


# A Systematic Literature Review on the Impact of Cybersecurity Threats on Corporate Governance During the Covid-19 Era



Gorejena Nyasha, Lilian Ifunanya Nwosu , Makuena Clementina Bereng, Calvin Mahlaule, and Tlotlo Segotso

**Abstract** When the Covid-19 pandemic erupted, many companies faced unprecedented challenges, including cybersecurity threats due to increased dependence on technology. Cybersecurity refers to the set of security measures that can be taken to protect cyberspace and user assets against unauthorized access and attacks. It has always been a challenge that has affected the company's existing corporate governance and compliance process. However, during the Covid-19 period, cyber-attacks and dangers increased significantly, posing a new set of challenges to the companies, which in turn had a negative effect on the economy. The purpose of this study was to provide a comprehensive Systematic Literature Review (SLR) on the effects of cybersecurity threats on corporate governance during the Covid-19 pandemic and to identify the existing literature review gaps as well as the challenges and recommendations on how to deal with the identified threats. A preferred reporting item for systematic and meta-analysis-based reviews (PRISMA) was conducted manually on 18 sampled publications. This study utilized a qualitative approach to review published research on corporate governance and cybersecurity threats during the Covid-19 era. The findings revealed that during the Covid-19 period, increasing cyber-attacks were carried out against many companies. The study also revealed that social distancing requirements forced most company directors to review corporate information and participate in sensitive discussions online in their homes or places far less secure than the director's typical business office or company boardroom. As a result, the increased volume of work being performed remotely presents opportunities for cybercriminals to tailor and retool schemes to target directors and those in charge of the company's corporate governance. This study could significantly contribute to the body of knowledge by highlighting the potential challenges cybersecurity as well as the suggestion on how companies could minimize the risks encountered.

---

G. Nyasha · L. I. Nwosu (✉) · M. C. Bereng · C. Mahlaule · T. Segotso  
North West University, Mafikeng, South Africa  
e-mail: [23012064@nwu.ac.za](mailto:23012064@nwu.ac.za); [20264860@nwu.ac.za](mailto:20264860@nwu.ac.za); [Tlotlo.Segotso@nwu.ac.za](mailto:Tlotlo.Segotso@nwu.ac.za)

**Keywords** COVID-19 · Cybersecurity · Corporate governance · Systematic literature review · Cybersecurity threats

## 1 Introduction

According to Perwej et al. (2021) the internet has recently started to play a bigger role in people's daily lives all across the world. Before the pandemic, most businesses did not allow their staff to work from home, and most board meetings were held in person. On the one hand, shifting from a stationary to a remote working environment requires companies' boards to pay more attention to the wave of potential cybersecurity attacks and incurring additional security costs (Antczak, 2022). Cybersecurity refers to "the methods that organisations uses to safeguard its products and information in cyberspace" (Perwej et al., 2021, pp. 669). During the Covid-19 era, many companies were confronted with unprecedented challenges, including those associated with cybersecurity threats due to increased dependence on technology (Soni et al. 2020). There are practices that were introduced during this era, such as lockdown and social distance. As a result, most employees were required to work remotely, resulting in many organisations relying significantly on technology.

The primary threat to systems from cyber-attacks is the online interactions of organisations, making it a challenging effort to defend them (Khan et al., 2020). Most executive staff working from home used various technologies to process, access, or transmit company documents or information, making it challenging to protect the corporate governance principles. Therefore, this made it easy for the cyber criminals to hack onto the systems to access the confidential information of these organisations (De et al., 2020; World Health Organisation [WHO], 2020). As cybercriminals exploit social flaws, cyber-attacks increased significantly during the Covid-19 pandemic (Alawida et al., 2022). The World Economic Forum (2019) defines cybercrime as malicious computer-mediated access to an entity or someone's information. System interference, forgeries, and identity theft are some prominent kinds of cybercrimes (Alawida et al., 2022; Duong et al., 2022). The rise in cybercrime has exposed the lack of cyber-skilled professionals in most countries (Peter, 2017). Due to a global shortage of qualified cybersecurity personnel, cybersecurity concerns exist today (Blažič, 2021).

Many variants of cyber-attacks occurred and identified during the global crisis caused by Covid-19 include "phishing, malware, distributed-denial-of-service (DDoS), denial-of-service (DoS), advanced persistent threat (APT), malicious social media messaging (MSMM), Business E-mail Compromise (BEC), botnet, ransomware amongst many others" (Auyorn et al., 2020; Babulak et al., 2020; Bossler, 2021; Alawida et al., 2022).

