2021; Ünvan, 2020; Hasham et al., 2019; Reid, 2018; Masciandaro, 2017; Gottschalk, 2008; Sakurai and Smith, 2003).

Financial loss is the most evident consequence of BEC fraud. Fraud is successful when the perpetrator can tailor the details of their approach to the target's individual vulnerabilities or shortcomings. To do so, criminals can extensively study the organization and its linked individuals to imitate a believable attack. Information about some organizations is freely available on the internet (Burns et al., 2019). Perpetrators may gather information about an organization and its employees by using public information or infiltrating social networking platforms. Therefore, individuals, organizations and governments must begin to invest more in cybersecurity to mitigate cyber-attacks such as BEC in crisis conditions.

1.9. Distributed denial-of-service (DDoS) attack

DDoS attack is a type of attack that cybercriminals deploy to render online services unavailable to users by generating a large amount of traffic. The number of DDoS attacks has surged thrice in the last three months compared to the prior three months. The overall number of reported DDoS attacks in the first quarter of 2020 was 242, while the number grew to 300 in the second quarter (Wu et al., 2020; Mansfield-Devine, 2015). The COVID-19 crisis has resulted in a considerable increase in fraudulent behavior. Many people's lives changed dramatically, making them more vulnerable: working from home rather than in an office, balancing childcare, and being concerned about health, financial resources and the future. The healthcare industry is particularly the hardest hit by COVID-19 since it has the most vulnerable and targeted systems. For instance, attackers launched a DDoS attack against the United States Department of Health and Human Services, causing significant damage to its servers (Stein et al., 2020). More also, financial sectors, like banks are equally affected as the healthcare industries.

As more heterogeneous devices connect online through Internet of Things (IoT) devices and enterprises build remote networking systems to augment pre-existing infrastructure, it unwittingly gives room for denial-of-service attacks to escalate.

Denial-of-Service attacks increased as more devices came online and organizations speedy-up remote access for their employees. In addition, the methods used by attackers are becoming more sophisticated as information systems get more advanced and digital. As a result, criminal and nationwide actors have long valued denial-of-service cyberattacks, which may create major economic interruptions for any organization connected to the internet.

DDoS attacks that interrupt critical healthcare operations can lead to patient death. Disruption of essential care and supplies to vulnerable patients due to a DDoS attack can result in the worst outcome of a disruption of healthcare operations leading to death. When assessing potential implications on health operation services, patients admitted to hospitals in critical condition and in need of quick access to treatment, as well as the safety and integrity of surgical procedures, are highly considered to be in danger. Therefore, more research is needed to mitigate DDoS attacks, especially during a crisis.

1.10. Denial-of-service (DoS) attack

Denial of Service (DoS) attacks are a type of cybercrime that is frequently used by more technical criminals. The attacker of DoS attempts to temporarily or permanently make certain services not available to users through Internet resources, such as paying for utility, paying for goods purchased, and paying for airline tickets online. Hacking entails jeopardizing a system's confidentiality or integrity, and it necessitates a decent level of skill. Tactics may include exploiting system flaws to gain access to systems. As more heterogeneous devices connect to the internet through the Internet of Things (IoT) devices, denial-of-service cyberattacks have increased, and enterprises have bolstered remote connectivity technologies to support pre-existing infrastructure. In addition, as telework grows in reaction to the new coronavirus and initiatives to foster social separation, threat actors seek to profit from the present danger scenario.

Organizations of all sizes frequently fail to follow asset and inventory organization best practices that would allow them to gain full awareness of their attack surface. Additionally, many IoT devices use default passwords and lack solid security postures, making them open to penetration and exploitation. Users are typically unaware that IoT devices have been infected, and an attacker may simply compromise many of these devices to launch a massive attack. DoS attacks disrupt system availability by flooding important services with unauthorized requests. The purpose is to take up all of the bandwidth allocated to genuine server queries in order to bring the server down. Hence, researchers need to urgently focus on preventing DoS attacks, especially during a crisis.

1.11. Malicious websites

Any act by a malicious attacker to undermine the security of a Web-based application is referred to as a malicious website apps attack. Web application or website apps attack can either target the application itself in order to get access to sensitive data, or they can use the application as a staging area for attacks against the application users. At the pinnacle of COVID-19, the use of the web to cause harm increased dangerously. As the number of people infected with coronavirus continues to rise, so do dangerous cyberattacks such as spam emails, phishing, malware, ransomware, and malicious domains that utilize the virus as bait (French et al., 2021). As a result, businesses of all sizes are under increasing pressure to tackle the obstacles posed by Covid-19-based cyber threats.

In reality, attackers are constantly devising new ways to assault and con people to profit from the fear and uncertainty surrounding the ongoing pandemic, keeping a step ahead. According to new Malwarebytes data, web skimming increased by 26 % in March 2020 compared to the prior month of February 2020. Another interesting discovery is that the number of people skimming the internet climbed slowly from January 2020 to February 2020 by 2.5 % and then increased dramatically between February and March 2020 by 26 %. While this is still a small increase, Malwarebytes feels it indicates a pattern that will become more visible in the months ahead. Hence, to move business, the executives should plan to prioritize operational capability towards eliminating malicious websites over the next two years. Similarly, research-

ers need to investigate how to block malicious websites for resiliency in digital business.

1.12. Malicious domains

Malicious domains are a type of cyber security breach that poses a serious threat to people's privacy and property by delivering malicious services such as phishing websites, spam servers, and command & control servers to Internet users. Cybercriminals have been exploiting, developing, and boosting their attacks at an alarming rate, taking advantage of the anxiety and uncertainty induced by COVID-19′s precarious social and economic bad conditions. The lockdown measures had particularly accelerated the creation of malicious web domains to make fictitious and concocted money from their target (Interpol., 2020). Thus Malicious websites (URLs) are used by threat actors to deceive the public, collect confidential data, and propagate malware to harm or corrupt systems and devices. A COVID-19 cybercrime assessment by INTERPOL revealed a considerable shift in target from individuals and small enterprises to major organizations, governments, and key infrastructure using malicious domains. Criminals are using new security weaknesses to steal data, create money, and cause disruption as organizations and companies rapidly deploy remote systems and networks to enable workers to work from home. One of INTERPOL's partner organizations detected 907,000 spam communicated messages, then 737 malware events, and 48,000 harmful Web links – all associated with COVID-19, over a four-month period, from January to April.

Malicious domains proliferated during the rise of COVID-19 and global lockdown countermeasures. Cybercriminals have begun registering domain names with keywords such as "coronavirus" or "COVID" to take advantage of the increasing demand for medical supplies and data about COVID-19. These phony websites support a wide range of criminal operations, such as *C*2 servers, malware deployment, and phishing. A private organization partner noticed and reported to INTERPOL a 569 % increase in illegal registrations, including phishing and malware, and a 788 % increase in high-risk registrations between February and March 2020. Therefore, researchers need to focus more on how to tackle malicious domains for resiliency in digital business. Likewise, to move businesses forward, the organization's executives must plan to prioritize operational capability toward eliminating malicious domains over the next two years.

1.13. Spam emails

Unsolicited or anonymous messages sent in bulk by email are known as email spam, sometimes known as junk email or simply spam. The name stems from a Monty Python joke in which the packaged pork product's name is mentioned. Spam is pervasive, inevitable, and monotonous. The amount of spam emails has risen by 300 times, and the number of harmful URLs has increased by 300 percent, especially at the peak of the COVID-19 crisis. The United States is the top country for spam and malware detection; most target consumers come from there (Cook, 2020). For instance, Google claims to have detected over 100 million phishing emails and 18 million daily spyware related to Covid-19 through its Gmail service. This is on top of the 240 million coronavirus-related spam emails sent daily. In addition, a study conducted by RiskIQ identified the top dangers for 2020 and found that cybercrime costs businesses roughly $24.70 per minute, while a malicious assault costs $4.95 per minute. As a result, cybercrime was forecasted to cost $11.4 million (£8.7 million) each minute globally by 2021, a 100 percent rise when relatively compared to the incidences of the year 2015.

Statistics have shown that 375 new threats of cyber-attacks are discovered every minute, and also a new vulnerability is discovered every 24 min, and more also, 16,172 records are compromised every minute. Every 16 min, there is a new Magecart cyber-attack. For example, the credit card skimmer attack vector, RiskIQ was - first discovered in 2018. "The world have seen thousands of new COVID-19 domains standing up daily, " said Steve Ginty, director of threat intelligence at RiskIQ. He stated this when asked how many COVID-19 domains they generally see in a day. Attackers usually leverage current events in their operations. Something as widespread and disruptive as COVID-19 has proven to be especially valuable to them, which is why we're seeing such a large-scale growth of COVID-19-related threat infrastructure".

Therefore, to move business, the executives must plan to prioritize operational capability towards eliminating malicious spam emails over the next two years. Likewise, researchers need to focus more on how to address malicious spam emails for resiliency in digital business.

1.14. Browsing apps

The COVID-19 pandemic has added new complexities to constraints in marketing, advertising and selling of business (Gursoy and Chi, 2021; Boiral et al., 2021; DiResta et al., 2020). It is difficult to break through the online clutter due to cautious consumers' opinions and a digital landscape inundated with an onslaught of news. As consumers stay at home, out-of-home marketing, advertising and selling become obsolete, and significant events are pushed back or pushed into a virtualized environment, a robust digital strategy is essential. The following use cases are gaining traction to enhance marketing, advertising, and sales for businesses:

(1) Live transaction data, consumer intent information, usage, and other digital datasets are used in real-time churn analytics (common in B2C, increasing use in B2B).
(2) AI-based lead creation and prioritization to find top customers and the relevant product/service requirement (B2B technology, professional services).
(3) AI-based pricing that takes into account dynamic cost changes (labor, materials, etc), market trends (competition, sector preferences), and internal price history (B2B technology, industrial goods, and telecommunications).
(4) Using webcasting as a vital marketing tool from home, by staff, with influencers to shift buyers online and distinguishing companies from home, through staff, with influencers, that is retail, food & beverage.
(5) Given WFH and rising online demand, hyper-local online marketing is extremely important across sectors of businesses.
(6) AI-assisted sales assistants assist customers who are mostly first-time buyers with buying online (retail) and a simple walkthrough of technical requirements of industrial equipment.

Therefore, research should focus on managers to plan operational ability in the direction of developing digital browsing apps towards marketing, advertising, and selling in order to take the organization forward and enhance cyber efficiency and safety for advancement in business.

1.15. Mobile apps

A mobile application, often known as an app, is a software application or computer program that runs on a mobile device such a laptop, tablet, phone, or smartwatch. Some organizations

use mobile device management systems (MDMS) applications to manage their employees' mobile devices by allowing system administrators to remotely deliver certificates, programs, access-control lists, and wipe stolen devices. After a security researcher told the vendor about issues patched in July 2020, many threat actors attacked one MDM, particularly MobileIron. CVE-2020-15505 and CVE-2020-15506, two of the three vulnerabilities, were rated critical with a CVSSv3 score of 9.8. The other vulnerability, CVE-2020-15507, was given a strong grade and a CVSSv3 score of 7.5. Exploiting these CVEs would result in remote code execution, authentication bypass, and unauthorized file reading, among other security problems.

During the spike of COVID-19 and the lockdown, cyber-attackers target mobile phones. For example, the computer emergency response team of India (CERT-In). The federal organization charged with combating cyber threats and protecting India's cyber space, has published a new advisory containing over a dozen recommendations for keeping personal mobile phones safe and secure.

2. Existing work

Many aspects of life have gone online as a result of the widespread adoption of digital technologies, ranging from commerce and social connections to business, industry, and, sadly, criminality. According to the most recent reports, cybercrime is increasing in frequency and severity (Lallie et al., 2021; Auyporn et al., 2020), with a forecast of $6 trillion in revenue by 2021 up from $3 trillion in 2015 (Adeyoju, 2019). It may even overtake traditional crime in terms of volume and cost (Netherlands, 2020). It is apparent that cybercrime may continue due to its profitable nature (McGuire, 2018) and low-risk level since cyber-criminals can launch assaults from anywhere on the planet.

Cybercrime, like traditional crime, is usually portrayed by the crime triangle (Khweiled et al., 2021), which stipulates that three variables must exist for cybercrime to happen: a victim, a motive, and an opportunity. The victim is the person who will be attacked, the motive is what motivates the criminal to perform the crime, and the opportunity is when the crime will be committed. For instance, it can be an innate vulnerability in the network or an unprotected system. Other criminological models include Routine Activity Theory (Yar, 2005) and the fraud triangle (Cressey, 1953). Employ similar factors to characterize crimes, with some replacing the victim with the attacker's means, which can be viewed as part of the opportunity.

Phishing attacks can take several forms, including email phishing, phishing websites, and phone phishing, popularly referred to as vishing. There are various types of phishing attacks, which are; Email phishing, Domain spoofing, Vishing, Smishing, Search engine phishing, Whaling, CEO fraud, spear phishing, Deceptive phishing, Pharming attack and Malware-based phishing.

2.1. The different types of phishing Cyber-attacks

The following are the most popular types of phishing cyber-attacks. They have been used in the past and are still being used to target unsuspecting people and organizations.

(i) Email phishing: Email phishing is a type of phishing assault. They frequently include harmful attachments and URLs that are designed to steal a victim's personal information.
(ii) Domain spoofing: In this form of phishing attack, attackers imitate prominent domains and aim to deceive users.
(iii) Vishing: In Vishing, the attacker calls the target on the phone and pretends to be someone from an organization with whom the victim is affiliated to obtain information from their target.
(iv) Smishing: Smishing is similar to Vishing; however, it occurs via text messaging.
(v) Spear Phishing: One of the most dreaded but powerful phishing strategies is spear phishing. Instead of arbitrarily targeting people, it selects individuals, conducts detailed studies on them, and then sends phishing emails to obtain related information from an organization.
(vi) Search engine phishing: This entails constructing bogus websites and webpages that can be accessed by typing specified keywords into search engines. People rarely hesitate to enter their private details on these pages since they look completely trustworthy.
(vii) Whaling: Whaling is similar to spear-phishing in that it targets the organization's top executives rather than simply any employee. It usually targets high-profile members of a company, such as the CEO and CFO.
(viii) The Chief executive officer (CEO) fraud: is a deception in which cybercriminals spoof business email accounts and impersonate CEOs in order to dupe an accounting or human resources (HR) employee into giving out private tax information or making illicit wire transfers.

The Federal Bureau of Investigation (FBI) refers to this type of scam as "BEC," or "Business Email Compromise." It defines it as "a sophisticated scam targeting firms that engage with international suppliers and/or make frequent wire transfer payments." The fraud is carried out by using computer intrusion or social engineering tactics to compromise legitimate company email accounts to make illicit financial transfers".

(ix) Deceptive phishing: The most common phishing fraud is deceptive phishing. Fraudsters pose as a real company to obtain people's personal information or login passwords. Attacks and a sense of urgency are used in these emails to terrify recipients into doing what the attackers want.
(x) Phishing based on malware. This technique occurs when a thief attaches a destructive computer program that appears to be useful to websites, emails, and other electronic documents on the Internet. Phishing based on malware or Malware based phishing is a form of a computer program that is also known as malware.
(xi) Phone phishing or voice phishing: is the practice of making false phone calls in order to dupe individuals into donating money or divulging personal information. It's a new label for a problem that's been around for a long time: phone scams. A common phishing method is for a criminal to pose as a trustworthy institution, organization, or government agency.
(xii) Pharming attack is a type of cyberattack in which users are directed to a false website that appears to be a genuine website. When users type in a legitimate web URL, they are led to a false website that looks exactly like the original one.
(xiii) Phishing websites: A phishing website is a domain with a name and appearance similar to an official website. They are designed to deceive someone into thinking it's real. Some pointers on how to spot a phishing website include; (a) visiting the website directly, (b) avoiding pop-ups and insecure sites. (c) keeping a close eye on the URL or web address. (d) Entering a fictitious password. (e) examine the website's content and design. (f) looking at online reviews and the payment options available on a website.

2.2. A monthly cyber-attacks during the COVID-19 pandemic

On a monthly basis there are incidences of cyber-attack during the global crisis of COVID-19. These incidences of cyber-attack

Table 3
A Summary of Monthly Cyber-attacks during the Covid-19 Pandemic.

