South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Cyberattacks and threats during COVID-19: A systematic literature review

Authors:
Joel Chigada[1]
Rujeko Madzinga[1]

Affiliations:
[1]Department of Information Systems, Faculty of Economic and Management Sciences, University of the Western Cape, Cape Town, South Africa

Corresponding author:
Joel Chigada,
chigadajm@gmail.com

Dates:
Received: 19 June 2020
Accepted: 22 Nov. 2020
Published: 19 Feb. 2021

How to cite this article:
Chigada, J. & Madzinga, R., 2021, 'Cyberattacks and threats during COVID-19: A systematic literature review', *South African Journal of Information Management* 23(1), a1277. https://doi.org/10.4102/sajim.v23i1.1277

Background: The novel Coronavirus Disease-2019 (COVID-19) pandemic, a deadly contagious disease has left the global village in disarray, driving people and firms, especially healthcare service providers to rely heavily on information communication technologies (ICTs) for administering telemedicine through digital tools. This study contributes to knowledge and information sharing and debates on cybersecurity.

Objective: The objective was to analyse the impact of cybercrimes on the global economy at a time when the whole world is focused on fighting and minimising the spread of COVID-19. The study also analysed common cybersecurity threats, attacks and information systems security vulnerabilities during the period of the pandemic.

Method: The study adopted a systematic literature review from December 2019 to June 2020. There are global research studies on cybersecurity issues brought about by the coronavirus pandemic, and therefore, literature survey was not limited to any geographic area. A mixed method research was adopted in this study.

Results: The study revealed that there is an exponential growth of cyberattacks and threats because the global economy has been paying much attention to the COVID-19 pandemic. During the pandemic, large corporations, healthcare industry and government agencies have been targets for cyberattacks and threats.

Conclusion: It has been demonstrated that cyberattacks and threats during the COVID-19 pandemic are rising exponentially, creating another wave of challenges for the global economy, which is already reeling under the novel coronavirus. Thus, exerting excessive pressure on financial and human resources that have to contend with the novel coronavirus, with the expectation that resources have to be mobilised to deal with cybercrimes. The study recommends that firms and individuals should devise cybersecurity interventions to protect their data and information systems infrastructure.

Keywords: cyberattacks; cyberthreats; COVID-19; information systems vulnerabilities; cybersecurity.

Introduction

Coronavirus Disease-2019 (COVID-19) is an airborne and contagious disease that has and continues to affect millions of people globally and claiming thousands of lives on a daily basis (World Health Organization [WHO] 2020c). With reference to the contagion impact of the COVID-19 pandemic, economies embarked on various interventions to flatten the curve or minimise infections. These include national lockdowns: no economic activity, no movement of people except for people working or providing essential services, leaving many people and firms heavily reliant on technologies to go about their business (National Institute of Communicable Diseases [NICD] 2020). Pursuant to strengthen laboratory and surveillance systems that can serve as a backbone for national policies to control the COVID-19 pandemic, the healthcare industry is heavily dependent on the use of ICTs to administer telemedicine (Council of Europe 2020).

The emergence of the COVID-19 pandemic has drastically altered business models, approaches to people's behaviours and lifestyles, resulting in 'working from home', but remotely connecting to their company's corporate information systems infrastructure. Cybercriminals have taken advantage of the pandemonium caused by the COVID-19 pandemic and a shift of attention to the pandemic. Individuals and firms have and continue to fall victim to cyberattacks and threats (WHO 2020a). The global economy is now confronted with the COVID-19 pandemic and cybersecurity warfare, heightening concerns amongst cybersecurity professionals who believe the rate of cybercrimes is rapidly increasing during the health pandemic.

The devastating impact on human lives and global economic activities are unprecedented prompting the researchers to explore the following research questions concerning cybersecurity rising in the midst of the COVID-19 pandemic:

- What factors are exacerbating cybercrimes during the COVID-19 pandemic?
- How are firms and governments responding to cybersecurity scourges during the COVID-19 pandemic?
- What impediments are affecting firms and governments' efforts when responding to cybersecurity challenges during the COVID-19 pandemic?

This study addressed the given questions in its review of cyberattacks and threats brought about by the global shift in focus to the COVID-19 pandemic. Globally, economies are determined to save lives and economic sustainability, but windows of opportunities have presented themselves to cybercrime syndicates. With scarce financial, information and human resources, the global economy might find it difficult to fight the COVID-19 pandemic and cybercrimes simultaneously, unless other stakeholders play a significant role to help governments fight cyberattacks and threats. This study contributes to debates around cybersecurity issues, specifically that the world is fighting the pandemic. In addition, the study shares knowledge and information with a view of informing policy, practice, future research and making statements for decision-making.