Everything has recently been converted to digital, and cybernetics uses a range of technologies, including cloud computing, smartphones, and Internet of Things techniques, among others. People use the Internet to purchase goods and services and other e-commerce activities (Alawida et al., 2022). Cybercriminals, on the one

hand, have redefined their targets and the types of cyber-attacks (Antczak, 2022). Poor data management practices and unchecked system controls within organisations are some of the contributors to cybersecurity risks (Abukari & Bankas, 2020). Company executives from different industries face a rapidly changing cyber-threat environment (Antczak, 2022). Thus, companies had to significantly improve their cybersecurity in order to keep up with the rapid changes in cyberspace presented by Covid-19. Directors who are in charge of the organisation's governance were required to conscientiously protect the confidentiality of the organisation's information despite the unprecedented disruptions caused by Covid-19. Good corporate governance and record-keeping are essential, especially in more challenging times such as the Covid-19 era. However, according to a survey by the Global Risk Survey approximately 79% of the board of directors indicated that their companies were not sufficiently prepared to deal with Cybersecurity threats on corporate governance.

Company records communicated through communication platforms such as Zoom or chat applications risk becoming subject to cyber-attacks (Chigada, 2020). In addition, board members have a fiduciary duty to maintain corporate confidence (Goldberg, 2020). A breach of the fiduciary duty of confidentiality could expose directors to personal liability.

In light of the above, this study aims to answer the following question: What are the effects of cybersecurity threats on corporate governance during the Covid-19 era? Moreover, this study provided an in-depth review of the related literature on the cybersecurity threats on corporate governance and provided suggestions on how organisations can alleviate the challenges encountered. Furthermore, the research elaborated on the gaps existing in the literature. The following objectives were formulated to answer the abovementioned question.

### ***1.1 Objectives of the Study***

The following objectives were developed to provide a comprehensive Systematic Literature Review (SLR) on the effects of cybersecurity threats on corporate governance during the COVID-19 era:

- To identify the cybersecurity issues organisations faced during the Covid-19 pandemic;
- To determine the impact of the cybersecurity on the threats posed by the Covid-19 pandemic; and
- To provide possible ways for mitigating the threat that cybersecurity poses to businesses.

As depicted in Fig. 1, the most prevalent threats to cybersecurity were identified.

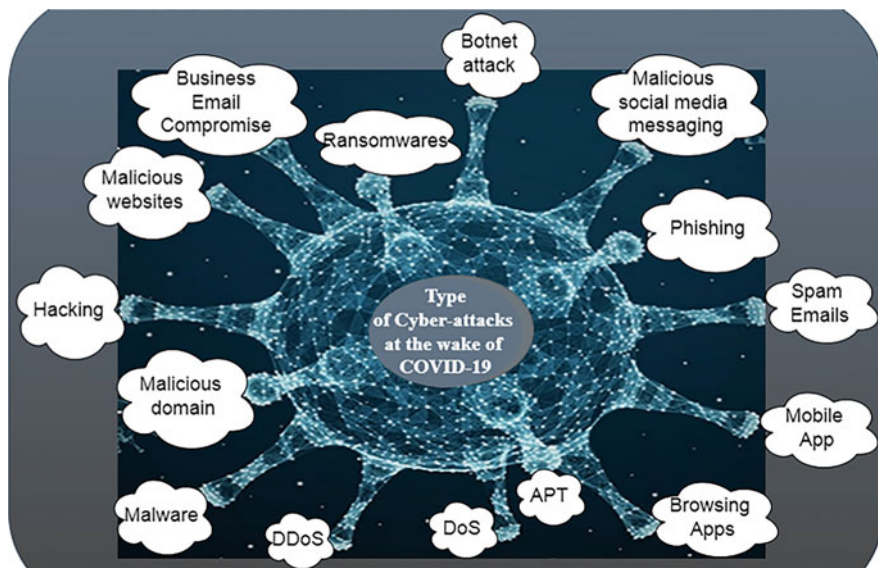


Fig. 1 Principal threats to Cybersecurity following Covid-19. Source: Alawida et al. (2022)

## 2 Methodology

This study used a qualitative method to review published research on corporate governance and cybersecurity threats during the Covid-19 era. A systematic literature review was performed using the PRISMA guidelines. PRISMA is a widely accepted guideline for systematic reviews and fits the current study's purpose. The use of SLR approach helps to correlate and draw conclusions from different sources on cybersecurity threats. Moreover, in the wake of Covid-19, researchers in the field of cybersecurity frequently employed the systematic review approach to carry out their studies (i.e. Alawida et al., 2022; Luhar et al., 2022; Perwej et al., 2021; Hazaa et al., 2021).

### 2.1 Keywords and Terms Identification

Methodologically, this study begins by searching various databases for publications that examine the overall ontology between cybersecurity and corporate governance in the Covid-19 era. Keywords and terms identifications, including bibliographical databases, were explored to facilitate the extraction of publications. This step assisted the researchers in identifying relevant publications from different search engines. For example, to ensure that the relevant literature was attained, the following keywords were included as part of the search titles 'Covid-19 and cybersecurity',

‘and ‘corporate governance’, ‘the cybersecurity threats during the Covid-19 era’, and ‘corporate governance and Covid-19’.