Date	Country	Type of attack	Attack details
February 2020	United States of America	Phishing	On February 12, 2020, Puerto Rico revealed that a firm it owned had fallen prey to a phishing scam in a plot to steal $4 million.
February 2020	United States of America	Phishing	In February 2020, the personal information of 10.6 million MGM Resorts guests was hacked on a cyber-attacks forum. This included information such as tourists' names, phone numbers, addresses, email addresses, and birth dates as well as those of tech CEOs, celebrities, and government employees.
February 2020	United States of America	DDoS	Amazon detailed the attack in its first-quarter 2020 threat report, stating that it happened in the month of February (Musotto and Wall, 2020).
February 2020	China	DoS	DoS on COVID-19 epidemic prevention units (Lallie et al., 2021).
February 2020	Singapore	Phishing	Phishing cyber-criminals steals email log-in username, passwords and credentials (Pras, 2021; Kaspersky, 2020).
February 2020	Japan	Phishing / Malware	Safety measures phishing cyber-attack shares emotet malware (Walter, 2020).
March 2020	France	DDoS	The devices of a group of hospitals in Paris that play a key role in combating the COVID-19 crisis in the capital were the target of DDoS attacks that impacted access to computers and email (Pranggono and Arabo, 2021).
March 2020	Italy	Malware	Distribution of Trickbot Malware through email (Zahra et al., 2021).
March 2020	United Kingdom	Ransomware	The Maze ransomware group has leaked the medical and personal information of thousands of former patients of a London-based medical research firm that offers COVID-19 testing (Tuttle, 2021).
March 2020	United Kingdom	Phishing	It was a free school meal deceptive short message service that directed the recipient to the website that stole payment credentials (Sultana and Jilani, 2021).
March 2020	Czech Republic	Ransomware	The Brno University Hospital, one of the country's COVID-19 testing laboratories, was impacted by a cyber-attack and then was forced to shut down its whole information technology network (Kolouch et al., 2022).
March 2020	Vietnam	Malware	LOKIBOT malware spread through email, purporting incorrect invoice payments (Zahra et al., 2021).
March 2020	Spain	Ransomware	It was a disguised email Netwalker ransomware attack that advised people on the use of restroom use (Lallie et al., 2021).
March 2020	China Mongolia	Malware	Chinese hackers were suspected of spreading the Vicious Panda virus to Mongolia using emails ostensibly from Mongolia's ministry of foreign affairs (Lallie et al., 2021; Smzdm.com, 2020).
March 2020	United States of America	DDoS	United States Department of Health and Human Services, that is deeply involved in the COVID-19 issue, was the victim of a DDoS attack (Lallie et al., 2021).
March 2020	Libya	Malware	Exfiltration of user's data using SpyMax malware through trojanized app (Rosso, 2020).
March 2020	Phillipines	Malware	It was a REMCOS malware communicated on the Internet in the Philippines at the early stage of lockdown (Zahra et al., 2021).
April 2020	Worldwide	DDoS	Credentials of World Health Organization Officials were Leaked (Khan et al., 2020; Ahmad, 2020).
March 2020	United States of America	Malware	It was SMS that requested the recipient to take the COVID-19 preparation test to specific a website that downloads malware into a victim system (Sultana and Jilani, 2021).
April 2020	China	Phishing	Vietnam has been accused of conducting a METALJACK phishing attack against Wuhan district offices (Särökaari, 2020).
April 2020	United States of America	Phishing	Zoom was subjected to a severe cyber-attack in San Jose, California. Zoom Video Communications were the most talked-about cybersecurity issue in April 2020, just as the video meeting software has become a critical tool for daily business activities all over industries (Khan et al., 2020).
April 2020	United States of America	Phishing	Magellan Health has been a victim of phishing. Over a five-day period, attackers got access to an organization server containing highly sensitive employee data.
April 2020	United States of America	Ransomware	A Maze hacking incident attacked cognizant information technology solutions company on April 18, 2020, which hindered the service online for some customers.
May 2020	Taiwan	Phishing	Emails revealed an unauthorized connection hacking tool that impersonated Taiwan's top infection-disease official and urged recipients to go and get coronavirus tests (Chigada andMadzinga, 2021).
Phishing	UK	Phishing	People were directed to a counterfeit track and trace website that gathered the credentials of the victim (Mertoiu and Mesnita, 2021).
May 2020	Japan	Undisclosed but suspected to be DDoS	On May 7, Nippon Telephone and Telegraph (NTT), Japan's largest firm and one of the largest in the world, was the victim of one of the most recent cyberattacks. Until May 11, the attack on the Firm went unnoticed.
May 2020	Nigeria	Undisclosed but suspected to be DDoS and unknown scammers.	Scammers pose as real and well-known organizations such as banks, travel agencies, insurance providers, and telecommunications companies, and use various excuses around COVID-19 to: • Ask for individuals' personal and financial information. • Trick them into opening malicious links or attachments. • Gain remote access to their computer. • Demand payment for a spurious service or something they did not purchase. • Divert individuals' regular account payments to different bank accounts.Scammers have set up fictitious online stores claiming to sell products that do not exist, such as COVID-19 cures or vaccinations and face masks.
May 2020	United States of America	Ransomware	A group of hackers known as "Maze" stole and published sensitive data from the Asheville Plastic Surgery Institute, as well as a similar volume of information from a plastic surgeon in Washington state. Patient names, birthdays, insurance information, order forms, and before-and-after photos are among the information contained in the database.
June 2020	United States of America	Ransomware	The University of California, San Francisco (UCSF), which had been working on the COVID-19 vaccine, was indeed the victim of a ransomware attack and was compelled to pay $1.14 million to malicious actors known as Netwalker (Pranggono and Arabo, 2021).

(*continued on next page*)

Table 3 (*continued*)

Date	Country	Type of attack	Attack details
June 2020	Canada	Ransomware	On an Android smartphone, Crycryptor ransomware masquerades as COVID-19 contact-tracing apps (Sun et al., 2021).
June 2020	Germany	Phishing	Phishing emails were sent to senior executives at a firm that handles personal protective equipment (PPE). The phishing links take executives to bogus Microsoft login pages to steal their login information (Ramadan et al., 2021).
June 2020	Worldwide	Botnet	In the COVID-19 era, coming across a bot account while browsing through Twitter is more likely. Researchers at Carnegie Mellon University revealed that most of the discussion surrounding the covid-19 pandemic and stay-at-home authorizations is fueled by propaganda and misinformation that use plausible botnet (Dornan, 2020)
July 2020	United States of America	Phishing	The social media platform was hacked, and hackers verified the Twitter accounts of high-profile US figures such as Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and others (Aslan et al., 2020).

include phishing, DDoS, malware, ransomware, botnet, etc. A summary of monthly cyber-attacks is presented in Table 3.

Table 3 proved that the year 2020 was a tumultuous one, with daily life disrupted and huge changes in the corporate environment, all of which were exacerbated by increased Internet fraud as a result of the COVID-19 disaster. Most organizations are more reliant on the Internet than ever because many people are working from home or relying on their digital devices to keep them connected and entertained. However, the current cybersecurity trends demonstrate that hackers are taking full advantage of these COVID-19 crisis times, wreaking havoc on different organizations and their data more than ever before. Therefore, the year 2020 has had a huge impact on the most recent cyberattacks, including deadly phishing, malware, DDoS, botnet, APT and ransomware.

2.3. Timeline of cyber-attacks related to COVID-19

The cyber-crime episodes resulting from the COVID-19 pandemic constitute a severe threat to the global population's safety and socio-economy development. Therefore, understanding their mechanics, as well as their propagation and reach, is critical. Many techniques for understanding how such events evolve have been offered in the literature, ranging from formal definitions to systematic approaches to examining the nature of threats. However, while these methods allow for the categorization of an attack, they frequently lack the ability to map bigger, spread events like the ones described in this paper when the pandemic causes a slew of unconnected occurrences.

People increasingly work from home, attend digital school, and conduct business online to prevent the spread of the Coronavirus; practically every country in the globe proclaimed a state of emergency. However, during the COVID-19 crisis, almost all economic sectors were constantly under cyber security threats. Cybersecurity most affected economic sectors are highlighted and discussed in the subsection below;

2.4. Cyber-security most affected economy sectors

Hackers also use credential stuffing tactics to get access to employees' credentials, and the stolen information is again sold to other criminals in the digital black market. One of the effects is that firms that rely significantly on videoconferencing platforms will be severely disrupted. Credential stuffing is a type of cyberattack in which hackers utilize stolen login and password combinations to obtain access to all other accounts. Because it is fairly usual for people to use the same password and username for many accounts, this is conceivable. Cyber-attack most affected economic sectors are highlighted in Fig. 2.

The war on the digital economy during the lockdown caused by the COVID-19 health crisis cannot be over-emphasized. Therefore, cyber-attack most affected economic sectors are discussed as follows;

(1) Financial sector

The financial industry faced numerous cyber security attacks during the COVID-19 crisis. At 5.85 million dollars, the mean cost of cybercrime in the financial services business is also among the highest of any industry (ibm.com, 2020; Najaf et al., 2020; Bossler, 2021). It has compelled financial institutions like banks and insurance firms to continue providing online assistance to their customers. Again, the majority of employees worked from home in an insecure network. Once employees are at work, they are bound by certain security measures, which were not there before and which became the new normal practice. Employees were more vulnerable to cyber risks when using an insecure net-

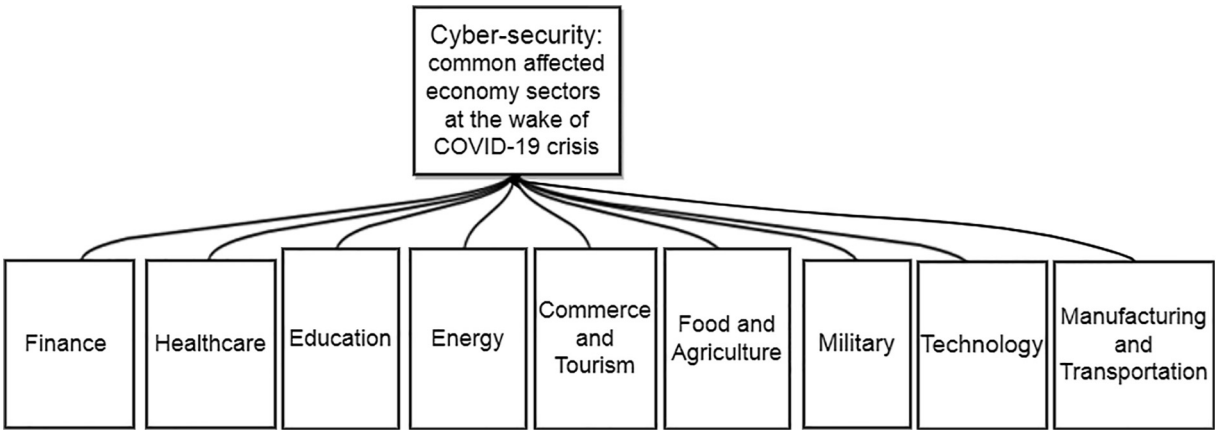

Fig. 2. Cyber-attack: most affected economy sectors at the wake of COVID-19 health crisis.

work (Babulak et al., 2020). Customers increasingly rely on online banking, which exposes them to hackers. Hackers commonly target the financial sector with distributed denial of service (DDoS), phishing, and malware cyberattacks. ATM transactions (Omolara et al., 2019a; Omolara et al., 2019b; Omolara et al., 2019c) were visited by hackers that stole bank credit cards to withdraw money. During the Covid-19 crisis, there was an increase in credit card fraud (Zhu et al., 2021; Payne and Morgan, 2020). Therefore, there is an urgent need to protect data from intruders by developing a hybrid cipher (Omolara et al., 2014) and up-to-date safe encryption algorithms to secure data in online transactions.

In the case of insurance firm cyber-attack, the Avaddon gang attacked the European insurance business AXA in May 2020. The incident occurred shortly after the corporation announced significant insurance policy modifications. In essence, AXA said it would no longer reimburse many of its clients for ransomware charges. The hacker group acquired access to a colossal 3 TB of data in this one-of-a-kind (and rather ironic) threat on a cyber-insurance corporation that made the news. Another significant insurance firm was hit by ransomware earlier in March 2020. On March 21, 2020, a hacker group targeted CNA's network, encrypting 15,000 devices, including many computers used by remote employees. The hacking group Evil Corp is suspected of being behind the attack, which uses a new strain of malware known as Phoenix CryptoLocker.

(2) Healthcare sector

A typical computer systems shutdown case occurred at Brno University Hospital due to a cyber-attack. The Brno University Hospital, is a significant Covid-19 testing site in the Czech Republic, was one of the first medical facilities obliged to turn away patients with serious illnesses and postpone surgeries. The World Health Organization (WHO) declared that cyber-attacks surged to fivefold during the COVID-19, causing public fear. Nearly 450 functional email addresses with a WHO username and passwords were compromised in the third week of April 2020 (World Health Organization. 2020). Hackers and invaders are well aware that the global healthcare system is in disarray as a result of the epidemic. Since more people use the remote care system, hackers were increasingly active in gaining access to healthcare systems all over the globe for financial benefit. Hackers attempted to gain access to a huge series of individual data and credentials of patients, according to the United States cybersecurity and infrastructure security agency and the United Kingdom's national cyber security centre (Lallie et al., 2021).

Throughout the pandemic, telemedicine became the only means to receive care. The treatment has made it easier for hackers to gather the needed information from specific patients. Before the pandemic, only 95 people in New York used telemedicine on a daily basis. However, during the disease outbreak, the number of patients surged by a factor of 44.30 times, and on a daily basis, nearly 4209 people used telemedicine. Ransomware assaults have increased dramatically as a result of these staggering numbers (Jalali et al., 2021). Different Cyber-attacks / data breaches in healthcare and academic organizations at the peak of the COVID-19 crisis, in Summary, is presented in Table 4.

(3) Education sector

The abrupt transformation induced by the COVID-19 crisis significantly impacted educational systems. Most students at all levels now rely on e-learning, putting them at risk of cybercrime. In addition, most educational institutions use applications like Zoom for their e-learning processes. However, because of the attack, for instance, some schools in California were compelled to suspend their program activities for a few periods (Harris and Jones, 2020). COVID-19's dreadful status jeopardized schooling at all levels. Education was also at risk as the pandemic spreads. Homebound students took classes through online e-tech systems, e-learning environments, and video-conferencing. Cybercriminals have hijacked video and teleconference sessions (known as Zoom-bombing) in the past to distribute unpleasant or dangerous content. Educational institutions should keep private information out of e-learning platforms. They should use a software-as-a-service (SaaS) solution rather than a local client. Furthermore, they should prevent third-party providers from having direct access, and evaluate vendors and their security documents on a regular basis.

In some countries like the United Arab Emirates (UAE), e-learning tools were deployed in higher education. For example, UNESCO supplied a variety of distant learning resources to assist many schools and organizations in adjusting to continuing their work during COVID-19 (UNESCO, 2020). Popular applications utilized to deliver lecture include WebEx, Zoom, Google Classroom, Ultra Collaborative, Skye, Blackboard Learn, GoToMeeting, Monitor Lockdown Browser, Respondus, amongst others. There are also many occasions where academic and non-academic staff and students communicate via social media platforms like Facebook, YouTube, WhatsApp, and others that offer online services that were used to promote education during the COVID-19 pandemic crisis. Thus, expert-led online courses were made available in English, French, Spanish, Italian, Portuguese, and other languages during the COVID-19 crisis.

Table 4
Different Cyber-attacks / data breaches in healthcare and academic organizations at the peak of COVID-19 crisis in summary as reported.