Methodology

The researchers adopted a systematic literature review through the lens of desktop research, where data were collected for the December 2019–May 2020 period. December 2019 was recorded as the official outbreak of COVID-19 in Wuhan, China, and since then researchers, scientists and other authors have extensively written and published literature on the subject matter (WHO 2020b). Systematic literature review permitted the researchers to formulate the three research questions, set inclusion and exclusion criterion, which were infused with meta-analysis to analyse, synthesise and disseminate research findings (Chigada & Hirschfelder 2017). Researchers used systematic literature review with the objective of identifying and retrieving international evidence on cybercrimes committed during the COVID-19 pandemic. This international evidence is relevant to the research questions, allowing the researchers to appraise and synthesise the results of this research to inform practice, policy and, in some cases, further research (Munn et al. 2018).

According to Takahashi et al. (2009), the use of pre-defined literary studies provides creditable sources allowing researchers to critically analyse findings, assumptions and limitations. Content analysis validates previous research by grouping the key content and interpreting its content (Payne & Payne 2004). The systematic literature review was chosen because of the empirical nature of the primary research question, which is exploratory (Babbie & Mouton 2012). Tranfield, Denyer and Smart (2003) stated that a systematic review establishes important scientific contributions to a field or question. Studies on cyberattacks and threats during the COVID-19 pandemic were drawn from December 2019 to June 2020. The inclusion criteria for studies considered in this research were cyberattacks and threats, cybersecurity and cybercrimes during the COVID-19 pandemic. The inclusion criteria were important because the objective was to critically appraise this research in order to answer a clearly formulated research question (Dewey & Drahota 2016). The researchers conducted a comprehensive search over multiple databases, internet sites and grey literature by identifying specific information searched, critiqued and reported within the December 2019 to June 2020 timeframe. This systematic review study was undertaken to confirm or refute that there is an exponential growth rate of cyberattacks and threats during the COVID-19 pandemic and that the global village is under severe stress fighting two pandemics simultaneously. Munn et al. (2018) stated that systematic literature review studies are undertaken to establish the quality of evidence and to address any uncertainty or variation in practice that may be occurring. The researchers used systematic literature to identify gaps, deficiencies and trends in the current evidence and help inform future research. At the conclusion of the study, the researchers produced statements to guide cybersecurity decision-making.

Coronavirus Disease-2019

On 30 January 2020, the Centers for Disease Control and Prevention (CDC) (2020) and the WHO (2020a) jointly announced the outbreak of a deadly respiratory novel coronavirus (COVID-19). The Coronavirus Disease-2019 is an infectious disease caused by a new strain of coronavirus. The 'CO' stands for corona, 'VI' stands for virus and 'D' stands for disease (Khan, Brohi & Zaman 2020). The virus that causes COVID-19 is transmitted mainly through droplets generated through coughing, sneezing and exhaling from an infected person. In addition, these droplets can land on surfaces, because they are too heavy to hang in the air, and thus, touching such surfaces exacerbates the transmission and infection rates. Exponential COVID-19 infection rates were recorded between February and June 2020 in Europe, United States and some Asian countries. With reference to Africa, South Africa recorded an average of 2500 daily infections, and thus, by 12 June 2020, the country had more than 60 000 cases of COVID-19 infections, 35 000 recoveries and more than 26 000 active cases. A total of 1354 deaths were recorded (Department of Health 2020).

To date, the WHO (2020b) stated that more than 46 million cases of COVID-19 infections have been reported globally. Out of the 46 million reported cases, more than 31 million people have recovered, whilst more than 1.2 million have succumbed to the pandemic. Countries experiencing high COVID-19 infection rates include the United States (9.4 million), India (8.2 million), Brazil (5.5 million) and Russia (1.7 million) (WHO 2020).

Reports by the WHO, CDC and other media indicate that there have been a slowdown rate of COVID-19 infections

globally, between July and September 2020, prompting many economies to remove hard-lockdown regulations to levels that focused on social distancing, wearing of masks, practising of other health-related practices, whilst reverting back to economic activities (WHO 2020b). With the easing of national lockdown from level five (complete national shutdown except for essential services), South Africa moved to level one on 01 October 2020, allowing industries and individuals to engage in full economic activities whilst observing and adhering to healthcare protocols. Recent reports by the National Department of Health (2020) and other media indicate that there is a second wave of worrisome COVID-19 infections in Gauteng, Eastern Cape, KwaZulu-Natal and Western Cape provinces. An exponential infection rate has been reported in the United States, Spain and United Kingdom, with the United Kingdom imposing a 1 month lockdown from 30 October to 02 December 2020. The United Kingdom has the highest official COVID-19-related death toll in Europe and is also grappling with more than 20 000 new COVID-19 daily infections (WHO 2020b).