## 2.2 Inclusion and Exclusion Criteria

Using the following inclusion and exclusion criteria, as shown in Table 1, articles were chosen for inclusion in this study.

## 2.3 Data Sources and Search Strategy

The literature search was conducted between December 2022 and the beginning of January 2023. The search was limited to journal articles, conference papers and book chapters published between 2020 and 2023. According to Sect. 3.2, specific keywords were used in the search. The databases consulted include Google Scholar, Science Direct, IEEE Xplore, Springer Link, Sabinet, Elsevier, Emerald Insight, Willey, and EBSCOhost. There are lots of available literature sources on these databases and RISMA recommended a search from this database to enable accurate data sources.

At the initial stage, the search process produced 55 publications, including journal articles, conference papers, book chapters, and website documents. The researchers evaluated the Abstracts of each publication and categorized them as either included or excluded for this study to ensure that relevant literature was included. The current investigation deemed 12 research publications relevant, reliable, and also acceptable for this study. The results of the search process are presented in Tables 2 and 3 below. The flow diagram based on PRISMA guidelines is shown in Fig. 2.

**Table 1** Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Published during and after the Covid-19 pandemic (2019–2023)	Published before the Covid-19 pandemic
Empirical research	Studies that are not empirical research, such as reviews
Written in English	Studies not written in English
Involves sample from an organisation	Studies not related to an organisation
Publications in journals, conferences, and book chapters	Publications that were replicated, as well as those related to epidemiology

**Table 2** Summary of search results

Search results	Number of publications	Exclusion from the current study	Inclusion in the current study
Journals	33	25	14
Conferences	10	7	3
Book chapters	6	5	1
Websites	6	6	0
Total	55	43	12

Source: Authors own construction

### 3 Result and Discussion

This section presents the findings of the study.

## 4 Cybersecurity Concerns Faced by Companies During the Covid-19 Pandemic

It was found that during the Covid-19 era, increasing cyber-attacks were carried out against many organisations. This was because more sensitive business information was exchanged electronically as a result of the change in working patterns from physical to remote. These motivated cybercriminals to increase their online criminal activities. Africa has been one of the continents where cybercrime activity has grown at the fastest rate (Kshetri, 2019). A week after the Covid-19 pandemic began, 310,000 devices, the majority of which were used for business purposes, were the target of cyber-attacks, to steal user credentials like passwords for use in unauthorized access to sensitive data held by entities (Prior, 2020). South Africa had the third-highest number of victims of cybercrime worldwide due to a lack of cybercrime laws and a failure to integrate technology (Koigi, 2020). Each sector was affected differently by cyber-attacks, which caused 36% of South African companies to lose income and 27% to suffer reputational harm (FTI Consulting, 2020). Financial institutions, research, health, and government institutions are some of the most targeted Cybersecurity concerns for businesses due to their intense focus on the disease (Chigada & Madzinga, 2021).

### 4.1 Financial Institutions

Due to their market dominance in terms of clients and their economic impact on financial markets, banking, digital aspects, and international connections, financial institutions continue to be a high target for cybercriminals (Chigada & Madzinga,

**Table 3** List of reviewed studies

Author	Country	Title	Cybersecurity threats presented by the Covid-19 pandemic	Measures that can be put in place to reduce the risk of Cybersecurity
AbukariandBankas (2020)	Ghana	Some Cybersecurity Hygienic Protocols for Teleworkers In Covid-19 pandemic Period And Beyond	Spreading of computer-related malwares, online bullying, unauthorised electronic transactions, child pornography and breach of privacy are some of the activities performed by cybercriminals.	Hygienic protocols that can assist in addressing the dangers of cybercrime in the era of COVID-19 are presented in the paper.
Alawida et al. (2022)	United Arab Emirates/ Nigeria	A deeper look into Cybersecurity issues in the wake of Covid-19: A survey	During the Covid-19 crisis, 15 distinct types of cyber attacks were identified, along with their most common pattern and devastating events.	In order to overcome the effects of the pandemic or other crisis of a similar nature, the study suggests that governments and organisations make decisions regarding Cybersecurity that are innovative and resilient
Alkhalil et al. (2021)	United Kingdom	Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	Theft of private information, business secrets, and government secrets are just a few of the significant losses that victims of phishing attacks can sustain.	The anatomy that is being proposed will assist in raising awareness of these phishing attacks and the methods that are utilised. Additionally, it aids in the creation of a comprehensive anti-phishing strategy. In addition, new approaches are suggested, and some precautionary measures are investigated.
Blazic (2021)	Slovenia	The Cybersecurity labour shortage in Europe: Moving to a new concept for	These results indicate that Cybersecurity topics are not covered in	Based on our findings, the emerging educational landscape is