S/No	Date of cyber-attack	Country of Cyber- attack	Organization	Report and impact of the attack	References
1	13 March 2020	Czech Republic	University hospital in Brno	The IT network went down, causing important surgeries to be postponed and emergency medical services to be jeopardized.	(https://www.zdnet.com/article/czechhospital-hit-by-cyber-attack-while-in-the-midst-of-acovid-19-outbreak/).
2	13 March 2020	Worldwide	World Health Organization (WHO)	Making a rogue website that looked like the WHO's official email system in order to steal employee passwords. According to WHO Chief Information Security Officer Flavio Aggio, the attack was unsuccessful. DarkHotel, a gang of sophisticated hackers, is suspected by many sources, according to Reuters.	(https://tech.newstatesman.com/security/who-cyberattack-covid19).
3	14 March 2020	United Kingdom	Hammersmith Medicines ResearchGroup, UK (COVID-19 Vaccine Trial Group)	A ransomware attack resulted in the disclosure of previous patients' private details, as well as an unsuccessful attempt to deactivate the network.	(https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisationpoised-for-work-on-Coronavirus).
4	16 March 2020	United States of America	Health and Human Services (HHS) Department	HHS servers were subjected to an unspecified attack.	(https://tech.newstatesman.com/security/us-healthhuman-services-department-cyber-attack).
5	22 March 2020	France	Paris Hospital Authority (AP-HP)	An attack on AP-HP servers that has not been identified.	(https://www.bloomberg.com/news/articles/2020–0323/paris-hospitals-target-of-failed-cyber-attackauthority-says).
6	4 April 2020	United Kingdom and Spain	Healthcare Workers	An attempt was made to disable anti-virus software as part of a ransomware attack.	(https://www.computing.co.uk/news/4012969/hospitalscoronavirus-ransomware; https://www.digitalhealth.net/2020/04/neither-covid-19nor-cyber-criminals-care-who-gets-infected-andsuffers/).
7	13 May 2020	United Kingdom	ARCHER Academic High-Performance Computing(HPC) network	It was an exploitation of login nodes to force all user passwords to be rewritten	(https://www.theregister.com/2020/05/13/uk_archer_supercomputer_cyberattack/).
8	13 May 2020	United Kingdom	Bam Construct and Interserve (Companies who helped construct temporary COVID-19 hospitals for the UK's National Health Service)	Unknown type of attack	(https://www.constructionnews.co.uk/contractors/bamconstruct/bam-construct-hit-by-cyber-attack-13–052020/).
9	10 June 2020	Iraq	Babylon Health (Appointment and video conferencing software for NHS doctors)	Due to a software flaw, there was a data leak.	(https://www.mobihealthnews.com/news/europe/babylon-health-admits-gp-hand-app-data-breach-caused software-issue).
10	16 July 2020	United States, United Kingdom and Canadian authorities	Governments	It was unspecified state-sponsored cyber-threats on institutions developing COVID-19 vaccines are alleged.	(https://www.theguardian.com/world/2020/jul/16/russian -state-sponsored-hackers-target-covid-19-vaccineresearchers).

(4) Military sector

A coronavirus-themed malware has been reported to overwrite a computer's Master Boot Record (MBR), rendering it unbootable. ''Coronavirus Installer" is written in the malware file's description. Thus, the Covid-19 crisis and lockdown regulation was used as a trap by another Coronavirus-themed malicious HTA file (HTML executable file). It is most likely from the infamous SideWinder organization, which is known for targeting military targets. A pop-up PDF enticement with click-bait headlines and photographs of the Pakistan army is included in this HTA file. The CEOs and top executives of energy providers face a unique set of cyber and safety threats. Employees who use their residences to access crucial plant production and grid networks increase the likelihood of a second-wave crisis; rolling power outages and safety occurrences parallel when keeping the electricity or lights on is critical. The rush to remote systems, understaffed facilities, and new working modes will be exploited by attackers.

(5) Energy sector

In the energy sector, in times of crisis, such as COVID-19, the focus is on how to protect the public and how to maintain power flowing to customers. Working remotely is the most important priority for utility companies, but this fact also exposes the energy business to threats from inside and outside its cyber defenses. Energy companies must protect their employees and concurrently avoid outages since lives are on the line. Energy companies are facing new cyber-risks as a result of remote working. Attackers will look for new weaknesses in an energy's infrastructure to exploit. Utilities are fundamentally changing their power generation workflows, and cybersecurity approaches and structures will need to be updated as well. New operational models will be required for distributed energy sources. Likewise, remote work and automation will boost productivity. Energy businesses will have to educate and train the next generation of workers. The frequency and sophistication of cyberattacks against electricity will continue to rise. As each trend forms the new reality, electricity companies will need to iteratively update cybersecurity policies to protect operations. Then keep the lights on both in the short, middle and long term.

The hack of Colonial Pipeline in late April received the most media attention of all the cyber and ransomware assaults in 2021. ''The Colonial Pipeline attack had such an impact because the pipeline is an integral part of the national critical infrastructure system," says Joe Giordano, director of Touro College Illinois' Cybersecurity Program. Gas supplies were disrupted all along the East Coast of the United States as a result of the system's downtime, producing confusion and panic.'' Due to the fact that most Americans are directly affected by gasoline shortages, this strike touched close to home for many people. The attack was carried out the DarkSide gang, which targeted the company's billing system and internal business network, causing major shortages across many states. Colonial Pipeline finally caved in to the cyber-attacker's demands and paid the group $4.4 million in bitcoin to avert additional disruption. Luckily, much of the $4.4 million ransom collected was recovered by US law enforcement. The money was traced thanks to the FBI's monitoring of bitcoin transactions and digital wallets.

(6) Manufacturing sector

If manufacturing sectors were under the impression that they were protected from cyberattacks, that belief is gradually disproving, especially in 2020. In the years 2017 and 2018, more people became cognizant of Industry 4.0 and the rise of cybercrime. However, many companies in the sector were completely uninformed of the risks. By 2019, the manufacturing industry had risen to the eighth most targeted sector by cyber criminals. Due to the pandemic restrictions, many organizations were compelled to rely nearly entirely on remote labor in 2020, which exacerbated the problem. While most of the world was unprepared for COVID-19′s impact, cyber attackers were prepared. The industrial industry has slipped from eighth to second place in terms of cyber-attacks. Monitoring the company's network ecosystem for anomalies is highly significant in protecting against cyber-attack. Some security procedures are impossible to implement when working from home during the COVID-19 crisis. For example, both legitimate and illegitimate directives came from outside the company. It is difficult to tell what they are and their intention. As a result, monitoring becomes even more important to distinguish between attackers and employees.

Some monitoring and surveillance can be automated, allowing relevant employees to spend more time investigating suspected activity. Nevertheless, the threat to the nation's essential infrastructure and government organizations has not flown under the radar. Public institutions such as government parastatals are beginning to implement stronger restrictions for corporations that secure sensitive data, despite their poor response to cyber threats in the past. The Cybersecurity Maturity Model Certification and the IoT Cybersecurity Act were introduced in 2020 as ways to implement minimal cybersecurity rules for enterprises that deal with government organizations. Even so, the full impact of these laws will not be felt until 2022 or 2026. Meanwhile, cybercriminals will continue targeting organizations that have ignored warnings and failed to implement cybersecurity solutions.

However, there is just one answer for industrial companies looking to avoid risks. They need to learn about the potential cybersecurity risks for manufacturing companies and how to create a comprehensive cybersecurity solution to identify and prevent attack vectors before they breach the company network.

(7) Technology sector

The year 2020 and 2021 are years of the top significant data breaches ever globally. These breaches badly affected technology industries (information technology) such as Google, Twitter, Zoom, Amazon, Finastra, CDProjekt Red, SolarWind supply chain, etc. On its Chrome update page, Google stated that it is aware of exploits for two vulnerabilities, CVE-2021–38000 and CVE-2021–38003. However, both issues have been resolved, but only if Chrome users upgrade their browsers. ''The Stable channel has been updated to 95.0," Google verified the upgrade. Some well-known and well-respected Twitter accounts were hacked and exploited to spread false information about Bitcoin. The accounts asked for Bitcoin from their followers in exchange for a double reward. Despite the tweets being only active for a brief period, they made more than $100,000 in Bitcoin. Those who were tricked into transferring Bitcoin got nothing in return.

Zoom moved from a little-known boutique business to one of the most well-known and frequently used videos and audio conferencing systems almost overnight because of the quick increase in individuals working from home due to COVID-19. In Q2 2020, it had a factor of 3.55 times increase in revenue year over year. With such rapid expansion, Zoom had multiple security incidents, the most notable of which was the sale of over 500,000 user accounts on a dark web forum. According to reports, the accounts were accessed by utilizing user IDs and passwords that had previously been exposed in other breaches, a practice known as credential stuffing.

Finastra, a provider of software solutions company to financial institutions in many parts of the world, notably 90 of the top 100

banks, was hit by a ransomware attack that interrupted operations and forced the company to temporarily isolate compromised servers from the world wide web. Finastra has the US $1.9 billion in revenue, 9,000 + employees, and about 8,600 customers, with a global footprint and a broad set of financial technology products. Finastra likely have been a victim because of a history of issues pertaining to obsolete security practices and devices, like having four Citrix (NetScaler) servers vulnerable to CVE-2019–19781 operating in early January 2020, according to Bad Packets. This company monitors and helps in identifying cyber-security threats. Finastra said it employed "isolation, inquiry, and containment" to bring the case to court.

Other attacks were launched on CDProjekt Red, a well-known videogame studio in Poland. The HelloKitty gang hacked the company in February of this year. The hacker group gained access to source code for in-development games as well as encrypted gadgets. CDProjekt, on the other hand, has declined to pay the ransom and has backups in place to salvage the lost data.

In April 2020, REvil gang requested a $50 million ransom from computer manufacturer Quanta, similar to the Acer computer hack. Although Quanta is not a household name, it is one of Apple's most important business partners. REvil went after Apple when the company declined to negotiate with the hacker organization. They threatened to reveal more sensitive documents and data after disclosing Apple product blueprints taken from Quanta. REvil seems to have halted the offensive by May.

The biggest cyberattack in the year 2020 was the SolarWind supply chain attack that affected prominent private companies, including Microsoft, FireEye, Cisco, and NVidia, as well as multiple United States government organizations. Additionally, Amazon was the target of a massive DDoS attack by attackers.

(8) Tourism sector

Marriott hotel disclosed that personal information of about 5.2 million hotel guests was improperly obtained in 2020, marking the company's second major data breach in less than two years. Marriott is one of the leading hotels, with 7,300 hotel and resort locations in 134 countries. The visitor information was hacked in mid-January using login credentials from personnel at a franchised location, according to the firm, which was notified at the end of February 2020. Marriott has deactivated those logins and is cooperating with investigators. However, according to a statement, Marriott claims that the data breach did not affect their Marriott Bonvoy account passwords or PINs, emails, passport information, credit card information, address, and driver's license numbers.

(9) Food and Agricultural sectors

Ransomware victims in the food and agriculture sector face enormous financial losses as a result of ransom payments, lost output, and remediation costs. Companies may potentially lose proprietary data and personally identifiable information (PII) as a result of a ransomware assault, as well as suffer reputational damage. For example, JBS S.A., a Brazilian meat processing corporation, was hit by a cyberattack on May 30, 2021, rendering its pork and beef slaughterhouses inoperable. Facilities in Australia, the United States, and Canada, were all hit by the attack. A ransomware attack on an unidentified US farm in January 2021 resulted in a $9 million loss because of the temporary closure of their farming operations. The identified adversary targeted their internal servers by getting full administrator access via hacked credentials. In another incidence, a United States bakery firm lost access to its server, data, and apps in July 2021, disrupting production, shipping, and receiving (MSP) due to the Sodinokibi/REvil ransomware attack. The ransomware was delivered using software used by an IT support managed service provider. The bakery was closed for about a week, causing delays in customer orders and ruining the company's reputation.

In the case of agricultural farm cyber-attacks, for example, a popular agricultural farm in the United States lost $9 million in productivity after being forced to shut down due to a ransomware threat. It is ultimately up to the firm whether or not to pay the ransom, but it is crucial to note that paying does not mean the problem is solved. According to the FBI, up to 80 % of ransomware victims who paid the blackmail experienced a repeated attack, either from the same criminals or from a new group, after paying the ransom. Likewise, Australia's agricultural business faced cyber-threat according to a new AgriFutures Australia research that examines the cyber hazards following two major cyber assaults in the last 12 months. Most rural agricultural industries that fail to protect themselves from cyber threats endanger not only themselves but also Australia's food security.

(10) Transportation sector

The number of ransomware cyberattacks is rising across all industries, but the transportation industry appears to be the hardest hit. Transportation organizations are more adversely affected by the global cybersecurity gap than others because they have not traditionally deployed significant security teams to defend their digital assets. According to Cybertalk.org, the transport sector saw a 186 % spike in weekly ransomware attacks between June 2020 and June 2021. For example, new York's Metropolitan Transportation Authority (MTA), North America's largest transportation network, had been targeted by a cyber-attacker, according to sources in June 2021. Downstate New York is served by the MTA, as are two counties in southwestern Connecticut. The transportation system handles about 11 million passengers on weekdays, and over 850,000 automobiles pass through the MTA's seven toll bridges. The MTA's network cyber-incidence was reportedly perpetrated by the Chinese attackers that allegedly used a zero-day vulnerability in a remote access product from Pulse Connect Secure.

(11) Commerce sector

The demand for goods and services has shifted to e-commerce. While the number of e-commerce in total retail in the United States climbed modestly from 9.6 % to 11.8 % between the first and second quarters of 2020, that is, from 9.6 % to 11.8 %, it jumped to 16.1 % between the first and second quarters of 2020. The trend in the United Kingdom is similar: between the first quarter of 2018 and the first quarter of 2020, the share of e-commerce in retail increased from 17.3 % to 20.3 %, before increasing dramatically to 31.3 percent between the first and second quarters of 2020. Similar trends can be seen in other places, such as the People's Republic of China, in which the share of online retail sales in cummulative net retail sales increased to 24.6 % from January to August 2020, from 19.4 % in August 2019 and 17.3 % in August 2018.

3. Methodology

Methodologically, this study started by looking for articles that looked at the overall ontology between COVID-19 and cybersecurity. Then, it was narrowed down to articles that looked at each affected economic sector, such as finance, healthcare, education, military, energy, manufacturing, tourism, technology, transportation, commerce, food, and agriculture. It searched various databases for papers connected to coronavirus OR COVID-19, including Science Direct, IEEE Xplore, Springer Link, PubMed, Willey, Emerald insight, Elsevier, and others, between March 2020 and

December 2021. The period under review was the peak period of the COVID-19 incidence. Thus, we explore literature for material that had been published regarding cybersecurity issues in organizations during the lockdown, movement restriction and COVID-19 crisis. However, this study eliminates any epidemiological articles and research that were replicated.

We used 300 articles covering a wide range of economic sectors mentioned earlier. It also encompasses changes in consumer behavior and business practices, employees, managers, ethical issues, and policy-related challenges. The goal of this study was to learn how organizations reacted during the outset of the COVID-19 pandemic, identify cyber-attacks, and analyze them in order to provide solutions based on best working and management practices. It delivers the following answers to the research questions: What is the impact of the COVID-19 epidemic on organization cybersecurity? What are the best cybersecurity techniques that corporations utilize for early pandemic response? How can organizations deal with a cybersecurity problem during a crisis?

Based on a scoping examination of relevant literature published on the subject, this research aimed to analyze the cybersecurity problems faced by various organizations. That is, published articles in journals, letters, newspapers, and magazines between March 2020 and December 2021. A scoping review, rather than a systematic review, is better for fast covering of broader subjects from publications with a variety of study designs without judging the quality of the studies considered (Arksey and O'Malley 2005). This strategy is also well suited to examining new challenges and informing policy changes (Colquhoun et al., 2014; Kastner et al., Peters et al., 2014). Therefore, the approach developed by Arksey and O'Malley was also applied in this study, which consists of five steps.

3.1. Identifying relevant articles

Two complementary search strategies were utilized to find relevant published articles; from mid-March 2020 to December 2021, a state-of-the-art examination of reports was conducted. Search engines: The table and timeline were created using a variety of search engines. These search engines were Google, Baidu, Yahoo, Qwant, DuckDuckGo, Bing, AOL., Ask.com, and Excite. Likewise, we utilized Search engines for research such as Google Scholar, Educational Resources Information Center, Microsoft Academic, Worldwide Science, Wolfram Alpha, and Refseek.

Keywords utilized: When compiling cyber-attack reports, a number of keywords have been used. The Google translation tool was utilized to translate non-English phrases (Google Translate, 2020). Additionally, independent sources were employed to validate the translation (Prates et al., 2020, Suhono et al., 2020). The criteria for locating reports have been established and presented in a manner comparable to existing evaluations in the cyber security literature. A search was conducted in the English language using the Eureka database, which specializes in print media, using the following keywords:

"COVID-19 OR coronavirus," "Organization and Cybersecurity" OR "Companies and Cybersecurity," "SME and Cybercrime and COVID-19″ OR "business and Cybersecurity or COVID-19," "manager and employee and COVID-19 and Cybercrime" OR "COVID-19 and Cybercrime," "COVID-19 and Cybercrime," Second, using the same terms, a Google News search was run to find other relevant articles. The first search results returned 4,874 potentially relevant articles. However, 3,012 of them were irrelevant, while 1,862 were included. The articles were examined again, and 1,102 duplicates were found. The methodical screening was the third step. The methodological screened number was 760. As a result of the methodological screening, 460 articles were found to be irrelevant for the study, and the final excluded articles were 60 because they were epidemiological studies. Therefore, 300 articles were found to be relevant for the study, as shown in Fig. 3.