These statistics demonstrate the need for more responsibility and concerted efforts from all stakeholders to flatten the curve. The emergence of the pandemic has brought panic, apprehension and anxiety to everyone with no solution or cure in sight. Whilst the global village's attention is focused on fighting and combating the spread of COVID-19, another wave of cybercrimes is growing exponentially, creating a headache for firms and cybersecurity experts. Cybercriminal syndicates are well-versed with global trends, have up-to-date information and know very well that everyone is focusing on the COVID-19 pandemic; therefore, with advanced intelligence, these criminals are attacking information systems designed to help fight the pandemic. These well-orchestrated attacks on information systems demonstrate the level of intelligence inherent in the minds of cybercriminals, prompting the global village, specifically cybersecurity and information systems experts, to be worried about the scourge.

Cybercrimes during Coronavirus Disease-2019

The World Economic Forum [WEF] (2019) defined cybercrimes as all unauthorised computer-mediated activities to a company or an individual's information with malicious intent. Cybercriminals illegally access information systems to steal, misuse and compromise the integrity of information for personal financial gains. In order to mitigate cybersecurity vulnerabilities, firms and individuals are compelled to protect their information assets through cybersecurity interventions and governance frameworks such as the Information Security Report Model (ISRM) and Information Systems Governance (ISG) framework.

Quade (2020) stated that cybercriminals are hacking into systems or internet-enabled devices for people working from remote locations because there is lack of security protocols for offsite connections. There are heightened acts of internet espionages, phishing campaigns, denial of service (DDoS) attacks, fake news portals and applications to steal very sensitive information from unsuspecting individuals, government officials and businesses.

Home-based work increases exposure to cyber-risks because individuals connect through less-reliable and unsecured Internet connections. Employees working from remote locations can access corporate networks using personal devices. Connected or logged on devices can get into the hands of unauthorised individuals through unsanctioned channels. In addition, social engineering attacks against employees and their families, and honest mistakes made in new workflows (caused by working remotely) are all new potential risks (Simonovich 2020).

Evidently, technology is bringing more challenges to firms and people because of increasing cyberattacks and threats to personal or company information assets. With reference to firms, more efforts are required to deal with the growing security demands emerging from the increased risk of cyberattacks and threats.

Although Goldberg (2020) asserted that firms have embraced the Fourth Industrial Revolution (4IR) technologies for improved efficiency and product/service standards, the emergence of the Fifth Industrial Revolution (5IR) is changing the business landscape. The combination of human beings and machines in the workplace denotes the magnitude and complexity of change. Human beings are now the front and centre of the production process (WEF 2019). As humans are front and centre for production, more people are regularly working remotely, and thus, firms are placing greater importance on human intelligence than ever before. As emphasis is placed on human intelligence, firms might overlook that individual ethical behaviour is a key determinant for human intelligence. This over-reliance on human intelligence creates windows of opportunities to engage in nefarious acts that affect organisational information systems and information assets (Chigada 2020a). Most cyberattacks and threats are perpetrated by human beings, and therefore, human behaviour, attitude and ethical conduct are paramount determinants that should be addressed in the 5IR era. The emergency of COVID-19 is compelling institutions to accelerate the adoption and use of technologies, specifically in telemedicine, vaccinations, diagnosis and data analytics. In line with these assertions and prospects, cybercriminals have gone a notch ahead by devising deadly security threats and attacks in the midst of the COVID-19 pandemic. These advanced cyberattacks and threats resonate with human intelligence as espoused in the 5IR era where people are now the front and centre of production (WEF 2019). Some of the leading cyberattacks and threats that have dominated during the COVID-19 pandemic period are identified as ransomware, malware, spam emails, malicious domains and DDoS (Khan et al. 2020).

Cybercriminals have identified COVID-19 disinformation as an opportunity to target research, healthcare organisations, government agencies and financial institutions (FIs) with the

knowledge that these organisations are focusing on the pandemic (PwC 2020; WEF 2020; WHO 2020a). Threat actors know that it might take some time before their nefarious acts are discovered because considerable attention is spent on mitigating the COVID-19 pandemic. The following discussion focuses on financial services, healthcare organisations and government agencies as prime targets for cybercrimes during the COVID-19 pandemic.

Financial services

During the COVID-19 pandemic, global systems have been attacked and millions of United States dollars have been lost through cybercrimes. Stock markets around the world and every aspect of the economy have been severely affected. The financial services industry has been attacked through phishing, malware and ransomware (Khan et al. 2020). With reference to widespread incidents of cyberattacks and threats, South African banks have embarked on a drive to educate their clientele regarding fake emails and phishing (South African Banks Risk Information Centre [SABRIC] 2020). A wide range of phishing scams (i.e. bogus communications that purport to be from a well-known and trusted source, which request confidential information [typically login/password details or banking information]) are circulated by hackers.

The PwC (2020) stated that the emergence of the COVID-19 pandemic has forced many FIs to move away from physical branches towards mobile services and digital communication, and thus, these changes continue to trigger exposure to risks. Clients conduct their banking transactions from their homes, and thus, with little or no security protocols (device-set-up; firewall protection, internal access controls and regular anti-virus updates) in place for their internet-enabled devices, clients' information is exposed to cybercriminals. This exposure applies to employees of FIs as well because they are working from secured office environments. Employees are confronted with phishing and social engineering attacks.