(continued)

**Table 3** (continued)

Author	Country	Title	Cybersecurity threats presented by the Covid-19 pandemic	Measures that can be put in place to reduce the risk of Cybersecurity
		education and training	private courses or Cybersecurity programmes offered by higher education institutions.	proposed, and the steps taken to improve education in both sectors are presented. In the concluding section, recommendations for improving Cybersecurity education and training are provided to stakeholders and academics.
De et al. (2020)	India	Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice		Aspects of surveillance and privacy gain importance with increased digital usage.
Duong et al. (2022)	Australia	Working from home users at risk of Covid-19ransomware attacks	The six attack vectors—social engineering, phishing, trojan, remote desktop protocol, drive-by download, and malvertising—are necessary to spread the dangerous malware (ransomware).	The study recommended that future work focus more on teaching and educating working-from-home users about the dangers of ransomware attacks and how to mitigate such an event from occurring.
Hakak et al. (2020)	Canada/ Saudi Arabia/ USA	Have You Been a Victim of Covid-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies	This study explored Covid-19-themed cyberattacks and categorised them into four categories: disrupting services, financial gains, information theft, and fearware, and further categorised into sub-categories	These categories were used in this study to present potential solutions for mitigation. In the event of future pandemics, the cyberattack taxonomy and potential mitigation strategies can also aid in planning

(continued)



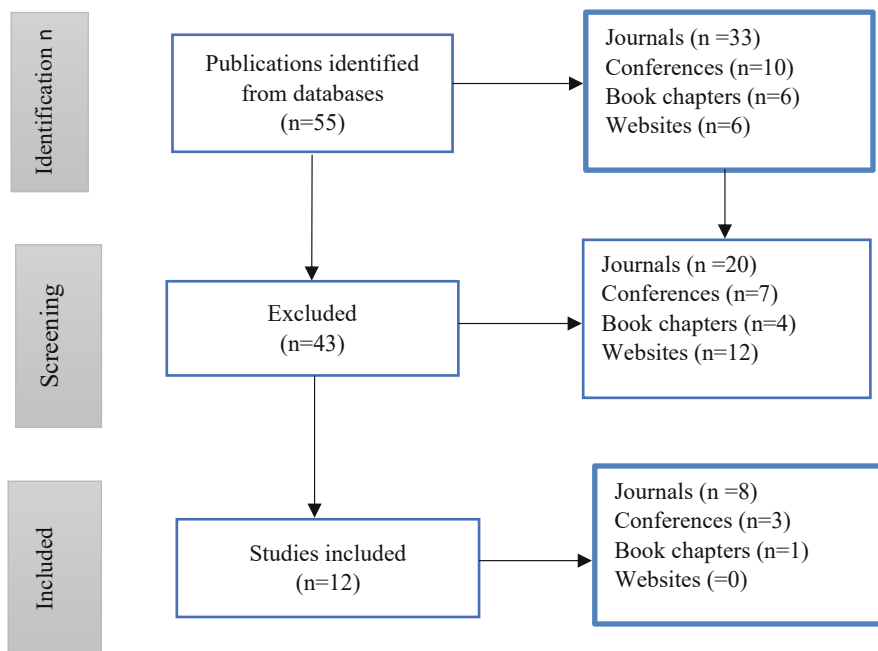
**Table 3** (continued)

Author	Country	Title	Cybersecurity threats presented by the Covid-19 pandemic	Measures that can be put in place to reduce the risk of Cybersecurity
			(e.g., malware, ransomware, phishing).	cyberattack prevention efforts.
Khan et al. (2020)	Malaysia	Ten Serious Threats to Cybersecurity During the Covid-19 pandemic.	The registration of spam e-mails, malicious websites, and domains has significantly increased. Individuals, government officials, and even medical and healthcare systems are being targeted by intruders.	In order to alleviate serious privacy concerns and improve the situation surrounding the Covid-19 pandemic, this paper identified Cybersecurity threats that must be avoided.
Kshetri (2019)	United States of America	Cybercrime and Cybersecurity in Africa		Numerous countries on the continent have developed legislation and strengthened enforcement measures to combat cyberthreats, according to the study, which reported a number of measures taken to address cyberthreats and improve Cybersecurity.
Uchendu et al. (2021)	United Kingdom	Creating a culture of Cybersecurity: Future requirements and current practices	The study provides an up-to-date description of the field and identifies unresolved issues that require further investigation, such as the significance of national culture and change management processes in an organisation's Cybersecurity culture.	We have been able to discover the advancements and difficulties currently faced in the field by investigating Cybersecurity culture, including information security culture and security culture.