3.2. Selecting relevant articles

The exclusion and inclusion criteria were created to aid in removing articles unrelated to the core study issue of analyzing the best practices used by organizations to manage the COVID-19 pandemic. Articles in the research describe corporate policies implemented expressly to address the COVID-19 crisis, focusing on North America, Europe, South America, Australia, Africa, and Asia. Furthermore, in order to be considered for the study, the article had to provide at least one concrete example of an organization's behavior, as well as the organization's name. Articles that only discussed broad corporate, social, or political topics or examined management perspectives on COVID-19-related issues were omitted. Finally, 60 articles were removed throughout the selection process, while 300 relevant articles were included out of 4,874 evaluated.

3.3. Selection criteria

The articles discussed in this paper are all mentioned in the 'References' section. Meanwhile, exclusion and inclusion criteria for reviewed articles are described in Table 5.

3.4. Data visualization

The data was analyzed and a data extraction grid was created using Microsoft Excel. Then, the sheet was divided into six sections: (i) general characteristics; (ii) design and (iii) cyber crisis impacts; (iv) organizational techniques for cybersecurity management practices; (v) organizational methods for cyber-attack management; and (iv) preventive measures. Likewise, several articles were analyzed to develop the first draft of the list of cyber-attack types in the study.

3.5. Getting information, processing, and reporting

Meanwhile, an online questionnaire was taken to address the cybersecurity issues in many types of attacks. Then, 900 organization executives responded to the online questionnaire plan to prioritize operational capabilities to address the cybersecurity issues in many types of attacks. The information gathered from the corporate executives was analyzed. In the following sections, figures and tables were developed to reveal the study's primary findings. The percentage of articles discussing a given item under each category was also assessed, and the results are presented in the Figures and Tables in the next section.

4. Result

4.1. Result on the number of articles processed in the study

The article mapping gives an overview of the topic's publications, notably in terms of organizational cybersecurity challenges during the global Covid-19 crisis. The article's goals and emphasis on specific subjects, most notably business sustainability, are also important considerations. The examination of the sectors covered

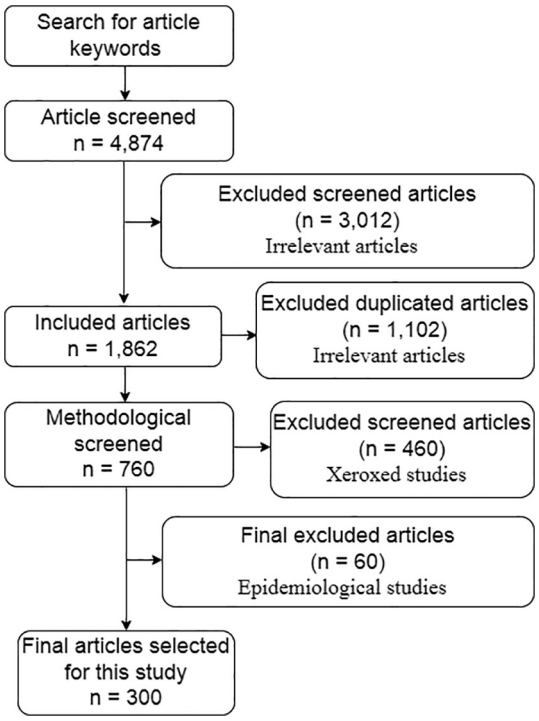

Fig. 3. Shows the screening and selection procedure for the articles.

in the articles reveals a diverse variety of activities and organizations involved in managing the COVID-19 problem and cybersecurity issues, as shown in Table 3. The analysis also highlights the crisis' breadth, as it impacts all sectors of the economy. The result of the number of articles processed in the review is summarized in Table 6.

Thus, Table 6 highlights the number of papers studied. After filtering and subsequent selection, three hundred (300) articles have been surveyed.

4.2. Result based on the percentages of screened and selected articles

The study removed 4,874 articles and 4,574 articles throughout the selection process. In comparison, 300 relevant articles were included, thus, accounting for 6 % of the included articles and 94 % of excluded articles, as shown in Fig. 4.

4.3. Results based on the types of cybersecurity questionaries' to participants'

The cybersecurity questionaries' to participants' was based on providing enough cyber threat knowledge. Every-one needs to be aware of the cyber security attack and risks in today's world. However, most people are uninformed of this issue, and many are unaware of the potential cyber risks. This is creating a vacuum in terms of preventing cyber-attacks, and cyber criminals are seizing the opportunity to further their nefarious goals. On a hundred persons, a survey was conducted to assess their understanding of cyber dangers. The outcome is displayed in Table 7.

Given the survey results in Table 6, it is evident that the majority of people are unaware of these issues, making it necessary to educate digital users on cyber insecurity. Users' awareness of cyber-security issues is urgently required to enable them protect and secure sensitive details in their devices. Likewise, organizations should prepare to educate their employees on cyber security problems by conducting training or workshops regularly. The government and agencies should provide similar training regularly for public consumption on radio and television. Furthermore, banks should help their customers take precautions against cyber criminals through constant text messages. To avoid losing their personal or organizational information, the general public should endeavor to gain a basic understanding of cyber security concerns and practise safety measures suggested by experts.

Table 5
Study exclusion and inclusion criteria.

Exclusion Criteria	• Irrelevant articles. • Xeroxed studies. • Epidemiological articles. • Relevant articles.
Inclusion Criteria	1- Published articles between March 2020 and December 2021. 2- English Language Write-up articles 3- Available or Found as full text. 4- Published articles in a peer-peer-reviewed journal. 5- Articles from reputable journals, conferences and letters, magazines, websites, news post and newspapers 6- Articles investigating cybersecurity issues during the COVID-19 pandemic.

Table 6
Result on the number of articles processed in the study.

Indexer	Search results	Excluded	Included
PubMed	470	398	58
Science Direct	384	275	23
Emerald insight	360	351	20
IEEE Xplore	375	365	18
ACM Digital Library	235	225	18
Directory of Open Access Journals (DOAJ)	280	264	12
Scopus	230	220	10
Compendex	260	255	17
Willey	225	220	11
Elsevier	228	220	15
Taylor and Francis	223	219	13
Springer Link	268	260	14
Academic Search Complete EBSCO Host	240	235	15
ERIC	225	220	9
World of Science (WoS)	223	213	11
Google Scholar	220	217	12
Journal Storage (JSTOR)	219	215	14
Others	209	202	10
Total	**4874**	**4574**	**300**

4.4. The background of the participants

Executives of organizations were among the respondents to the online questionnaire on plans to prioritize operational capabilities in order to address the cybersecurity challenges in many types of attacks. The analysis of the characteristics of the survey is shown in Table 8.

Table 8 reveals the background of the participants in the survey. Generally, there are more male participants than their female counterparts. The number of males accounts for 61 %, while that of females accounts for 39 %. The age group between 18 and 30 have the least participants, accounting for 10 %. However, the age group between 56 and above has the most participants, accounting for 30 %. The highest level of educational qualification of the participants was master's degree. But it was interesting to know that many of them are graduates and some participants have obtained

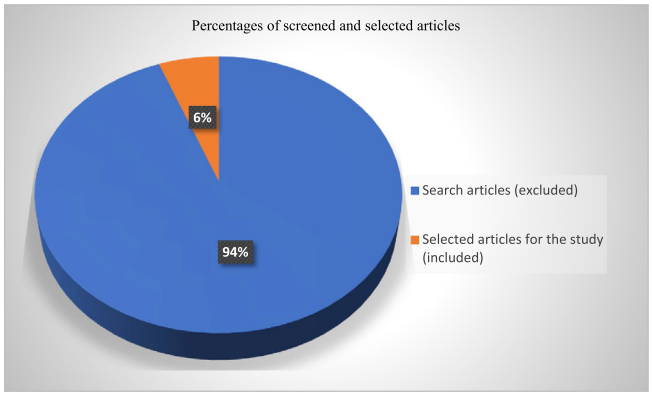

Fig. 4. Percentages of Included and Excluded Articles in the Study.

doctorate degrees. Experts and non-experts in cybersecurity both participated in the survey. However, it was observed that cybersecurity experts are business executives with significant numbers who made valuable contributions to the validity of this study.

4.5. Result on economic sectors and number of articles reviewed in percentage

Several economic sectors hit by the pandemic have been identified in the literature and by online interaction with the organization executives for the period under study, that is, from March 2020 to December 2021. This study explores the business types affected and the number of articles in percentage is presented in Table 9.

Table 9 revealed the main sectors of the global economy affected by cyber-attack during the COVID-19 crisis. The number of articles reviewed in percentage was calculated as follows; Finance (14 %), Healthcare (13 %), Information technology companies (12 %), Manufacturing (11 %), Transportation (10 %), and Education (9 %). Others include Energy (8 %), Food and Agriculture (7 %), Tourism (6 %), Commerce (4 %), Military (3 %), and Other sectors (3 %). The sudden lockdown of these industries for months has adversely affected their operational capabilities, but they have had to adjust rapidly, especially by creating telework, online sales, and delivery services.

Table 7
Result of the survey based on the types of cybersecurity questionnaires to the participants.

S/n	Question	Correct Answer	Incorrect Answer
1	What is Hacking?	36 %	64 %
2	What is DoS attack?	21 %	79 %
3	What is Phishing?	27 %	73 %
4	What is Malware?	18 %	82 %
5	What is APT cyber-attack?	18 %	82 %
6	What is Ransomware?	22 %	78 %
7	What is Botnet cyber-attack?	22 %	78 %
8	What is Spam Email attack?	22 %	78 %
9	What is Browsing Apps attack?	22 %	78 %
10	What is Mobile Apps attack?	22 %	78 %
11	What is DDoS attack?	30 %	70 %
12	What is Malicious Domain?	20 %	80 %
13	What are Malicious Websites?	40 %	60 %
14	What is Business Email compromise (BEC)?	23 %	77 %
15	What is Malicious social media messaging (MSMM)	36 %	74 %

Table 8
Result of characteristics of the survey.

Gender	Frequency	Percentages (%)
Male	552	61
Female	348	39
Total	**900**	**100**
Age group	**Frequency**	**Percentages (%)**
18–30	93	10
31–36	104	12
37–43	195	22
44–55	237	26
56 and above	271	30
Total	**900**	**100**
Educational qualification	**Frequency**	**Percentages (%)**
Undergraduate	104	12
First degree	317	35
Master degree	387	43
Doctorate degree	92	10
Total	**900**	**100**
Participants Area of Expertize	**Number of experts and non-experts in cybersecurity**	**Percentages (%)**
Cybersecurity	238	26
Non-Cybersecurity	662	74
Total	**900**	**100**

4.6. Result of the number of articles reviewed continentally and their percentages

This coverage on specific continents was due largely to the inclusion and specific criteria for the articles, specifically in terms of English language online contact. Notwithstanding, approximately-one-third of the articles had a global outlook and focused on measures put in place against cyber-attacks by big organizations and businesses in different countries or on the worldwide platform.

The articles primarily covered continent by continent and are arranged in alphabetical order: Africa, Asia, Australia, Europe, North America, and South America. The continental distribution of the organizations cited in the articles is shown in Table 10.

Furthermore, the number of articles in percentage per continent is highlighted in Fig. 5.

Fig. 5 reveals the percentages of continental distribution of the organizations cited in the articles. North America top the number of articles studied with 28 %. The next is Europe-based articles with 23 %, then Asia with 19 %, Australia with 12 %, Africa with 9 %, and South America with 9 % respectively.

4.7. Result of some cyber-attacks reported cases during the Covid-19 pandemic per month

A result of some cyber-attack cases reported globally during the COVID-19 pandemic between March 2020 and December 2021 can be presented in Table 11.

Furthermore, the result of some cyber-attack during the COVID-19 crisis, as highlighted in Table 10, between March 2020 and December 2021 is clearly shown in Fig. 6.

Table 9 and Fig. 6 revealed that cyber-attacks on the global economy were severe in certain months within 2020 and 2021. For example, cyber-attacks were severe between April and July 2020 and then slowed down from August to November but rose again in December of that year. In the following year, 2021, it became severe in January and February, then slowed down in March but rose again in April and May. Then, it slowed down gradually between June and September, then picked up again in October; and finally slowed down in.

Table 9
The result on the economy business sector and the number of articles reviewed in percentage.

S/n	Economy and business sectors	Number of articles	Percentage of number of articles
1	Finance	44	14
2	Healthcare	40	13
3	Information technology companies	35	12
4	Manufacturing	33	11
5	Transportation	30	10
6	Education	27	9
7	Energy	25	8
8	Food and Agriculture	20	7
9	Tourism industry	17	6
10	Military	10	3
11	Commerce	11	4
12	Other economy sectors	8	3
	Total	**300**	**100**

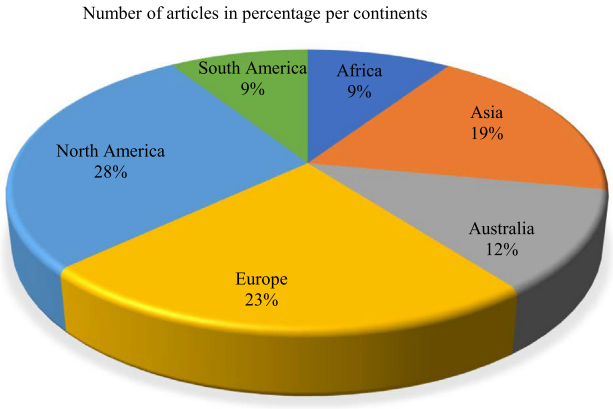

Fig. 5. Percentages of continental distribution of the organizations cited in the articles.

Table 10
Alphabetical order of continents, number of articles reviewed and their percentages.

S/n	Continent	Number of articles	Percentage of number of articles
1	Africa	28	14
2	Asia	56	13
3	Australia	35	12
4	Europe	70	11
5	North America	84	10
6	South America	27	9
	Total	**300**	**100**

4.8. Result of the respondents to the questionnaires on the main types of cyber-attack experienced during the COVID-19 crisis

This study explored the types of cybersecurity problems encountered at the wake of the COVID-19 crisis and analyzed the frequency of cyber-attack obtained from the respondent questionnaire. The analysis results are as follows: Malware was 7 %, phishing was 7 %, ransomware 2 %, distributed denial-of-service 6 %, browsing apps 6 %, malicious domains 9 %, denial-of-service 10 %, mobile apps 8 %, and malicious websites 10 %. Others are spam emails, capped at 13 %, malicious social media messaging 6 %, business email compromise at 4 %, APT at 1 %, Botnet attack at 2 %, and hacking attacks at 37 %. Therefore, the main types of cyber-attack reported, their frequency and percentages at the peak of the COVID-19 phenomena are summarized in Table 12.

Thus, organization executives look forward to prioritizing operational capabilities in cybersecurity and IT resiliency to boost business in diverse areas, as well as to increase profit. Even though many cyber-attack prevention mechanisms have been implemented, attackers often come up with some out-of-the-box scheme that can attack the network at all times. Some of the negative repercussions of falling victim to cyber-attacks include; (i) identity theft (ii) financial losses (iii) ransomware attack (iv) network slowdown (v) communication breakdown (vi) data loss breakdown (vii) data leak (viii) information breach (ix) network breakdown (x) loss of customer (xi) business bankruptcy and failure, etc.

Many types of cyber-attacks that occurred during the COVID-19 crisis were analyzed, and the result is presented as follows;

4.9. Result on the types of most common cyber-attack between March 2020 and December 2021

Different organization executives responded to the online questionnaires, which investigated the plan to prioritize operational capabilities in addressing cybersecurity issues in the next two years. The questionnaire's data was evaluated and the result was obtained. About 900 organization executives were contacted online to answer questionnaires designed on plans to prioritize operational capabilities to address the cybersecurity issues in the next two years. Interestingly, a large proportion of them responded. That is, 895 out of 900 organization executives responded to the online questionnaire plan to prioritize operational capabilities to address the cybersecurity issues in many types of attacks as listed in Table 13.