Between February and April 2020, cyberattacks and threats on FIs increased by more than 238% globally, at a time when the global economy was working tirelessly to fight the COVID-19 infections. The COVID-19 crisis created a perfect climate for cybercriminals. Ransomware attacks grew ninefold in the period, with phishing emails as the primary source (PwC 2020). Cyberattacks and threats are dramatically increasing because cybercriminals (human intelligence) have better knowledge of the policies and procedures of FIs, thus can easily identify the financial institution's blind spots.

Crisanto and Prenio (2020) stated that cybercriminals are and continue to exploit the vulnerabilities opened up by the COVID-19 pandemic, increasing the risks of cyberattacks, money laundering (ML) and terrorist financing (TF). There is an increase in ML and TF perpetrated through increased misuse of online financial services and virtual assets to move and conceal illicit funds and possible corruption connected with government stimulus funds (e.g. the R500 billion COVID-19 stimulus package). In addition, more than 1500 high-risk domains (set-up by threat actors) were created containing both a COVID-19 and financial theme (Crisanto & Prenio 2020) with the objective of stealing from the unsuspecting public or firms.

Healthcare systems

Most healthcare organisations rely on ICT applications, which offer patients and healthcare personnel e-healthcare services. The COVID-19 pandemic has exposed these e-healthcare services, escalating the battle currently faced by healthcare institutions resulting in overstretched resources and personnel that are responding to the novel coronavirus (Khan et al. 2020). In the United States, the CDC and other healthcare facilities have been attacked by DDoS through millions of connection requests. The WHO was also exposed to malicious attacks thrown at a critical time for global response and a key component of a collective resilience. The attack on the WHO impacted critical services where criminals launched spear-phishing attacks imitating the WHO and CDC, using the pandemic to spread malware and ransomware and launch fraudulent websites to prey on users (Balsom & Dixon 2020).

The Czech Republic hospital responsible for running most of the country's COVID-19 testing was held at ransom and forced to shut down its IT network. The United States Department of Health and Human Services (HHS) was a victim of DDoS attack (WHO 2020a). Cybercriminals have been targeting healthcare organisations that are at the forefront of dealing the COVID-19 pandemic, especially hospitals, research organisations, laboratories and pharmaceutical companies. Healthcare records are attractive for scammers attempting to commit fraud, identity theft or credit card scams (Chigada 2020b). There has been an increase of misinformation of COVID-19 through different platforms creating panic and uncertainty.

During the pandemic, ransomware on healthcare organisations are increasing at an alarming rate (WHO 2020a). Cyberattacks and threats on healthcare organisations are exacerbated because the healthcare industry significantly lags behind in terms of cybersecurity, lack of digital literacy amongst personnel, outdated software and insufficient regulations and enforcements (PwC 2020). Organisers of these cyberattacks hope to gather information relating to the outbreak of COVID-19. The WHO (2020a) reported that more than 450 email addresses and passwords were leaked by hackers who accessed the WHO server. Fake news and spread of disinformation are major threat contributors, especially in Asia (International police organisation [Interpol] 2020a) Threat actors use data harvesting to deceive people to execute malware, remote access Trojans, spyware, divert money and build botnets through the use of COVID-19-related information as a lure.

Government and other outlets

At a time when South Africa's Parliament is closed and all its meetings are currently held by video conference calls as the country remains under strict lockdown regulations, hackers disrupted the meeting by sharing obscene material using the Zoom platform during the virtual held meeting (Ogomotsi Magome 2020). In addition to the rapid growth of Zoom's popularity being deemed as unsafe in many countries, it has been banned in United States and Taiwan for communication (Khan et al. 2020). South African institutions are staying in touch with their clients and employees through Microsoft Teams, Google Meet and Zoom, despite cyberthreats and hacking incidents on Zoom meetings.

The Interpol (2020) reported that cybercriminals are focusing their attention on government agencies and large firms to cause irreparable damage to information systems infrastructure. Focusing on the pandemic and shift cyberthreat landscape puts additional strain on law enforcement agencies globally because of the exponential growth of cyberthreats and attacks. Cyberattacks and threats are boosted by exploiting the fear and uncertainty caused by unstable social and economic situation caused by the COVID-19 pandemic (Interpol 2020). Furthermore, people use teleconferencing tools and platforms in virtual office space, and thus, cybercriminals are aware of the security vulnerabilities in these tools.

Why exponential cybercrimes during the novel coronavirus?