(continued)

**Table 3** (continued)

Author	Country	Title	Cybersecurity threats presented by the Covid-19 pandemic	Measures that can be put in place to reduce the risk of Cybersecurity
Zahra et al. (2022)	India/ United States of America	Detecting Covid-19chaos-driven phishing/malicious URL attacks by fuzzy logic and data mining-based intelligence system	The Covid-19 pandemic altered our way of life and led to a widespread shift to digital platforms as businesses virtually eliminated in-person experiences. However, this change also increased people’s susceptibility to cybercrime.	The study offers a thoroughly researched set of mitigation strategies which can be employed to prevent the attacks. It also proposes a fuzzy logic and data mining-based intelligence system for detecting Covid-19 themed malicious URL/phishing attacks.



**Fig. 2** PRISMA flow diagram. Source: Authors own construction

2021). According to PricewaterhouseCoopers [PWC] (2020) the banking industry is mainly affected by ransomware cybersecurity threats, which have increased more than nine times in South Africa since the beginning of the Covid-19 outbreak. The cause of the rise in cyber-attacks on financial institutions is the heavy reliance on digital applications rather than in-person attendance at financial branches to conduct financial operations (Chigada & Madzinga, 2021). During the first three months of the Covid-19 pandemic, concerns about cybersecurity increased by 238% worldwide due to sudden changes in working procedures and a lack of awareness of technical applications like firewall defences and ongoing virus updates (Chigada & Madzinga, 2021).

#### 4.1.1 Healthcare and Research Institutions

The primary sources of updates and news on Covid-19 are among the front-line institutions, such as research laboratories, hospitals, and pharmaceutical companies. Cybercriminals target these groups to frighten the public and spread panic, so they may devise cunning ways to commit fraud such as identity theft (Chigada & Madzinga, 2021). The authors revealed various reasons which result in these fraud which includes, obsolete software, weak legislation, and a lack of digital literacy, influenced attacks on medical and scientific organisations. It appears that to help curb the spread of Covid-19, healthcare professionals had to rely heavily on e-healthcare services. As a result, the e-mails and passwords of more than 450 healthcare workers were made public (WHO, 2020).

According to a study by Chigada (2020), healthcare institutions are particularly vulnerable to cyber-attacks and threats because they collect and maintain sensitive patient data that cybercriminals can utilise. Medical data protection should be treated carefully, according to Chigada (2020), as it is a target for cybercriminals. Hackers install ransomware to prevent users from accessing their data or operating systems until some kind of ransom is paid to the hackers.

It is important to remember that ransomware can also attack PCs, servers, cloud-based file sharing, and other devices, severely disrupting an organisation's fundamental operations. Businesses could be destroyed by ransomware. If malware prohibits consumers from accessing data for one day, businesses' revenue will suffer. The most typical means of ransomware distribution are malicious attachments in phishing e-mails that encourage downloads. According to reports, ransomware affected some businesses in 2021, including Acer, Accenture, Kia Motors, CNA Financial Corp., etc. The fact that businesses would prefer not to report an infection owing to possible legal implications and brand damage is known to cybercriminals. In conclusion, businesses should utilize a trustworthy multilayered security solution because it is virtually hard to decode the files that are being held for ransom without having access to the private key. The study concludes that certain businesses are failing to manage the risks due to the substantial increase in dangers brought on by the Covid-19 pandemic's progression.

## 4.2 *Government Institutions*

Hakak et al. (2020) mention that government officials used Zoom and other official video conferencing programmes for their meetings, which escalated cyber-attacks due to the services vulnerabilities and made them popular among cybercriminals. The introduction of the R500 billion government stimulus package, which is also covered by the corruption the nation is fighting, was one of the other elements that led to the attacks (Chigada & Madzinga, 2021). Cyber-attacks had a significant negative impact on several governmental organisations, notably Transnet. Moyo (2021) claims that the Transnet IT networks have been modified, disrupting regular business in order to give hackers unrestricted access to the operations of such companies, causing irreparable harm to government bodies.

Due to the growing threat of cybercrime, most South African firms are in a dire dilemma. Growing worries about cybersecurity are putting both people and companies at risk. The biggest consequences include reputational damage that lowers a company's client base and revenue. Companies that lag in technological and computer security advancements suffer the worst outcomes. Cybercriminals regularly take confidential information from companies and use it as leverage to obtain favours from those companies. If South African businesses are to overcome their concerns about cybersecurity, cybercrime must be viewed as a distinct pandemic. This will raise awareness of cybersecurity offenses' risks and damage to everyone interested in the nation, from citizens to high government officials. This will ensure that the right policies and laws are quickly devised and thoroughly implemented, and that compliance is ensured to battle the cybercrime epidemic. The study concludes that South African organisations continue to face severe cybersecurity risks and concerns as a result of their organisation's lack of technological advancements and skilled technical personnel to handle cybersecurity challenges.