Table 11
Result of some cyber-attack cases reported during the Covid-19 pandemic per month.

S/n	Months	Number of reported cases of cyber-attacks globally at the wake of COVID-19 in the year 2020	Number of reported cases of cyber-attacks globally at the wake of COVID-19 in the year 2021
1	January	–	800
2	February	–	780
3	March	300	650
4	April	750	750
5	May	700	700
6	June	580	580
7	July	500	560
8	August	300	550
9	September	300	500
10	October	280	580
11	November	400	540
12	December	420	530

895 out of 900 organization executives that responded to the online questionnaires planned to prioritize operational capabilities to address the cybersecurity issues in many attacks, as listed in Table 13.

Table 13 was further analyzed to produce a graph for more clarity. Therefore, organizations' executives planning to curb certain types of cyber-attack in the next two years was in the following hierarchical order as presented in Fig. 7.

Fig. 7demonstrates that business executives plan to prioritize operational capabilities in cybersecurity to advance ICT resilience, sustain business and maximize profit. According to the analysis of the collated questionnaire, about 135 respondents out of 900 business executives that participated in the online interview planned to mitigate cyber-hacking in their organizations. In contrast, 110 business executives want to focus on reducing cyber-phishing that affected their operations during the COVID-19 crisis. Meanwhile, 90 business executives want to concentrate on tackling business

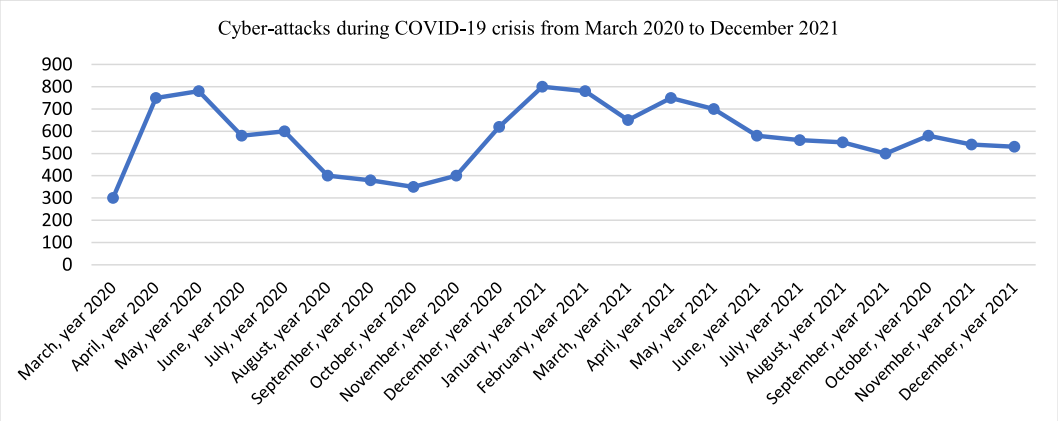

Fig. 6. Cyber-attacks during the COVID-19 crisis between March 2020 and December 2021.

Table 12
Results on the main types of cyber-attacks, frequency of attack and percentages between March 2020 and December 2021.

S/n	Types of cyber-attack	Frequency of attack	Percentages of attack
1	Phishing	140	7
2	Malware	131	7
3	Distributed denial-of-service (DDoS)	123	6
4	Ransomware	40	2
5	Browsing apps	125	6
6	Denial-of-service (DoS)	122	6
7	Malicious domains	168	9
8	Mobile apps	150	8
9	Website apps	121	6
10	Business email compromise (BEC)	70	4
11	Malicious social media messaging (MSMM)	119	6
12	Advanced persistent threat (APT)	25	1
13	Botnet	35	2
14	Hacking	330	17
15	Spam emails	250	13

email compromise (BEC) attacks that paralyzed business activities in their organization during the COVID-19 crisis. Moreover, 80 business executives want to address the issue of spam emails that are predominant in their organization's network during the COVID-19 crisis. Likewise, 72 business executives promised to eliminate common malicious domain network attacks that have beclouded their organization's cloud computing.

Similarly, 65 business executives vow to stop malicious mobile apps causing vulnerability in their organization's Internet infrastructure. DDoS and DoS are other cyber-attacks that 115 business executives planned to extenuate within the next two years. Malware is a deadly type of cyber weapon that 49 business executives plan to palliate in their different organizations over the next two years. Ransomware is also an exploitative type of cyber-attacks that 40 business executives are planning to counter in their organizations within the next two years. Finally, botnets are a dangerous type of cyber-attacks that 35 business executives planned to mitigate in their various organizations in the next two years. Interestingly, 30 business executives wanted to resolve the problem of malicious browsing apps, and 28 planned to prioritize operational capabilities to curtail vulnerable website apps.

Moreover, over the next two years, 25 organization executives planned to handle malicious social media messaging (MSMM) troubling their digital network. Furthermore, 21 business executives seek to address the challenges of APT attacks in their organizations in the next two years.

Table 13
Result of the number of organizations' executives plan to minimize certain types of cyber-attacks in the next two years.

S/n	Type of cybersecurity challenges	Number of organization's executives planned to minimize a type of cyber-attack	Percentage of organization's executives planned to minimize a type of cyber-attack
1	APT	21	2
2	MSMM	25	3
3	Website apps	28	3
4	Browsing apps	30	3
5	Botnet	35	4
6	Ransomware	40	5
7	Malware	49	6
8	DoS	55	6
9	DDoS	60	7
10	Mobile apps	65	7
11	Malicious domains	72	8
12	Spam emails	80	9
13	BEC	90	10
14	Phishing	110	12
15	Hacking	135	15
	Total	**895**	**100**

4.10. Result on types of most common phishing attack

Many types of phishing attacks that occurred at the peak of the COVID-19 crisis were analyzed, and the result is summarized in Table 14.

Although many email phishing prevention mechanisms have been implemented, attackers often come up with some out-of-the-box email phishing scheme that manages to mislead people at all times. The following are some of the negative repercussions of falling victim to phishing emails: (i) identity theft, (ii) financial losses, (iii) ransomware attack, (iv) economic slowdown, and (v) communication breakdown.

Therefore, the types of phishing attacks that occurred throughout the epidemic and their percentages are depicted in Fig. 8.

Therefore, the various types of phishing attacks that occurred throughout the epidemic, as well as their percentages, is presented in Fig. 8. According to the data breach investigations report, one out of every 14 people clicked on a link or opened an attachment

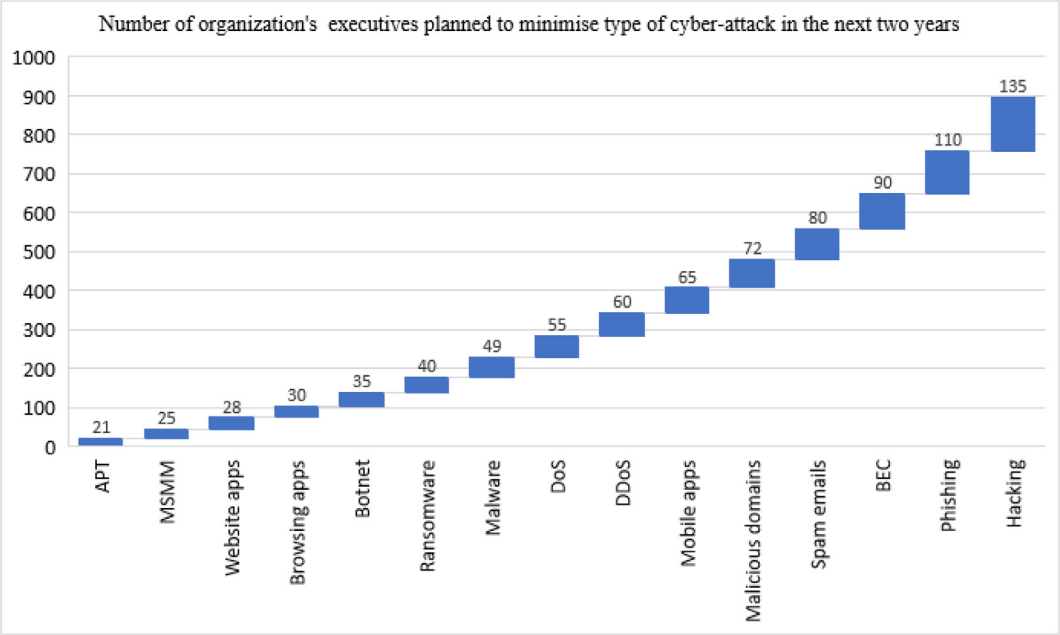

Fig. 7. Number of organization executives planned at minimizing difference cyber-attacks to advance ICT resilient.

in a phishing message. Likewise, a report from the BBC news on April 13, 2020, focused on how hackers are preying on Covid-19′s fears, as phishing emails were discovered and used in French, English, Italian, Turkish, and Japanese to attack people. As a result, individuals, as well as businesses such as aircraft, transportation, manufacturing, hospitality, healthcare, and insurance, are being targeted by cybercriminals. In addition, security experts noted that an increase in email frauds tied to the coronavirus is the worst in recent years.

4.11. Result of the main objectives of the articles reviewed

The main objectives of the articles reviewed can be summarized with analyzed results. The result of the main objectives of the articles reviewed can be summarized as depicted in Table 15.

Table 14
Types of phishing attacks between March 2020 and December 2021.

S/n	Types of phishing attacks	Frequency of attacked	Percentages of attacked
1	Email phishing	40	22
2	Domain spoofing	15	8
3	Vishing	12	7
4	Smishing	10	6
5	Spear Phishing	11	6
6	Search engine phishing	8	4
7	Whaling	7	4
8	Mobile phone phishing	20	11
9	Website phishing	15	8
10	Browsing phishing	10	5
11	Pharming attack	10	5
12	Deceptive phishing	25	14
	Total	**183**	**100**

5. Discussion

The goal of this study was to examine the effect of cybersecurity on organizations during the global COVID-19 crisis using a scoping review of relevant articles published on this topic in journals, conferences, magazines, media broadcasts and newspapers between March 2020 and December 2021. The study's analysis of the 300 articles provides the challenges faced by organizations, companies, small and medium scale (SMEs), as well as a global view of the major initiatives in this new and unusual situation, which frequently calls into question the possibility of "business as usual" and may even threaten companies' survival.

The article contributes significantly to the emerging literature on pandemic management in organizations. To our knowledge, it is the first systematic study of the practical measures implemented by businesses during the pandemic, based on a large number of concrete examples. The current literature on the COVID-9 crisis is based on health and medical rather than a business managerial perspective, and studies focusing specifically on business are still few. These studies tend to concentrate on specific industries and economic sectors, such as finance, healthcare, education, manufacturing, transportation, IT, energy, commerce, tourism, etc.

The data was generated from the global survey through online contact and responses, especially from the distinct organizations and business executives, revealed differences in cyber-attack techniques. After evaluation, the result showed that hacking attack was most frequent, with a record of 330, accounting for 37 % of the overall attacks. The second was spam emails with an attack frequency of 250, which account for 13 %. The third was Malicious domains, with 168 attacks accounting for 9 %. Finally, mobile apps with 150 attacks accounted for 8 % of the total attack, as earlier presented in Table 2. However, APT attacks recorded 2 % as the least common type of attacks leveraged during the global COVID-19 crisis for the period under study.

In general, 99 % of organizations and their executives intend to prioritize cybersecurity over the next two years. However, 15 % of organizations and their executives intend to focus on reducing hacking attacks, which were most frequent in the period under review. Then, 12 % of the respondent vowed to concentrate on reducing Phishing attacks, and 10 % set priority on BEC attacks. Next was spam emails with 9 %, which executives intend to reduce, followed by Malicious domains 8 % which they planned to minimize as presented in Table 8. However, 2 % are ready to minimize APT attacks in the next two years. In the future, the organizations

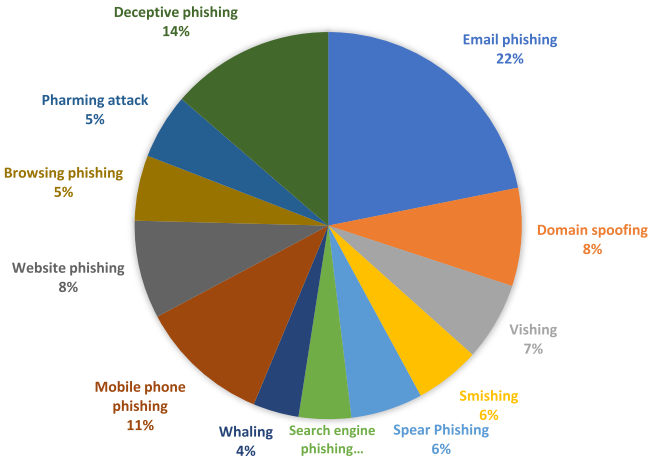

Fig. 8. Various Types of Phishing Attacks.

and their executives equally plan to use artificial intelligence to improve cybersecurity. Therefore, it is not surprising that the hacking rate was the highest type of cyber-attacks, which organizations and their executive priority is built upon in the next two years.

Similarly, 27 % of the respondents believed that email phishing was the most common among different phishing attacks and must be most critical. Mobile phone phishing was also found scary with 14 %, Domain spoofing and Website phishing attacks were each 10 %. However, search engine phishing and whaling recorded 5 % as the least common type of phishing threats during the global COVID-19 crisis for the period under study. A summary of implications, future research issues, and actionable insights of COVID-19 and cybersecurity is presented in Table 16.

6. Solution to the identified cybersecurity challenges

(i) Phishing: When malicious communications pass via the computer, anti-spam software and anti-phishing security can be employed to protect users. Other forms of threats are protected by anti-malware. anti-malware software, like anti-spam software, can be designed by software security experts to detect even the most evasive malware. Phishing is the leading cause of all cyber-attacks, and it continues to be one of the easiest ways to steal sensitive information and spread malware. MetaPhish, on the other hand, was built to provide an effective defense against these threats and allow businesses to determine how vulnerable they are to phishing.

(ii) Malware: Installing anti-virus software is one of the most fundamental strategies to protect against malware. Anti-virus software can safeguard valuable devices against harmful viruses that could compromise the system. It will run a scan on the computer to detect and remove malware such as viruses, as well as give automatic updates to improve protection against newly generated malware or viruses. Likewise, purchasing software applications from reputable sources reduce the risk of malware infection on the device. Big companies will take great care to avoid tarnishing their reputation by disseminating malware. One may verify a source's validity by looking at the entire name, list of published apps, and contact information in the app description on Apple or Google Play. The Malwarebytes Threat Intelligence Team (MTIT) needs to keep an eye on the threat landscape, especially for attempts that try to capitalize on the public's concern over the COVID-19 problem.

(iii) DDoS: Distributed denial of service (DDoS) attack prevention solutions can help protect IT infrastructure. Multi-level protection techniques are also required for computer networks and applications. This could include DDoS prevention management systems that include firewalls, content filtering, anti-spam, VPNs, and other security layers to monitor malicious activities and identify traffic anomalies.

Table 15
Result of the main objectives of the articles reviewed.

S/n	Article's Objectives	Number of articles	Percentages of articles
1	Challenges faced by organizations during COVID-19	9	3
2	Cyber-security challenges during COVID-19	10	3
3	Emerging cyber-attack issues in COVID-19	7	2
4	Implication of COVID-19 pandemic	9	3
5	Cyber-attack implication for governance	7	2
6	COVID-19 trends and security concerns	8	3
7	Cost of doing business and cyber-attack	7	2
8	The COVID-19 pandemic and trends in technology	9	3
9	Cybercrime during COVID-19	7	2
10	Reflection of COVID-19 crisis on business	8	3
11	Policy framework on business to curb cyber-attack during COVID-19	7	2
12	COVID-19 crisis implication on economic and cybersecurity	6	2
13	COVID-19 and cybersecurity problems, solutions and future	5	2
14	COVID-19, cyber-attack and types of business affected	7	2
15	Is COVID-19 changing the cybercrime landscape?	8	3
16	COVID-19 and cyber-attack disruptions of business	7	2
17	Digitization priority in business and emerging issues	6	2
18	Private sector in fragile and conflict situations during COVID-19	8	3
19	Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic	7	2
20	Technology adoption in emerging markets during COVID-19 crisis	9	3
21	Preparation for business resumption and cybersecurity	10	3
22	The long-term impacts of COVID-19 related cybercrime	7	2
23	The EU integrates COVID-19 into its long-term fight against disinformation	6	2
24	COVID-19 cyber security threats to MSMES	9	3
25	COVID-19 disruptions increase risk of cyber-attacks on MSMEs	8	3
26	Key cyber security risks for MSMES in the context of the COVID-19 crisis	5	2
27	Phishing and Business Email Compromise attacks using COVID-19 as bait	8	3
28	Malware distribution using COVID-19 as bait	6	2
29	Remote working and supply chain threats	9	3
30	2021 data risk report financial services	5	2
31	A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic	7	2
32	Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic	8	3
33	Cyber Security Threats During Covid-19 Pandemic	6	2
34	Cyber Security Attacks on Smart Home During Covid-19 Pandemic	7	2
35	Cybersecurity During COVID-19	8	3
36	Cybersecurity post-COVID-19: Lessons learned and policy recommendations	11	4
37	Distributed denial of service (DDOS) attacks	8	3
38	How Covid-19 is Dramatically Changing Cybersecurity	7	2
39	IT Risk and Resilience— Cybersecurity Response to COVID-19	8	3
40	Pandemic Parallels: What Can Cybersecurity Learn From COVID-19?	6	2
	Total	**300**	**100 %**

Table 16
COVID-19 and the Cybersecurity: A Summary of Implications, Future Research Issues, and Actionable Insights.