It is also important to distinguish cybersecurity from information systems security to enable people understand the level of preparedness/readiness required by their firms. Cybersecurity and information systems security are often used interchangeably, yet the two are different but share multiple similarities. Khan et al. (2020) defined '*Cybersecurity* as the practice of protecting systems, networks and programs from digital attacks'. The International Telecommunications Union [ITU] 2020) defined cybersecurity as the collection of tools, policies, security concepts, guidelines, risk management approaches, best practices, assurance and technologies that can used to protect the user, organisation and cyber environment, whilst information systems security entails the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability (Chigada & Kyobe 2018).

National lockdowns, working from home or remote access to a company's network allow employees to use unsecured WiFi connection networks. Employees can remotely access their company networks through virtual private networks (VPNs), privileged access management (PAM), vendor privileged access management (VPAM), which are susceptible to hackers and intrusions if additional security protocols and features are not enhanced (Stevens 2018), giving birth to cybersecurity vulnerabilities. Cybercriminals monitor users' login activities and behaviour patterns, providing an opportunity to track and trail unsuspecting victims.

Abukari and Bankas (2020) stated that unsecured information systems protocols and poor data management practices are contributing to cybersecurity vulnerabilities. Employees' unethical behaviour contributes to security breaches because these employees understand the weaknesses of their organisations' cybersecurity governance structures. Vlachos (2011) stated that most malicious attacks happen when employees pass on sensitive information to cybercriminals. In addition, the concept of bring your own device (BYOD) is exacerbating security breaches because employees connect to a company's network using multiple devices, which, in some instances, are shared with friends and relatives, oblivious to the fact that these devices have sensitive login credentials (Frost & Sullivan 2016).

Employees who make use of the company network often by-pass security protocol, which prohibits users from accessing unsecure sites. Through this reckless behaviour, they expose the organisational network to threats of virus and data breaches. This threat becomes increasingly apparent as individuals access public WiFi. Lederer and Mendelow (2013) stated that public WiFi is unsecure and known for security vulnerability that pose not only a huge risk to personal devices but also an even bigger risk to organisational data assets which could have major financial impact that could cripple the organisation.

With reference to cyberattacks and threats to medical records, cybercriminals might be motivated to commit crimes because they have available buyers of medical information (WHO 2020a). Healthcare facilities store an incredible amount of confidential patient information, which can be easily sold. This information includes credit card, full names, identities, payment history and COVID-19-related information, which makes healthcare organisations more attractive to cybercriminals (PwC 2020). In addition, there has been an exponential growth of cyberattacks and threats because a large number of devices are used in healthcare organisations, which makes it hard to stay on top of security. Healthcare staff are often too busy to stay educated on the latest threats to devices leaving IT specialists with the task of protecting an entire hardware network against attacks (SwivelSecure 2020).

Cybercriminals are knowledgeable that healthcare information needs to be open and shareable between staff, both on-site and remotely and on multiple devices. Information technology personnel are not always available to assess the credentials of every device, especially in critical environments. With limited budgets, healthcare organisations are not keeping abreast with latest technologies, and therefore, the use of outdated technology means the healthcare industry is unprepared for attacks and threats (SwivelSecure 2020).

Discussion of findings

The Australian Institute of Criminology (2020), Khan et al. (2020), WEF (2020), ITU (2020) and WHO (2020c) have all come to some consensus regarding the common types of cyberattacks and threats perpetrated during the COVID-19 pandemic. These attacks are a continuation of what has been known before, but with a shift in focus towards the global novel coronavirus, cybercriminals have enhanced the tempo by using sophisticated and complex strategies to attack unsuspecting firms and individuals. These cyberattacks are usually aimed at accessing, changing or destroying sensitive information; extorting money from users; or interrupting normal business processes.

The PwC (2020) and WEF (2020) agreed that more cybersecurity companies are implementing artificial intelligence (AI)-driven algorithms to prevent threats, whilst on the other hand, hackers are also devising complex tactics in cyberattacks and hacking, keeping cybersecurity experts more worried and actively looking for solutions. Thus, in our hyperconnected world, there is no effective global security that can be implemented without understanding and mastering the science of cybersecurity (Stevens 2018). The four key themes that emerged during the study were: (1) common cyberattacks and threats, (2) exponential growth rate of cyberattacks and threats on healthcare organisations, (3) financial losses, and (4) lastly, the interventions put in place by governments, firms and individuals.

Common cyberattacks and threats

The Australian Institute of Criminology (2020) stated that between February and March 2020, there has been more than 260% increase in malicious universal resource locators (URLs) globally. This is corroborated by Khan et al. (2020) who stated that cybercriminals have isolated the United States as their prime target, and coincidentally, the United States has been the top location for detecting these cyberattacks. The following sections explain through literature, past studies and commentaries how cyber-attacks and threats have been perpetrated during the COVID-19 pandemic.