## 5 **Cybersecurity's Impact on the Threats Posed by the Covid-19 Pandemic**

Cybersecurity prevents virtual assaults on systems, networks, and software (Khan et al., 2020). In order to ensure information integrity, confidentiality, and availability, information systems must be safeguarded against unauthorised access, disclosure and destruction. Lack of adequate cybersecurity can harm an organisation's brand, result in financial loss, and negatively impact its operations. The common cyber threats and attacks that harm businesses are depicted are set out below:

## **5.1 Malware Cyber Attacks**

Any threat to business systems and personal internet-connected gadgets is malicious malware Ganiyu and Jimoh (2018). Cybercriminals employ malware to infect computers and use them to mine bitcoin, steal financial data, fool victims into supplying personal information, and take over several machines to perform denial-of-service assaults (Alkhalil et al., 2021). In addition, Malware can cause data leaks, and malfunctioning corporate systems can stop operations. As a result, several sizable websites have promoted themselves as tools that protect users from COVID-19.

### **5.1.1 Business e-mail Compromise Threat**

Numerous individuals worldwide have been impacted by Covid-19, which cybercriminals have routinely exploited to taint corporate e-mails. Hackers have recently been found to have compromised business e-mails (Zahra et al., 2022). Zahra et al. (2022) add that hackers frequently target personal information held by financial organisations. By sending phishing e-mails that deceive recipients into providing their personal information.

### **5.1.2 Ransomware Cyber-Attacks and Threats**

Cook (2020) asserts that because employees may access corporate networks from home, hackers can afford to lock users out of their systems and assume that firms will agree to pay a ransom in exchange for their access. Accessing corporate networks from home is regarded as dangerous due to its manual targeting and frequent use in multistage attacks inspired by Emotetmalware (malicious links) and tricot malware (Cook, 2020). Additionally, ransomware refers to encrypting data so that it cannot be later decrypted using passwords (Khan et al., 2020).

### **5.1.3 Impersonating Websites**

To persuade naïve internet users to share vital information, more than 86,000 fake websites with information regarding Covid-19 have been created (PricewaterhouseCoopers [PwC], 2020). Users and businesses have encountered the black NET RAT, a malware that facilitates the start of cyber-attack by loading remote files (WHO, 2020). It is possible for cybercriminals to legitimately acquire a certificate whose domain name contains a specific character that would deceive all commonly used browsers into thinking it is an attacker (PwC, 2020). Attackers ask certificate authorities to issue certificates for subdomains of malicious websites, and since the hacker legitimately controls the parent domain, certificate authorities issue

certificates for the domain (Bayhack, 2020). Attacks that mimic other websites can boost the return on investment for cybercriminals.

#### **5.1.4 Mobile Threats and Browsing Applications**

Due to the boom in smartphone use, cybercriminals now have more opportunities. The overuse of mobile devices by people allows cybercriminals to produce bogus software that deceives consumers. Cybercriminals recently created a mobile app called Covidlock and falsely claimed that it was derived from an Android app in order to follow Covid-19 cases (WHO, 2020). Many people use unsafe public networks to look up information on company servers. Since hackers can simply access this public Wi-Fi hotspot and infect users with malware, users are exposed to attackers (Abukari & Bankas, 2020).

### ***5.2 Ways for Mitigating the Threat That Cybersecurity Poses***

End-point security, network security, content inspection, and other measures have been used to lessen cyber-attacks. Thaldar and Townsend (2021) affirm that the Protection of Personal Information Act aims to protect individuals from harm by safeguarding their personal information in order to prevent the theft of their money, their identity, and, more generally, their right to privacy, which is a fundamental human right. To do this, the legislation specifies the circumstances under which it is acceptable for someone to process another person's personal information. Zahra et al. (2022) state that some precautions taken to stop ransomware attacks included not opening e-mails from unknown senders and requiring encryption to be turned on or installed on all computers. To prevent unauthorised access, a robust multi-factor authentication procedure should be implemented. A plan was put forward by Alkhalil et al. (2021) to lessen the likelihood of password guessing. The method has been shown to be highly secure. It employs BAN-logic to offer manual authentication. Ganiyu and Jimoh (2018) observed that malware is a hazardous programme that a Winlocker can eliminate. Winlocker is a mechanism that most banks are still educating their customers on as it is intended to lock users out of a compromised machine or device (Fenwick et al., 2019). This suggests that as soon as the hacker enters their credentials, Winlocker will capture the hackers' identities.