Work Domain	Implications	Issues for Future Research	Insight-Driven Actions
Emergent national lockdown, changes in the place of work practices at the wake of COVID-19 crisis and cybersecurity issues.			
Hacking	The lockdown measure and high rise in digital hacking have caused employees to lose control of their organization's network system. Organizations may protect themselves by sensitizing employees to be careful of hackers and also emails from unknown sources. Organizations like banks, schools, hospitals, airlines, restaurants, and supermarkets must adopt the best cybersecurity practices to sustain post-pandemic business.	What are the strategies that an organization such as bank, school, hospital, airline, restaurant, and supermarket need to put in place to prevent malicious cyber-criminals such as hackers? How will increase in hacking policies affect employee attitudes to work and behaviors to their employers? How will an organization invest in technologies such as cloud computing, Internet of things, artificial intelligence, and blockchain, to detect and prevent cyber-hacking even in a crisis situation like COVID-19?	Employees should build an innovative to mitigate vulnerability of hacker both in hardware and software system to avoid sudden loss of job of information or data breach. Organization managers in different sector of economy should adopt and encourage routines that will improve innovation and skill on how to mitigate hacking in various form to an atmosphere of confidentiality, integrity and authorization to data access. Governments could also implement a balanced method for ICT resilient in business and economy with new policy that will include lesson learn from hacking attacks in COVID-19 crisis.
Malware	Employees should learn how to mitigate Malware attack using software like anti-Malware and other professional strategy with critical decision-making in an uncertain environment. Likewise, employees who are compelled to work online especially on team projects need to navigate the indirect and direct conflicts that could result in performance losses through cyber-attack by Malware. Organization managers need to possess rapid adaptability to both survive and then thrive in business in unprecedented environment regarding cybersecurity.	What are the strategies that an organization need to adopt to prevent malicious Malware cyber-attack such as worms and viruses? How will one identify the features of cyber-attack like Malware? How will rapid adaptation to new security ideas or environment promote organization operation or progress? How will employees or customer's security awareness affect their emotional expression and team communication affect business resiliency, viability, sustainability or confidentiality? What are the methods that can help in dealing with cybersecurity in a complex, unprecedented, and change in doing business? How will these methods impact outcomes?	Employees team members need to pay attention to the ICT infrastructural security and nature of adaptation to new novel ideas or environment as well as communication flows with their managers. Likewise, employees team members need to pay attention to innovative ideas of customers, public opinions and experts advise. Furthermore, employees team members need to pay attention to stakeholders in the industry on how to reduce cyber-attack especially on how to identify Malware and counter it for business advancement. Organizations should enable opportunities for non-task interactions among employees and customers to build security and emotional ontology and confidentiality to continue among them. More also, organizations can better guide their security investments toward technologies with the largest potential cost savings. Furthermore, they can focus those technologies on the internal activities with the greatest strategic impact on improving cybersecurity protection.
Ransomware	Employee's must seek a novel approach to minimize data breach or data stealing which may lead to paying ransome of money to cyber-criminals. Managers/leaders are faced with new challenges to respond to cyber criminal's demand for ransome pay with high level decision than usual.	What are the strategies that an organization need to follow to prevent cyber-attack such as Ransomware? How will employees handle the issue of data breach or stolen data from an organization for financial benefit by the cybercriminals in a difficult situation like COVID-19 crisis? What are the best practices in handling the issue of data	Organizations and business leaders plan ahead on how to address ransomware attack to avoid loss or bankruptcy

Table 16 (*continued*)

Work Domain	Implications	Issues for Future Research	Insight-Driven Actions
	Organizations must seek ease way of dealing with call to pay ransome of money to cyber-criminals when sensitive data are stolen. A new security measure must be put in place to discover the cybercriminal without the need to pay money.	breach or stolen data from an organization for financial benefit by the cybercriminals in a difficult situation? How would the impact of data breach or stolen data and the ransome payment be on an organization like banks, schools, hospitals, airlines, restaurants, and supermarkets?	
Phishing	Countries with a sizeable developed Internet connectivity saw the greatest type of phishing attacks of the century at the peak of COVID-19 crisis. Business owners with a developed digital ecosystem can accelerate growth through phishing free environment especially in the period of upheavals.	What are the strategies that an organization need to adapt to prevent cyber-adversaries such as phishing? How will one identify the features of phishing cyber-attack? How will one carry out feature selection (Abiodun et al. 2021) of phishing cyber-attack? How will phishing attacks on digital technology adoption such as Internet affect business operation particularly crisis scenario? How will employees and managers shift to working from home and socializing through the Internet fast track phishing operation and detection business in crisis? What methods or technologies to apply in order to successful halt the phishing kind of attack during coronavirus or any crisis? How will technologies be applied to successful halt the phishing kind of attack during coronavirus and restoring normalcy in the society? How will phishing kind of cyber-attack have an impact on business or organization?	Phishing cyber-attacks may not allow users to have confident in the use of technology or build one's business all around customer which must not be ignored. Organization or business leaders must take advantage of being able to access the Internet to promote their themselves even at difficult time such as COVID-19 crisis.
Spam emails	The present COVID-19 crisis is wake-up call to organization about the awareness creation on common cyber-attacks including spam emails.Organizations should ensure all employees are training to identify common spam emails attack especially during crisis.It is vital for organization to improve the computer ecosystem that will be devour of threat. So that they can maximize profit, and optimize use of cloud based technologies to support remote management and monitoring of essential services.	What are the strategies that an organization need to put together in order to prevent cyber-attackers such as spam emails? How will one identify the features of spam emails? What are the best ICT tools that can be utilized to address spam email attack? How can ICT tools be used to address spam email attack? What are the technical measures that can be deployed by a staff and an organization to mitigate spam email attack?	Computer and online resiliency can be enable when pre-caution and pro-active measure against spam emails are adequately used in an organization.
Distributed Denial of Service **(DDoS)**	Individual and employees that utilize or maintain ICT infrastructure such as the Internet connections must take cognizant of DDoS cyber-attack and zero-day vulnerabilities. With the challenges of multiple cyber-attack reported at the peak of COVID-19, organizations should be highly concerned about the rising cybersecurity to demonstrate commitment towards network security, protection and safety.	What are the strategies that an organization need to deploy to prevent cyber-attack such as DDoS? How will one identify the features of cyber-attack such as DDoS? How will an organization address cyber-attack such as DDoS?	Employees and employers should be worried about increasing DDoS cyber-attack to show commitment toward their organization's computer network infrastructural security, protection and safety. Employers must be concerned about the sophisticated tools such as DDoS utilizing by the cyber –adversaries to disrupt business and cause loss.
Denial of Service (DoS) attack	Employees in banks, schools, hospitals, airlines, restaurants, and supermarkets need to learn how to use IoT systems to address state-of-the-art cybersecurity issues and they should conversant with cloud computing and DoS challenges. Management need to address DoS issue of non-compliances with latest technology that can drive organization operation for maximum advantages such as IoT devices, cloud computing and mobility as well as DoS cyber-attack.	What are the strategies that an organization need to adopt to prevent cyber-attack such as denial of service (DoS)? How will an organization invest in technologies such as artificial intelligence, Internet of things, blockchain, and cloud in order to recover from COVID-19 attacked?	Employees and employers must be concerned about the rising DoS cyber-attack to show commitment toward their organization ICT infrastructural security, protection and safety. Leaders must be concerned about the sophisticated tools such as DoS applying by the cyber-attackers to disrupt business and loss. Business leaders must be razor focused on commercial outcomes, work with the talent they have and trust the digital ecosystem.

(*continued on next page*)

Table 16 (*continued*)

Work Domain	Implications	Issues for Future Research	Insight-Driven Actions
Mobile apps	Employees need to understand how to build their skills to address emerging issues to meet employer's innovation demand and customers' needs specially in the use of mobile applications to solve emerging challenges. Organization's executives must know that enhancing operating-model resiliency in mobile apps will require adapting employee's skills and positions to post-pandemic modes of working to avoid sudden attack.	What are the strategies that an organization need to imbibe to prevent cyber-attack such as mobile apps attack? How can organization like banks, schools, hospitals, airlines adopt and promote procedures that increase trust of employees while keeping in mind the expenses of additional investment through mobile apps? How to address increasing long-term mobile apps damaged caused by cyber-attacked at the event of coronavirus crisis?	Individual or Internet users should create novel ideal to mitigate vulnerability of mobile devices through apps. Users of both in hardware and software system must avoid the use of any kind of mobile apps to eliminate loss of credentials or personal data breach. Organization executives should build manpower that will improve skill on how to mitigate attack in diverse form including the use of mobile apps. Governments could also implement a balanced method for ICT resilient with new policy that will include lesson learn from hacking mobile apps during COVID-19 crisis.
Browsing apps	Employees need to be innovative after COVID-19 incidence to bring new product to meet competitive market and consumer demands through reliable browsing apps which can improved customer retention and gain new customers.An organization like banks, schools, hospitals, airlines, restaurants, and supermarkets can gain from operational innovation of browsing apps by meeting consumer demands or demand, that will result in increasing market share or improve customer retention.	What are the strategies that an organization need to put in place to prevent cyber-attackers in browsing apps? How will an organizations such as banks, schools, hospitals, airlines gain from operational innovation by meeting consumer demands or demand, that can bring about increasing market sharing or promote customer retention?	Individual that utilize digital technology should seek a novel ideal to mitigate vulnerability of computer devices via browsing apps. Users of hardware and software system must be careful of using any type of browsing apps to avoid loss of information or data breach. Business managers must build manpower that will enhance skill on how to counter attack in various form such as the use of browsing apps. Governments could also implement a balanced method for ICT resilient with new policy that will incorporate lesson learn from hacking of mobile apps during COVID-19 crisis.
Website apps	Employees need to be innovative to bring new product to meet competitive market and consumer demands which can improve customer retention and gain new customers. Leaders must emphasize operational competence, such as fresh business entrance with a larger proportion of investment in ICT.	What are the strategies that an organization such as bank, school, hospital, airline, restaurant, and supermarket need to put in place to prevent cyber-attack such as website apps? How will employee's innovation bring new product to meet competitive market and consumer demands in order to enhance customer retention and attract new customers by effective website apps?	To achieve more success in business, managers must plan to prioritize website capabilities and control apps available on business website.To regain loss after the COVID-19 crisis, it is critical for companies to prioritize new website apps to retain old customers and gain new ones in to maximize profit.
Malicious domains	Employees need to be bring a novel ideal into online marketing, advertising, and selling Amid COVID-19. Managers must plan to emphasize operational ability in the direction of digital marketing, advertising, and selling in order to take the organization forward and enhance efficiency	What are the strategies that an organization need to put in place to prevent cyber-attack such as domain? How will an organization like banks, schools, hospitals, airlines, restaurants, and supermarkets identify software tool that can be used to promote digital marketing, advertising, and selling by preventing malicious domains? How will an organization apply software tool to digital marketing, advertising, and selling in order to promote business? How will digital marketing, advertising, and selling promote business?	Organization should begin investing in technologies such as artificial intelligence to detect malicious domains in cloud in computing in order to prevent early cyber-attack in a crisis scenario like COVID-19. As consumers stay at home, selling, advertising and out-of-home marketing becomes obsolete and, paramount events are pushed back or left in a virtualized platform, then a strong defensive digital strategy against malicious domains are critical for business to advance.
Botnet attack	Due to the sheer loss of social structure, social ties and, status unemployment has both economic and hidden consequences. Those who remain as workers in organizations that have laid off workers as a result of the COVID-19 issue face both direct and indirect losses. Employees and employer's relationship must be balanced to move business forward and optimize performance	What are the strategies that an organization need to put in place to prevent cyber-attack such as Botnet?What are the long-term effects of lack of job on mental health, and how can the jobless get job again? How does the COVID-19 pandemic changed an organizational working conditions and shattered employees and employer's relationship, but given room for government to have upper hand in the control of workforce?	As consumers stay at home working, advertising and out-of-home marketing and rendering services becomes outdated and, important events are delay or pushed away into an online environment, then a strong defensive digital strategy against botnet is essential for business to grow.Organization require perseverance and tenacity, and sustainability even in the multiple attack of Botnet need to seek for assistance and information from others. COVID-19 phenomena have significantly altered organizations working conditions and broken employees and employer's relationship and given room to cyber-adversaries to have an upper hand to destroy business using dreaded attack via botnet.

Table 16 (*continued*)

Work Domain	Implications	Issues for Future Research	Insight-Driven Actions
Malicious Social Media Messaging	Employees need to be alert of malicious social media messaging while bringing new social media messaging product to meet competitive market and consumer perspectives which can project customer retention and to gain new customers.	What are the methods that an organization such as bank, school, hospital, airline, restaurant, and supermarket need to put in place to prevent cyber-attack such as malicious social media messaging?	Individuals, employees and organizations must learn how to prevent falling victim to this scam, and be curious of emails purporting to come from trusted individual, organization and government, as they can be fraudulent.
	Organization managers must create awareness to employees on cybersecurity issues such as malicious social media messaging to avoid been a victim.	How will employees prevent falling victim of malicious social media messaging?	Organizations should avail themselves the opportunity to be connected to Internet to promote their businesses in legitimate social media platform and take precaution of malicious social media messaging even in a crisis period such as
		How will employee's innovation bring new product to meet competitive market and consumer demands in order to enhance customer retention and attract new customers by effective website apps?	COVID-19.To regain loss after the COVID-19 crisis, it is critical for companies to sanitize and train employees about the danger of business email scam.
Business Email Compromise	Employees need to be alert of business email compromise while enabling new product and services to meet competitive market and consumer perspectives which can encourage old customer retention and to accept new customers.	What are the procedures that an organization such as bank, school, hospital, airline, restaurant, and supermarket need to put in place to prevent cyber-attack such as **business email scam**?	Individuals, employees and organizations must learn how to prevent falling victim to this scam, and be curious of emails purporting to come from trusted individual, organization and government, as they can be fraudulent.To achieve more success in business, managers must plan to prioritize website capabilities and control apps available on business website and emails.To regain loss after the COVID-19 crisis, it is critical for companies to sanitize and train employees about the danger of business email scam.
	Organization managers must create unique environment to let their employees share knowledge on cybersecurity issues such as malicious business email compromise to avoid falling victim.	How will employees prevent falling victim of business email scam?	
		How will employee's innovation bring new product to meet competitive market and consumer demands in order to enhance customer retention and attract new customers by effective business email that can detect scam?	

Primary technical tools used to mitigate DDoS attacks are (1) Loading scripts onto load balancers to filter malicious traffic, (2) Web Application Firewalls, (3) Third-party BGP-based scrubbing, (4) Third-party DNS-based scrubbing, (5) Network blocks based on Layer 3 or 4 characteristics, (6) Upstream Filtering, (7) Connection rate-limiting, (8) Blackhole and sinkhole routing, (9) Packet/Session Time-to-Live (TTL) Restrictions and (10) Protocol/Port Filtering.

Operational control to mitigate DDoS attacks: The following operational controls should be employed to prevent DDoS attacks. (1) Attribution – organizations should engage their law enforcement partners and work with them during DDoS botnet takedown missions, which will increase understanding of adversary TTPS and aid in preventing future attacks.