Malicious domains

Cybercriminals have and continue to create fake domains on the internet with the intention to deceive their victims. Khan et al. (2020) stated that internet users are confused by a plethora of replicating domains resulting in being attacked. By the end of January 2020, more than 4000 domains linked to coronavirus had been up and running. Checkpoint Risk Intelligence (2020) asserted that 3% of these domains are malicious and another 5% of them are suspicious. Hackers use these malicious domains to scam and get personal information for nefarious intentions (Chigada 2020a). The WHO (2020a), WEF (2020), Google (Palmer 2020) and CDC (2020) stated that there are more than 86 000 new active but risky or malicious domains related to the COVID-19 pandemic. These malicious domains contain keywords related to COVID-19 which are mostly found in the United States, Germany, Russia and Italy. The other worrying trend with malicious domains is that they are found in public clouds and entire internet. Cybercriminals are using the cloud to disguise phishing attacks and malware delivery attempts because it is difficult to defend threats coming from the cloud (Palmer 2020). What is more imperative is that many enterprises are turning to cloud service platforms during the pandemic with the hope of leveraging cloud native security tools.

Denial of service attack

The WHO (2020a) and CDC (2020) stated that there has been a spike of cyberattacks on government and healthcare organisations during the COVID-19 pandemic. Hackers interrupt the communication channels of government and healthcare institutions by flooding the systems with millions of users at the same time. The Department of Health and Human Services in the United States has been recently attacked. In South Africa, the Life Healthcare has been hit by cybercriminals, affecting all its 66 hospitals. The attacks inflicted widespread damage, affecting the admissions, business systems and email servers (White 2020). The International police organisation (Interpol) warned that under the global economy hospitals and governments are and will continue to be prime targets for cyberattacks and threats. With more people working from home or remote locations, DDoS attacks are likely to increase. Threat actors send multiple requests to the attacked web resource with the aim of overloading the capacity of the website and prevent the website from functioning well (White 2020).

Malware

Ganiyu and Jimoh (2018) defined malware as a dangerous application harmful to personal internet-enabled devices and company systems. Malware can lead to data leakage of information, whilst company systems could malfunction causing a standstill in operations. Many hackers use mobile devices as a target for malicious attacks through phishing emails and hyperlink attachments. Personal devices can be infected by malware at any given time if the device is connected to the corporate network. Cybercriminals are using interactive coronavirus maps and websites to spread malware, spywares and Trojans to unsuspecting firms' networks and mobile devices. Spam emails have been used by criminals to lure their victims. For example, First National Bank (FNB) in South Africa has been confronted with these attacks, where customers have been receiving spam and unsolicited emails requesting them to click on links sent to clients' mobile devices. Winlocker is used to lock users out of affected machines or devices, drop some files and modify windows registry, alerting the user to login. As soon as the users login, their credentials are stolen by Winlocker, and therefore, banks are on a campaign to educate their clients against clicking on suspicious links sent to them (Fuentes 2020).

Impersonating websites

Users and firms have been exposed to BlackNET RAT, a virus that purports to be a program developed by the

Harvard University. The virus helps to launch the DDoS attack by loading remote files, and thus, it works as a botnet. In the end, the virus executes malicious scripts, collecting browser cookies and passwords. A good example for BlackNET RAT is the fake website coronavirusmedicalkit.com created to deceive users, which states that the WHO provides vaccine kits for COVID-19, whilst it is a known fact that there are no valid COVID-19 vaccines (WHO 2020c). Hackers and fraudsters create unsanctioned websites that people access even these websites are prohibited. More than 86 000 malicious domains have been created bearing COVID-19 related information to attract unsuspecting computer users to provide sensitive information. When visiting a secure website, the browser examines the website's certificate to verify its authenticity. However, threat actors can legitimately obtain a certificate with a special character in the domain name that would fool all popular browsers into believing an attacker (PwC 2020; WEF 2020). Attackers request certificates for subdomain of a malicious site (e.g. PayPal.com\0.badguy.com) using the null/0 in the URL, and thus, certificate authorities (CAs) will issue the certificate for the domain because the hacker legitimately owns the root domain nadguy.com (Bayhack 2020).

Spam emails

Spam emails have been used by scammers and hackers for ill-intentions. There are numerous spam emails containing COVID-19-related fake messages for malicious attacks (WHO 2020a) (Bayhack 2020):

> Gmail reported to have blocked more than 100 million phishing emails on a daily basis. In the first week of April 2020, Google reported 18 million daily malware and phishing emails related to COVID-19. This is in addition to more than 240 million COVID-19-related daily spam messages. (n.p.)

Hackers use spoofing to fool their victims and ask them to donate in bitcoins with the deception that the emails are legitimately coming from the WHO. The WHO (2020a) advised its users that their official website: 'www.who.int' ends with '.int' and not '.org', and thus, people should be wary of emails emanating from fake websites.