The steps taken to reduce cybersecurity risk appear to be somewhat successful. However, there may be room for improvement, and some measures may not be all-inclusive. Cybercriminals will not be able to access the private data of companies because the machines they utilise are encrypted, preventing any unauthorised access. Employees would comprehend and be aware of how to handle some cyber-attacks they may encounter using security awareness programmes. Although some may argue that awareness campaigns are insufficient, stakeholders should be encouraged to use the code of conduct and pertinent measures that discourage unethical

behaviour. It is crucial to remember that unsecured Wi-Fi must never be used. In order to attempt and limit the harm cybercriminals might cause the firm, the stakeholders must develop security awareness programmes and adhere to the code of conduct. The study's conclusion highlights the necessity for businesses to work together to combat the emerging Cybersecurity pandemic.

## 6 Conclusions and Recommendations

Since most people were working from home and utilising unsecured internet websites, the study indicated that the rate of cybercrime surged significantly during the Covid-19 pandemic. Additionally, it was discovered that different businesses attempted but failed to use malware software to reduce the danger of cybersecurity for confidentiality purposes. In order to ensure that systems and procedures are regularly updated, it is advised that organisations have the required IT-protected structure in place at the workplace.

Establishing ongoing cyber-security frameworks for financial institutions are advised to help identify suspect sources and electronic activities early. Organisations should establish a standard for implementing new technologies and devices, test IT systems to find weaknesses, and assess cybersecurity measures routinely. By strengthening the rules governing cybercrime and giving more authority to the agencies in charge of investigating and prosecuting cybercriminals, the government can raise its awareness of cyber-attacks. However, this is insufficient given the strategies criminals continue to develop to circumvent the law. The healthcare, financial, and other organisations fighting cybersecurity issues should consider educating and raising citizens' understanding of cybersecurity issues and expanding international cooperation in this fight. Globally, nations should create a strategy to coordinate their responses to cyber-attacks by exchanging information and working with international organisations.

The first step in combating cybersecurity risks should be regularly updating an organisation's cybersecurity policy and ensuring all employees and clients have access to adequate information about the issue. In addition, companies should ensure that their software and operating systems, and those of their employees and customers, are regularly updated. They should also implement password controls and launch education campaigns to inform stakeholders about cyber threats and countermeasures. Furthermore, South African businesses must use emerging technologies and data analytics to reduce their technological weaknesses and withstand cybersecurity threats. Additionally, it is advised that companies hire competent and experienced personnel because South African businesses lack these professionals.

The study recommended that directors conscientiously satisfy their confidentiality obligations despite the unprecedented disruptions caused by Covid-19. This study further recommended that boards of directors comply with the code on corporate governance, such as King IV report, especially on technology and

information governance requirements. Finally, this study suggests that company directors must view cybersecurity as a risk management issue affecting the entire organisation rather than just technology.

This study aimed to provide a comprehensive Systematic Literature Review (SLR) on the effects of cybersecurity threats on corporate governance during the Covid-19 pandemic. The introduction served as the foundation for achieving the study's objective. The research objectives that guided the study were derived from the research question. Section 2 of the article discussed the research methods and material comprising a systematic review using a preferred reporting item for systematic review (PRISMA). Section 3 provided the discussion of the results. Lastly, recommendations, as well as future research suggestions were provided.

## References

- Abukari, A. M., & Bankas, E. K. (2020). Some Cybersecurity hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, *11*(4), 1401–1407.
- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10, Part A), 8176–8206. <https://doi.org/10.1016/j.jksuci.2022.08.003>
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy [Review]. *Frontiers in Computer Science*, *3*. <https://doi.org/10.3389/fcomp.2021.563060>
- Antczak, J. (2022). The impact of the COVID-19 pandemic on business entity Cybersecurity. *Inżynieria Bezpieczeństwa Obiektów Antropogenicznych*, *1*, 7–15.
- Auyorn, W., Piromsopa, K., & Chaiyawat, T. (2020). Critical factors in Cybersecurity for SMEs in technological innovation era. ISPIIM Conference Proceedings. *The International Society for Professional Innovation Management (ISPIM)*, 1–10.
- Babulak, E., Hyatt, J., Seok, K. K., & Ju, J. S. (2020). COVID-19 & Cybersecurity challenges US, Canada & Korea. *International Journal of Transactions on Machine Learning and Data Mining*, *2*, 43–59.
- Bayhack, J. (2020). Cybercrime continues during COVID-19. *Bizcommunity*. Available from: <https://www.bizcommunity.com/Article/196/661/203999.html> (Accessed 15 May 2020).
- Blažič, B. J. (2021). The Cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, *67*, 101769. <https://doi.org/10.1016/j.techsoc.2021.101769>
- Bossler, A. M. (2021). Neutralizing cyber-attacks: Techniques of neutralization and willingness to commit cyber-attacks. *American Journal of Criminal Justice*, *46*(6), 911–934.
- Chigada, J. (2020). *Towards an aligned South African national Cybersecurity policy framework*. Unpublished PhD thesis.
- Chigada, J., & Madzinga, R. (2021). Cyber-attacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1–11.
- Cook, A. (2020). *COVID-19: Companies and verticals at risk for cyber-attacks*. Available from: <https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/> (Accessed 4 May 2020).