(2) Lessons learned – organizations should prepare a detailed post-incident report, discuss lessons learned, and update incident response plans as necessary. Furthermore, lessons learned from the DDoS attack should be used to legislate on cyber-crime.

(iv) DoS: Firewalls are effective in preventing DoS attacks because they can help block the offending internet protocol (IP) addresses or the ports the adversary is attacking. However, this has the disadvantage of preventing genuine queries through those ports. Intrusion prevention systems (IPS) detect and refuse non-legitimate server requests. Another DoS attack prevention strategy is to scan the hard drive to detect Trojans on network connections and backdoors, as well as, educate users about the dangers of installing unknown software.

(v) Malicious Social Media Messaging: To avoid being hacked on social media, it is crucial to be aware of what is available to the general population on phone. Examine one's privacy options. Strangers should not be accepted as friends. There should be caution when checking in or sharing one's whereabouts with others. Tags for Personal review information should not be shared over the internet. Anything you would not want others to see should not be shared.

(vi) Hacking: Hackers masquerading as the world health organization (WHO) send messages to people's emails that an attached file explains how to stop the sickness from spreading. They say that "one small measure can cure the infected person." However, according to Proofpoint, the email attachment contains no relevant information, and instead, it will infect personal computers with malicious software known as AgentTesla Keylogger. AgentTesla Keylogger could record every keystroke and send it to the attackers, allowing them to track their victims' online activities. Therefore, to prevent falling victim to this kind or other variants of such scams, users or organizations must be skeptical of emails purporting to come from WHO, as they are sometimes fraudulent. Instead, users or organizations are advised to go to the organization's official website or social media outlets for the most up-to-date information. Individuals, organizations, and the government must invest more in cybersecurity to mitigate cyber-attack and better protect themselves during a crisis.

(vii) Business Email Compromise (BEC): Spear phishing or impersonating an internal email account is the most common BEC tactic. IT measures such as virtual private networks (VPNs) and application-based multi-factor authentication (MFA) can help to curtail, prevent or detect BEC.

(viii) APT: Selecting a firewall as the first line of security against APT operations is critical. The three most prevalent forms of firewalls are software firewalls, hardware firewalls, and cloud firewalls, all of which can help prevent APTs.

(ix) Mobile apps: Hackers deploy their own apps in the form of utilities, games, and other items that will monitor user behaviors and inputs behind the scenes. It enables them to steal various information, including what other apps the user has installed, network activities, the user's keyboard, and so on. However, to ensure

the security of mobile apps, users must encrypt source code, conduct penetration tests, conduct a thorough question and answer, ensure security check, and secure data in transit. Similarly, users should encrypt files and databases, provide data security provisions, apply the latest cryptography techniques, implement high-level authentication, and secure the backend.

(x) Browsing apps: Working in tandem with the behavioural firewall, intelligent browsing apps such as web application firewall (WAF) can protect against these weaknesses, preventing sophisticated and hazardous cyberattacks.

(xi) Spam emails: Marking spam emails as spam, deleting spam emails, and marking as spam are all simple techniques to help remove spam emails. Also, using a third-party spam filter and keeping email addresses private is a sure way to avoid spam mail attacks.

(xii) Botnet: re-install software, especially the operating system. Email attachments from suspicious or unknown sources should also be avoided. Most botnet malware will be prevented from ever being installed on a computer by a reliable antivirus, and it will typically be easy to delete if the computer is already infected. Some recommended brands are TotalAV, Norton, Bitdefender, and Malwarebytes.

(xiii) Website apps: Web applications frequently feature a whitelist and blacklist of requests to prevent these attacks, although these can also be evaded. The simplest approach to prevent this particular type of attack is to program web applications so that code cannot be executed or injected.

(xiv) Malicious domains: The attacker can construct their new malicious domains to put malware and avoid using the original websites of an organization to put malware. The term "custom or fake malicious domains" refers to domains established by attackers themselves that are unknown or well-known to most people and only exist for a brief time to avoid discovery.

Therefore, in order to avoid infection or attack from malicious domains, users must maintain their computers and update software regularly. When necessary, the user can use a non-administrator account before clicking on any links or downloading anything. When opening email attachments or photos, they need to take precautions. Pop-up windows that ask the user to download software are not to be trusted and must be scanned. Importantly, file-sharing should be limited.

(xv) Ransomware: A variety of good monitoring applications, frequent file backups, anti-malware software, and user training is required for effective ransomware attack prevention. Although no cyber-defense can totally eliminate threats, one can considerably lower the chances of an adversary succeeding. File recovery is one of the most remarkable ways to recover from a ransomware attack. Maintaining a safe, up-to-date backup of all important files is the most reliable strategy to evade a ransomware attack. For example, a known Acronis cyber protect home office can be used to back up files; it could actively strive to detect and prevent ransomware attacks.

7. Future projections

The study's key topics of projection and worry for the future are as follows:

(1) In the foreseeable future, there is a strong likelihood of an increase in cybercrime. Cyber attackers will continue to ratchet in their malicious activities and develop more sophisticated and advanced modi operandi due to the vulnerabilities associated with working from home and the opportunity for higher financial gain.

(2) To capitalize on public worry over the pandemic, cyber actors are expected to continue spreading coronavirus-themed internet frauds and phishing tactics.

(3) Due to the economic slump and shift in the business climate, business email compromise techniques are likely to increase, creating new opportunities for criminal activity.

(4) Once a COVID-19 vaccine is ready, there will undoubtedly be another surge in phishing attacks targeting medical products.

(5) People all around the world are becoming more reliant on the internet, which is opening up new chances for many businesses and individuals who are not keeping their cyber defenses up to date.

(6) There is a need for more private to public sector collaboration to effectively combat the threat COVID-19 brings to cyber security.

(7) BEC fraud is a constant threat to all enterprises, people, law enforcement, and society as a whole. Perpetrators' tactics are dubiously effective, and the financial losses sustained by businesses can be crippling. According to the information presented in this analysis, there is a global upsurge of fraud victimization and losses associated with fraud Internet Crime Complaint Centre (ICCC) and BEC fraud seem to be adopting that trend (Cross and Gillett, 2020).

(8) In addition, studies on the human consequences of BEC fraud are scarce. While the financial losses sustained by BEC fraud are well-known, little is known about the human and professional consequences of victimization. Currently, there is inadequate knowledge of how businesses handle BEC fraud in terms of both internal and external messaging. This is an area where best practice concepts that might be supported to improve an organization's reaction to BEC fraud could be identified. Analogous to data breaches, denial of the situation is unlikely to result in a successful future recovery.

(9) Data breaches have become an unwelcome aspect of the present world, and BEC fraud is no exception. Unfortunately, this will, without a doubt, continue to rise in the future.

(10) To more successfully tackle this crime category of BEC in the new decade, there is indeed a fundamental need for organizations and governments to invest in knowledge and research across both technology and human factors.

(11) Intelligence-gathering methods. Organizations should encourage the proactive use of cyber threat information to identify and address important indications of attacks (IOC).

(12) Risk control. Organizations can use governance, risk, and compliance (GRC) systems for better risk management. GRC solutions give you a clear picture of your company's risk exposure and help you connect the dots between different risk disciplines, for example, cybersecurity, operational risks, and business continuity.

(13) Be ready for an attack. Companies are recommended to conduct frequent cyber crisis simulation exercises to prepare for a cyberattack in these high-risk times.

(14) There is no such thing as zero trust. Organizations such as CISOs and CIOs should think about creating a zero-trust cybersecurity strategy. Only authorized and authenticated users and devices are allowed access to apps and data in this security paradigm.

(15) Another ransomware strain that could emerge in the future is one that explicitly targets backups. This would be quite troublesome because they are the only sure-fire ways to avoid malware. Ransomware has been discovered to attack intelligent thermostats, according to researchers. This ransomware could lock one's home or business's thermostat and only allow you to modify it if you pay a ransom.

(16) Immutable and distributed ledgers with auditable records are available with blockchain technology, making it suitable for tracking every asset in supply chain management. It relies on a distributed, private, secure, and immutable record-keeping system (Khurshid, 2020). Using blockchain, governments and hospitals may find COVID-19 suspected cases, places linked to reported cases, and infected areas with high risks. Blockchain has also been used to ensure healthcare data security (Hossain et al., 2020). Keeping track of patients and analyzing their symptoms or reactions to the disease is critical during the COVID-19 epidemic. Many countries affected by COVID-19, notably in healthcare, have found blockchain to be a helpful platform.

(17) Research should also focus on data exfiltration prevention, such as developing a cognitive model (Taofeek et al., 2022; Omolara et al., 2019a; Omolara et al., 2019b; Omolara et al., 2019c) that can deceive attackers who intend to steal data for ransoms, terrorism or any other purposes.

(18) More also different encryption schemes and techniques such as honey encryption techniques (Omolara et al., 2019a; Omolara et al., 2019b; Omolara et al., 2019c), enhanced one-time pad algorithms, quantum-based algorithms, amongst other state-of-the-art encryption schemes can be used to safeguide communicated and non-communicated data (Omolara et al., 2018a; Omolara et al., 2018b).

(19) Furthermore, more encryption schemes can be applied to secure patient information to thwart electronic health record threats based on decoys messages (Esther Omolara et al., 2020) to prevent access to malicious attackers, especially during a crisis. Therefore, more research should be focused on different encryption paradigms that address the challenges of unauthorized data theft and penetration by malicious attackers.

(20) Contact tracing or tracing based on quantum computing will be exponentially powerful in future studies (Slussarenko and Pryde, 2019). Artificial learning techniques and powerful computational intelligence tools like Monte-Carlo or particle filter tracking solutions may be included. Quantum sensing uses quantum entanglements' sensitivities to increase the timing, network synchronization, location precision, and accelerometer accuracy (Degen et al., 2017). Thus, leveraging such technologies will be a good line of action in these unprecedented times.

8. Recommendations

The following recommendations are considered as additional solutions to the cybersecurity initially identified for users of digital systems, which include first prevention strategies and second prevention strategies:

A. The First Steps in Preventing Cyber-Attacks.

(1) Step 1: The user should ensure that anti-virus software is updated on all devices.

(2) Step 2: Ensure the device's firewall is turned on.

(3) Step 3: Do away with any software that has been pirated.

(4) Step 4: Avoid accessing unfamiliar websites that may include phishing material.

(5) Step 5: The user should not save their username or password in the browser.

(6) Step 6: The user should not click on any email links until they have been ascertained safe.

(7) Step 7: Users can find security-certified websites; that is, those that begin with 'HTTPS://' are safe.

(8) Step 8: The user should not save credit/debit card information in the browser.

(9) Step 9: The user should always review the website address and double-check the address, whether it is a phishing site or not, before making a credit and debit card payment.

(10) Step 10: Users should not use the same password for all accounts.

(11) Step 11: Passwords must be sufficiently strong and not contain notable dates or numerals such as date of birth or private numbers.

(12) Step 12: Users should maintain the habit of installing a commercial operating system rather than pirated software.

(13) Step 13: Users should ensure that the system's operating system is updated.

9. Practitioner recommendations

It is important to know that the COVID-19 crisis period is for a limited time as huge measures are being taken to find a vaccine that will address the debilitating health issue. Nevertheless, the crisis period could compound an already difficult situation for information technology (IT) and cybersecurity.professionals. Therefore, it is necessary to adhere to several professional advice from experts that could assist in preserving the digital ecosystem during the COVID-19 health crisis following the cybersecurity implications.

(1) Protection against DDoS attacks. An organization must maintain the firewall turned on to minimize DDoS attacks. In addition, Ingress and Egress filtering can assist control overflow by detecting the origin of the Internet protocol range (Balas et al., 2020).

(2) Protection against phishing. Phishing attacks continue to unfold as a new danger for internet users. Cyber attackers send phishing emails with counterfeit website links to collect personal information and utilize it for financial gain. To minimize the risk of such attacks, having a good understanding of the modus operandi of phishing emails is essential. For example, clicking on phishing links is a bad idea. In addition, users should not provide their login information to vulnerable websites.

(3) Anti-malware protection. Malware attacks can be reduced by using up-to-date anti-virus gadgets. Nevertheless, there is a need for firmware updates to reflect the latest patch, and firewalls need to be enabled (Gounder and Farik, 2017).

(4) Anti-ransomware protection. Ransomware steals data from a device solely for financial gain. End-users have the option of using updated anti-virus software. Then, to avoid ransomware attacks, an upgraded operating system can give an updated patch file.

(5) Anti-hacking measures. The following precautions can be taken to avoid hacking. User must not reveal their login details or password to people. However, they should ensure that their Passwords are complex enough that they cannot be easily guessed. Account information should not be shared.

(6) It is necessary for educational institutions to keep private information out of e-learning platforms; the use of a software-as-a-service (SaaS) solution rather than a local client prevents third-party providers from having direct access. More so, vendors and their security documents should be evaluated regularly.

(7) A novel blockchain-based system might be provided to connect intercountry for COVID-19 and track infected or tested patients internationally. Similarly, developing a blockchain-based system for secure home quarantine administration may help curtail some of the challenges.

(8) One of the most advanced quantum applications is quantum communications (Manzalini, 2020). Therefore, improved cybersecurity in communications and greater privacy protection will almost certainly be one of its key benefits for tracing susceptible applications (Ahmed et al., 2020).

(9) Nowadays, cyber terrorism has increased. Therefore, there is an urgent need on how to prevent cyber-terrorism using modern

scientific approaches such as AI (Dilek et al., 2015), machine learning algorithms (Salih et al., 2021; Zhang et al., 2021; Naik et al., 2021), mathematical models (Oludare et al., 2018), forensic DNA profiling (Oludare et al., 2018) amongst others. Likewise, there is a need for increasing forensic investigation (Arshad et al. 2022; Arshad et al. 2020) into crime scene to searching for evidence that can be used for justice.

(10) Some businesses will have to switch to new operating models. To overcome the barriers in providing secure procedures for staff who work from home or are remotely linked, IT and cybersecurity rights would involve a careful investigation and prompt attention. Staff assistance and remote control would be essential. Before permitting the upgraded equipment to rejoin to the network, cybersecurity experts must ensure that people transferring from home to office are subjected to serious systems and access controls.

(11) Businesses will have to reset their security networks to ensure that there are no outliers. To assess any digital gaps in the firewall, physical and digital components must be reset. In order to support remote work, device and data access rights granted during the pandemic would need to be examined to see if they might be canceled or altered. IT infrastructure would have to be checked for flaws, improper routes, and forged identities. This is based on the discussion and findings from previous sections, as cybercriminals may have devised methods to gain access to regular security systems.

(12) Emerging cyber threats that have unfolded as a result of the outbreak must be understood. Security specialists would need to review their digital capabilities to ensure that key business activities can withstand cyber-attacks during a lockout. In addition, in order to ensure sustainability amid a health emergency, they will look into crucial supply linkages, particularly digital distribution networks.

(13) Organizations' security infrastructures should be reevaluated. This comprises re-assessing secure authentication tools, substantial remote access frameworks, risk and context-based secure authentication strategies.

(14) The security architecture of organizations should be re-evaluated. Secure authentication technologies, robust remote access mechanisms, and risk and context-based authenticating user procedures are all part of this.

(15) The security team would also have to share the lessons learned throughout the incident. This will help them design effective countermeasures in the case of a future epidemic. According to experts, security systems need to be re-calibrated, especially in terms of provision, scalability, remote management capabilities, and cloud-based dependability.

(16) Security team should collaborate with trusted stakeholders ahead of time in order to prepare for dynamic scaling, service delivery, and solution offering. Planning involves both creative and methodical thinking. Leaders are increasingly expected to use innovative methods and evaluate new functioning technology. Automation, especially, boosts operational efficiency while reducing the need for human interaction.

(17) Organizations will be forced to optimize expenditures and accelerate their digital revolutions as they adjust to the new normal post-crisis. These initiatives would need security leaders to adopt evolving technologies such as the Internet, IoT, Blockchain, 5G, and service models that have been adjusted to do more with less. That is crucial to operating in the most cost-effective way feasible.

(18) Anti-malware software detects and disables malware using behavioral heuristics analysis, signature detection, and, in certain cases, artificial intelligence. Anti-malware software should be deployed across every digital endpoint of an organization's network. However, ensuring that current anti-malware is properly deployed within all devices with network connectivity in today's age of bringing your own device (BYOD) workplaces might be challenging.