Ransomware

Hospitals, education and public institutions have been subjected to ransomware. As a result of work from home or remote location access to corporate networks, hackers can afford to lock users out of their systems, and thus, cybercriminals are optimistic that these institutions can pay a ransom (Khan et al. 2020). Email attachments, links and compromised credentials are the most widely used approaches to infect an information system. A new ransomware called CoronaVirus was developed and spread through system optimisation software websites, luring victims to download the fake setup file. The CoronaVirus ransomware steals passwords, thereby encrypting data which cannot be unencrypted later (Cook 2020).

A South African commercial bank's information systems and computer were hacked or held hostage, with cybercriminals demanding a ransomware. More than 7 million customers' information was exposed, and thus, the commercial bank downplayed the extent of damage it suffered financially. Another South African credit bureau's server was hacked into exposing more than 24 million clients, and over 800 000 business' data were handed to a suspected fraudster. Not much information was shared relating to the severity of identity theft, cyberattacks and how much was lost in financial terms. However, being a Credit Bureau linked with all credit providers, South African FIs were on high alert because their systems were also vulnerable. The challenge with South African cyber laws is that they are fragmented and incoherent (Chigada & Kyobe 2018), and thus, Experian could not be penalised.

Significant increases of Ryuk ransomware have been detected during the COVID-19 pandemic. SonicWall (2020) stated that ransomware is a young family of cybercrimes. Its increase has been attributable to many people working from home and mobile workforces. The Ryuk (ransomware) is dangerous because it is targeted, manual and often leveraged through a multistage attack triggered by Emotet and TrickBot malware. Ryuk threat actors gained notoriety in 2019 demanding multimillion dollar ransoms from companies, hospitals and government agencies.

Fake or malicious social media accounts

Social networking platforms play an important role in information, video and knowledge sharing. However, hackers are gaining access to Facebook, WhatsApp and other social platforms for nefarious intentions. There have been numerous cases of fake Facebook accounts and impersonification resulting in the spread of fake information. In addition, hackers lure their victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, they are redirected to a social media phishing website, resulting in theft of login credentials (Cook 2020). Current attacks use social networking platforms as a delivery mechanism, and there are reports that advanced attacks will leverage users' contacts, location and business activities.

Browsing applications

With the advent of smartphones, users can 'surf the net' or browse the internet quickly anywhere and at any time. However, cybercriminals have developed a fake browsing application purporting that the app propagates COVID-19 information, allegedly indicating that it comes from WHO. With anxiety and curiosity to access first-hand information, users are lured to download and install the application through malicious links where hackers set-in the D-Link or Linksys routers, which open browsers automatically (The Australian Criminology Institute 2020). The user is prompted to download a COVID-19 Info app, where their credentials are stolen without suspicions.

Mobile threats

Life without a smartphone and internet connected devices is becoming impossible for many people. The proliferation of smartphones is creating another opportunity for cybercriminals to develop fake applications with the intention of deceiving smartphone users. Recently a mobile application, called CovidLock (ransomware), was developed by cybercriminals, which misrepresented that it was developed from an Android app to track COVID-19 cases (WEF 2020; WHO 2020a). However, it has been identified as a fake application, because victims' phones are locked and they are given 48 h to pay US$100 in bitcoin recovery. If the victim fails to pay the ransom, the victims' credentials are stolen and used for ill-intentions.

Many people access unsecure public networks (public WiFi access points) to connect to a company's servers looking for information. In some other instances, internet users access malicious or impersonating domains, which further exposes their login credentials. Hackers can easily access these public WiFi points and infect with malware, thus exposing mobile device users to attacks (Dixon & Balson 2020).

Business email compromise

Dixon and Balson (2020) stated that intruders are taking advantage of the COVID-19 pandemic by using coronavirus as a tool to convince targets to make transactions to an intruder purporting to be a legit employee working in the same company. First National Bank, Standard Bank and Nedbank have been recent targets of business email compromise and hacking. More than 1.7 million user accounts were hacked into at Nedbank in February 2020. However, as a result of the sensitivity of cybersecurity, not much information was provided in the Nedbank cyberattack to demonstrate the extent of damages (Isa 2020).

Cyberattacks and threats on healthcare organisations

The study established that healthcare organisations are most vulnerable to cyberattacks and threats because threat actors know very well that these institutions gather and keep vital patient information such identities, credit card details, COVID-19-related information which, if accessed, can be used for nefarious intentions. The WEF (2020) stated that four new malware samples are created every second, globally, an indication that cybercriminals are operating at highly sophisticated and complex levels. Past studies noted that in 2020, more phishing attacks will be launched because of the number of phishing kits available in the cyberspace. These kits will provide people with basic technological knowledge to run their own phishing attacks because only 65% of all URLs are considered trustworthy (Gravrock 2019). Interpol (2020) highlighted that malware, which has been relatively dormant for the past few months, was re-detected since the outbreak of COVID-19. The WHO (2020a) predicted that healthcare organisations will be the prime target because medical records are highly desired by cybercriminals and can sell for as much as US$1000, depending on the information they provide to the buyer. Cybercriminals engage in medical identify theft, that is, they assume a victims' identity in order to make fraudulent medical claims, insurance or forge prescriptions and drug labels. Chigada (2020) asserted that identity theft is a cause for concern because cybercriminals are stealing from the dead, that is, they access medical information of dead people with malicious intentions.