- De, R., Pandey, N., & Pal, A. (2020). Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, 55, 102171. <https://doi.org/10.1016/j.ijinfomgt.2020.102171>
- Duong, A. A., Bello, A., & Maurushat, A. (2022). Working from home users at risk of COVID-19 ransomware attacks. *Cybersecurity and Cognitive Science*, 51–87. <https://doi.org/10.1016/B978-0-323-90570-1.00001-2>.
- Fenwick, M., McCahery, J. A., & Vermeulen, E. P. (2019). The end of ‘corporate’ governance. Hello platform governance. *European Business Organization Law Review*, 20(1), 171–199.
- FTI Consulting. (2020). *Cybersecurity-resilience-south-africa*. Available from <https://www.fticonsulting.com/emea/-/media/files/emea%2D%2Dfiles/insights/articles/2019/sep/cybersecurityCybersecurity-resilience-south-africa.pdf?rev=79d87847b6474daa8a90439cae59eae9&hash=730D8EC6ED57B6866852D2795A7C10FB>.
- Ganiyu, S. O., & Jimoh, R. G. (2018). Characterising risk factors and countermeasures for risk evaluation of bring your own device strategy. *International Journal of Information Security Science*, 7(1), 49–59.
- Goldberg, C. (2020). *Cybersecurity and data privacy*. Available from <https://www.martindale.com/industry-group/goldberg-segalla-llp-5000609/CybersecurityCybersecurity-and-Data-Privacy/> (Accessed 8 February 2020).
- Hakak, S., Khan, W. Z., Imran, M., Choo, K. R., & Shoaib, M. (2020). Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access*, 8, 124134–124144. <https://doi.org/10.1109/ACCESS.2020.3006172>
- Hazaa, Y. M. H., Almaqtari, F. A., & Al-Swidi, A. (2021). Factors influencing crisis management: A systematic review and synthesis for future research. *Cogent Business & Management*, 8(1), 1878979.
- Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly Cybersecurity threats amid COVID-19 pandemic Covid-19 pandemic*. TechRxiv. <https://doi.org/10.36227/techrxiv.12278792.v1>.
- Koigi. (2020). *Cyber-crimes*. Available from: <https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/>. (Accessed 19 March 2022).
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81. <https://doi.org/10.1080/1097198X.2019.1603527>
- Luhar, I., Luhar, S., & Abdullah, M. M. A. B. (2022). Challenges and impacts of COVID-19 pandemic Covid-19 pandemic on global waste management systems: A review. *Journal Of Composites Science*, 6, 271. <https://doi.org/10.3390/jcs6090271>
- Moyo. (2021). Available from <https://www.itweb.co.za/content/wbrpOqgYAwY7DLZn>. (Accessed 9 May 2022).
- Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the Cybersecurity. *International Journal of Scientific Research and Management*, 9(12), 669–710.
- Peter, A. S. (2017). Cyber resilience preparedness of Africa’s top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, 17, 49–59.
- PricewaterhouseCoopers. (2020). *Impact of COVID-19: The world has changed and so have we*. Available from <https://www.pwc.co.za/en/about-us/integrated-report-2020/impact-of-covid-19.html>. (Accessed 10 April 2022).
- Prior. (2020). Massive increase in South Africa network attack. Available from: <https://mybroadband.co.za/news/internet-of-things/344479-massive-increase-in-south-african-network-attacks.html>. (Accessed 10 March 2022).
- Soni, V., Kukreja, D., & Sharma, D. K. (2020, December). Security vs. flexibility: Striking a balance in the pandemic era. In *In 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–5). IEEE.
- Thaldar, D., & Townsend, B. (2021). Protecting personal information in research: Is a code of conduct the solution? *South African Journal of Science*, 117, 1–2.

- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a Cybersecurity culture: Current practices and future needs. *Computers & Security, 109*, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- World Economic Forum. (2019). *Global risks report: Global risks perception survey 2018–2019*. Available from <https://www.weforum.org/reports/the-global-risks-report-2019> (Accessed 9 March 2022).
- World Health Organization. (2020). *Beware of criminals pretending to be WHO*. Available from <https://www.who.int/about/communications/cyber-security> (Accessed viewed 21 May 2021).
- Zahra, S. R., Chishti, M. A., Baba, A. I., & Wu, F. (2022). Detecting COVID-19chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal, 23*, 197–214. <https://doi.org/10.1016/j.eij.2021.12.003>