(19) Educational institutions should introduce courses on cyber security to create awareness for young students and researchers in the field of computer science in order to meet the future need on how to address the cyber-attacks challenges.

(20) Some essential '*must know*' cyber security measures must be introduced in a syllabus as a general mandatory cybersecurity course for students in all the higher education programme to provide more solutions in the field.

10. Conclusion

The contribution of this paper should, however, be considered in light of some limitations. First, our research is a general literature review with an informative purpose, which might suggest that there is a possibility of a subjective selection of literature. Notwithstanding, the databases we have used, such as PubMed, IEEE Xplore, Emerald insight, Willey, ACM Digital Library, Google Scholar, Semantic Scholar, and EBSCO, represent the most cited articles. Asides, the purpose and the informative nature of this paper do not require a systematic review of the literature. Secondly, during the conception and development of this paper, the COVID-19 pandemic is still ravaging. Therefore, it was not possible to accurately identify the long-term challenges and opportunities. Therefore, future research should be directed toward longitudinal analysis to identify these challenges and opportunities.

Selected articles included in the survey were from March 2020 to December 2021. Following the COVID-19 pandemic, it is vital for top executives to look internally rather than outwardly to prioritize operational competencies across key areas for the recovery of their businesses in the next two years. The data explored for this study came from an online global poll, and the responses, particularly from different organizations and business executives, highlighted variances in cyber-attack strategies. After analysis, it was discovered that hacking attacks were the most common, accounting for 17 percent of all incidents, with a total of 330 attacks. The second was spam emails, which accounted for 13 % of all attacks with a frequency of 250. Finally, malicious domains came in third with 168 attacks, accounting for 9 % of all attacks.

As seen in Table 3, mobile apps with 150 attack occurrences account for 8 % of all attacks. Throughout the global COVID-19 crisis, however, APT attacks were the least common sort of attack, accounting for 2 % of all attacks during the research period. Moreover, over the next two years, 99 percent of firms and their CEOs plan to emphasize on emanating cybersecurity issues. Also, 15 % of firms and their leaders plan to work on lowering hacking attacks, which were the most common throughout the study period.

With the proliferation of IoT devices, technological advancements, demand for access to sophisticated systems, and historical trends, DDoS attacks will expectedly grow in volume and frequency. Cybercriminals are expected to continue to seek and exploit vulnerabilities within these systems in an attempt to weaponize them for DDoS and RDoS campaigns. Plans to implement 5G capabilities coupled with recent and ongoing shifts to digitization by organizations have provided new grounds for intrusion by threat actors. It is imperative for organizations to remain vigilant in securing critical infrastructure by monitoring pre-existing and new technologies, ensuring new policies are being followed, and adhering to security best practices for managing enterprise networks and remote workforces.

The study focuses on current cyber challenges in the context of the COVID-19 pandemic. This pandemic has seen the most Internet

usage and attack ever. Many people worldwide use the Internet to continue their contact, businesses, education, and medical care, amongst others. This pandemic has put every-one's stress levels to the test. Likewise, people have also used the Internet to reduce their stress levels. This epidemic has demonstrated that people can perform their duty at home, go to school, and participate in other activities. However, cybercriminals have seized the opportunity to profit from the general public's widespread usage of the Internet. But due to a lack of awareness of the tactics, dynamism and complexity of cyber security and its associated loopholes, cyber security attacks have escalated dramatically during this epidemic.

Every digital user must understand and engage with the digital world with a proactive approach as if an impending cyber threat is looming. Considering that cyber-attacks constitute a severe danger to individuals, government and private organizations, it has become a top priority to provide every internet-connected individual with a basic understanding of cyber security to prevent crucial data from falling into the hands of cyber thieves.

COVID-19 is only the start. In the future, the globe may be confronted with an increasing number of viruses like this. As a result, it's time to start thinking about the future. We should all learn from the COVID-19 epidemic so that every-one can better prepare well for the future and ensure that Cyber Security does not cause any more problems for the world at large. Cybersecurity concerns must be on the agendas of executive committee meetings of organizations; they should be given special attention in light of the increased threats during crisis scenarios. Rather than reacting to successful cyberattacks, organizations should be proactive in dealing with them and devise strategies to prevent them. Although prevention measures are crucial, cyber-attack detection, response, and recovery skills are also required. Future research will focus on executives prioritizing operational capabilities in the direction of cost management, health and cybersecurity.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

While accepting sole accountability for the article's substance, the authors want to thank the reviewers for their important remarks in this survey research efforts.

Compliance with ethical standards

Funding information: This work has been fully supported by Abu Dhabi University under Grant No 19300635.

Human and animal's rights: This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent: Informed consent was not required in this article as no humans or animals were involved.

References

Abiodun, O.I., Abiodun, E.O., Alawida, M., Alkhawaldeh, R.S., Arshad, H., 2021a. A review on the security of the internet of things: challenges and solutions. Wireless Pers. Commun. 119 (3), 2603–2637.

Abiodun, E.O., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A., Alkhawaldeh, R.S., 2021b. A systematic review of emerging feature selection optimization methods for optimal text classification: the present state and prospective opportunities. Neural Comput. Appl. 33 (22), 15091–15118.

Achim, M. V., Văidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The impact of the development of society on economic and financial crime. Case Study for European Union Member States. Risks, 9(5), 97.

Adeyoju, A. (2019). Cybercrime and Cybersecurity: FinTech's Greatest Challenges. Available at SSRN 3486277.

Ahmed, N., Michelin, R.A., Xue, W., et al., 2020. A survey of covid-19 contact tracing apps. IEEE Access 8, 134577–134601.

Arshad, H., Omlara, E., Abiodun, I.O., Aminu, A., 2020. A semi-automated forensic investigation model for online social networks. Comp. Security 97, 101946.

Arshad, H., Abdullah, S., Alawida, M., Alabdulatif, A., Abiodun, O.I., Riaz, O., 2022. A multi-layer semantic approach for digital forensics automation for online social networks. Sensors 22 (3), 1115.

Auyporn, W., Piromsopa, K., Chaiyawat, T., 2020. Critical Factors in Cybersecurity for SMEs in Technological Innovation Era. In: ISPIM Conference Proceedings. The International Society for Professional Innovation Management (ISPIM), pp. 1–10.

Babulak, E., Hyatt, J., Seok, K.K., Ju, J.S., 2020. COVID-19 & cyber security challenges US, Canada & Korea. Int. J. Trans. Machine Learn. Data Mining 2020 (2), 43–59.

Balas, V.E., Kumar, R., Srivastava, R. (Eds.), 2020. Recent trends and advances in artificial intelligence and internet of things. Springer, pp. 389–425.

Bossler, A.M., 2021. Neutralizing cyber attacks: techniques of neutralization and willingness to commit cyber attacks. Am. J. Criminal Justice 46 (6), 911–934.

Burns, A.J., Johnson, M.E., Caputo, D.D., 2019. Spear phishing in a barrel: Insights from a targeted phishing campaign. J. Organiz. Comp. Electr. Commerce 29 (1), 24–39.

Cbsnews (2021). https://www.cbsnews.com/news/us-covid-relief-hacking-hackers-arrested-indonesia-aid-program-scam/.

Cressey, D. R. (1953). Other people's money; a study of the social psychology of embezzlement.

Cross, C., Gillett, R., 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. J. Financial Crime.

Cross, C., Kelly, M., 2016. The problem of 'white noise': examining current prevention approaches to online fraud. J. Financial Crime 23 (4), 806–828.

Das, S., 2015. The Cyber Security Ecosystem: Post-Global Financial Crisis. In Managing in Recovering Markets. Springer, New Delhi, pp. 453–459.

De Mello, R.C., Jimenez, M.F., Ribeiro, M.R., Guimarães, R.L., Frizera-Neto, A., 2019. On human-in-the-loop CPS in healthcare: a cloud-enabled mobility assistance service. Robotica 37 (9), 1477–1493.

Degen, C.L., Reinhard, F., Cappellaro, P., 2017. Quantum sensing. Rev. Mod. Phys. 89, 035002.

Dilek, S., Çakır, H., Aydın, M., 2015. Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.

Esther Omolara, A., Jantan, A., Abiodun, O.I., Arshad, H., Dada, K.V., Emmanuel, E., 2020. HoneyDetails: A prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. Health Inf. J. 26 (3), 2083–2104.

French, G., Hulse, M., Nguyen, D., Sobotka, K., Webster, K., Corman, J., Ewing, M., 2021. Impact of hospital strain on excess deaths during the COVID-19 pandemic—United States, July 2020–July 2021. Morb. Mortal. Wkly Rep. 70 (46), 1613.

Gottschalk, P., 2008. Stages of financial crime by business organizations. J. Financial Crime.

Gounder, M.P., Farik, M., 2017. New ways to fight malware. Int. J. Sci. Technol. Res. 6.

Greathorn.com (2021). Cybersecurity Insiders. https://info.greathorn.com/hubfs/Reports/2021-Business-Email-Compromise-Report-GreatHorn.pdf.

Harris, A., Jones, M., 2020. COVID 19–school leadership in disruptive times. School Leadership Manage. 40 (4), 243–247.

Hasham, S., Joshi, S., Mikkelsen, D., 2019. Financial crime and fraud in the age of cybersecurity. McKinsey & Company, pp. 1–11.

Hill, M., 2020. HMRC Shuts Down Almost 300 COVID19 Phishing Scam Sites, 2020, https://www.infosecuritymagazine.com/news/hmrc-covid19-phishing-scams/, (Accessed 10 June 2020).

Hossain, M.S., Muhammad, G., Guizani, N., 2020. Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics. IEEE Network 34, 126–132.

ibm.com (2020). https://www.ibm.com/annualreport/.

Interpol. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19.

Jalali, M.S., Landman, A., Gordon, W.J., 2021. Telemedicine, privacy, and information security in the age of COVID-19. J. Am. Med. Inform. Assoc. 28 (3), 671–672.

Kaspersky, (2020). Coronavirus phishing, 2020.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Khurshid, A., 2020. Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. JMIR Med. Inf. 8, e20477.

Khweiled, R., Jazzar, M., Eleyan, D., 2021. Cybercrimes during COVID-19 Pandemic. Int. J. Inf. Eng. Electr. Business 13 (2).

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comp. Security 105, 102248.

Mansfield-Devine, S., 2015. The growth and evolution of DDoS. Network Security 2015 (10), 13–20.

Manzalini, A., 2020. Quantum communications in future networks and services. Quantum Rep. 2, 221–232.

Masciandaro, D. (Ed.), 2017. Global financial crime: terrorism, money laundering and offshore centres. Taylor & Francis.
McGuire, M., 2018. Understanding the growth of the cybercrime economy. In RSA conference, USA.
Mertoiu, G.B., Mesnita, G., 2021. Global crises and cybersecurity atacks–an analysis during the covid-19 pandemic. Acta Scient. Polonorum Oeconomia 20 (4), 39–48.
Mohamed, N. A., Jantan, A., Abiodun, O. I., 2018. An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1, pp. 14-16).
Naidoo, R., 2020. A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. 29 (3), 306–321.
Naik, B., Mehta, A., Yagnik, H., Shah, M., 2021. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex Intelligent Syst., 1–18
Najaf, K., Schinckus, C., Yoong, L.C., 2020. VaR and market value of fintech companies: an analysis and evidence from global data. Managerial Finance.
NCSC, (2020). NCSC Shines Light on Scams Being Foiled via Pioneering New Reporting Service, 2020, https://www.actionfraud.police.uk/news/cyber-expertsshine-light-on-online-scams-as-british-public-flag-over160000-suspect-emails, (Accessed 7 May 2020).
Netherlands, C. B. S. (2020). Less traditional crime, more cybercrime.
Sky News, (2020). Coronavirus: Fraud victims have lost more than £4.6m to virus-related scams, 2020. https://news.sky.com/story/coronavirus-fraud-victimshave-lost-more-than-4-6m-to-virus-related-scams11996721.
Ng, A.W., Kwok, B.K., 2017. Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. J. Financial Regul. Compliance.
Omolara, A. E., Jantan, A., Abiodun, O. I., & Arshad, H. (2018). An enhanced practical difficulty of one-time pad algorithm resolving the key management and distribution problem. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).
Omolara, A.E., Jantan, A., Abiodun, O.I., Singh, M.M., Anbar, M., Kemi, D.V., 2018b. State-of-the-art in big data application techniques to financial crime: a survey. Int. J. Comp. Sci. Network Security 18 (7), 6–16.
Omolara, A.E., Jantan, A., Abiodun, O.I., 2019b. A comprehensive review of honey encryption scheme. Indonesian J. Electr. Eng. Comp. Sci. 13 (2), 649–656.
Omolara, A.E., Jantan, A., Abiodun, O.I., Dada, K.V., Arshad, H., Emmanuel, E., 2019c. A deception model robust to eavesdropping over communication for social network systems. IEEE Access 7, 100881–100898.
Omolara, A. E., Jantan, A., Abiodun, O. I., Arshad, H., & Mohamed, N. A. (2019). Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication. Int. J. Electr. Comp. Eng. (2088–8708), 9(3).
Omolara, O.E., Oludare, A.I., Abdulahi, S.E., 2014. Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication. Comp. Eng. Intelligent Syst. 5 (5), 34–46.
Pras, I.A., 2021. Investigating an Association Between DDoS and Phishing Attacks. University OF Twente). Doctoral dissertation.
Prates, M.O., Avelar, P.H., Lamb, L.C., 2020. Assessing gender bias in machine translation: a case study with google translate. Neural Comput. Appl. 32 (10), 6363–6381.
Reid, A.S., 2018. In: Financial crime in the twenty-first century: the rise of the virtual collar criminal. Palgrave Macmillan, London, pp. 231–251.
Rosso, K. D. (2020). New threat discovery shows commercial surveillanceware operators latest to exploit covid-19.
Sakurai, Y., Smith, R. G. (2003). Gambling as a motivation for the commission of financial crime.
Salih, A., Zeebaree, S.T., Ameen, S., Alkhyyat, A., Shukur, H.M., 2021. A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In: 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic"(IEC). IEEE, pp. 61–66.
Särökaari, N. (2020). Phishing attacks and mitigation tactics.
Slussarenko, S., Pryde, G.J., 2019. Photonic quantum information processing: A concise review. Appl. Phys. Rev. 6, 041303.
Smzdm.com, Hackers are using the "coronavirus" fear for phishing 2020.
Suhono, S., Zuniati, M., Pratiwi, W., Hasyim, U.A.A., 2020. Clarifying google translate problems of Indonesia-English translation of abstract scientific writing. EAI 24–25, 1–13.
Sultana, J., Jilani, A.K., 2021. Classifying Cyberattacks Amid Covid-19 Using Support Vector Machine. In Security Incidents & Response Against Cyber Attacks. Springer, Cham, pp. 161–175.
Taofeek, O.T., Alawida, M., Alabdulatif, A., Omolara, A.E., Abiodun, O.I., 2022. A cognitive deception model for generating fake documents to curb data exfiltration in networks during cyber-attacks. IEEE Access.
Thakur, K., Ali, M. L., Jiang, N., & Qiu, M. (2016, April). Impact of cyber-attacks on critical infrastructure. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 183–186). IEEE.
Tidy, J., 2020. Coronavirus: Israel enables emergency spy powers. BBC News 17.
UNESCO: (2020). Distance Learning Solutions (2020).
Ünvan, Y. A. (2020). Financial Crime: A Review of Literature. Contemporary Issues in Audit Management and Forensic Accounting.
Walter, J., 2020. Threat intel| cyber-attacks leveraging the covid-19/coronavirus pandemic. SentinelLABS. Sep, 4.
Watters, P.A., McCombie, S., Layton, R., Pieprzyk, J., 2012. Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP). J. Money Laundering Control.
World Health Organization. (2020). WHO reports fivefold increase in cyber attacks, urges vigilance. News release), April, 23.
Wu, S., Chen, Y., Li, M., Luo, X., Liu, Z., Liu, L., 2020. Survive and thrive: A stochastic game for DDoS attacks in bitcoin mining pools. IEEE/ACM Trans. Networking 28 (2), 874–887.
Yar, M., 2005. The novelty of 'cybercrime' an assessment in light of routine activity theory. Eur. J. Criminol. 2 (4), 407–427.
Zahra, S.R., Chishti, M.A., Baba, A.I., Wu, F., 2021. Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. Egypt. Inf. J.
Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Choo, K.K.R., 2021. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif. Intell. Rev., 1–25