Financial losses

The World Bank (2019), WHO (2020a), WEF (2020), CDC (2020) and Cybersecurity Ventures (2020) predicted that cybercrime damages will cost the world US$6 trillion by 2021, up from US$3 tn in 2015. This huge financial loss represents the greatest transfer of economic wealth in history, creating more risks for innovation and investment. After analysing findings from past studies, there was a dearth of information pertaining to financial losses incurred during the COVID-19 pandemic. This demonstrates two issues: (1) there was no available data on financial losses to date, and (2) it would have been difficult to quantify financial losses because there were complex cybercrimes happening at the time the studies were conducted.

Interventions to mitigate cybercrimes

The study established that in the last six months (December 2019–May 2020), past studies have varying suggestions to firms and individuals to combat cybercrimes. These are discussed in the following sections.

Cybersecurity awareness

Aldawood and Geoff (2020) stated that most firms have unprotected data and poor cybersecurity practices in place, thus making them vulnerable to security breaches. Cybersecurity awareness campaigns and educational programmes, prevention and developing a cybersecurity culture would help address the problems. Binwal (2015) advocated for a cybersecurity governance framework that focuses on the key components of a governance structure. A cybersecurity framework actually contains a whole set of management tools, a comprehensive risk management approach and a security awareness programme covering everyone in the organisation from top to bottom. Abukari and Bankas (2020) concurred that security awareness programmes are key to educating and training teleworkers to equip them in identifying potential threats. Teleworkers, organisations and government agencies must be very vigilant and work together to combat cybercrime in this COVID-19 pandemic era.

Cybersecurity governance frameworks

The Australian Criminology Institute (2020), Stein and Jacobs (2020) disagreed that awareness campaigns alone are not adequate to deter would-be cybercriminals. However, concerted efforts from all stakeholders are required to develop cogent cybersecurity governance frameworks, code

of conduct and relevant interventions that deter unethical behaviour. The United Nations Conference on Trade and Development (UNCTAD) (2019) has warned that developing countries are increasingly being targeted by cybercriminals because of the lack of enforcement of relevant legislation. As a result of risk factors associated with people who operate, manage or use any organisational services or assets, a cybersecurity governance framework should be implemented. Strategies to maintain cybersecurity include maintaining good cyber hygiene, verifying sources and staying up-to-date on official updates (Abukari & Bankas 2020).

Chigada (2020) stated that ISRM, information systems management benchmarking and Business Continuity Guide can be used to assure the implementation of security. Da Veiga and Eloff (2017) suggested that corporate executives and board of directors should invest a large amount of resources for security measures. Ohki et al. (2009) suggested the adoption and use of the ISG Framework as key portion of corporate security programme. The ISG comprises several elements (stakeholders, auditors, managers, corporate executives, information security management and enterprise). Information security incidents require quick decisions and actions to reduce information losses (Ohki et al. 2009).

Cybersecurity protocols

Cybersecurity protocols for those using teleworking in the era of the COVID-19 pandemic and other security domains such as social engineering, fake news and applications, encryption schemes protocols (educational protocols individuals and training protocols for the organisation) should be used (Abukari & Bankas 2020). Certain protocols need to be observed, as such attempts may help ease the pressure on the cyber landscape if the digital platform governance is taken seriously at different levels in the organisation. It is these continuous improvement initiatives that make a difference in being proactive rather than reactive in the pandemic era and thereafter. Desktop sharing that provides organisations with the privilege of sharing files in real time remotely has authentication challenges. Moreover, the use of VPNs for teleworkers face threats from hackers because of the use of unsecured WiFi networks at various locations. These unsecured WiFi network connections stand a chance of weakening the security protocols provided by VPNs (Abukari & Bankas 2020).

Employees working from remote locations should use the VPNs. Whilst not specific to remote access, strict information security policies (including data access control and extensive logging and monitoring policies) underpin remote access security. Some firms have had weaknesses in the implementation of such policies and are, therefore, more likely to be successfully attacked during the pandemic (International Monetary Fund [IMF] 2020). Robust controls over configurations at both ends of the remote connection should be implemented to prevent potential malicious use. This entails that employees should not have administration rights on company-owned notebooks, security configurations and up-to-date endpoint security solutions should be in place (IMF 2020).

Firms should implement additional security controls for critical functions that are normally not allowed to work remotely. For example, users performing such assignments should only connect using firm-owned and controlled devices that are fully patched and configured to high security levels. The study established that authorities should issue further guidance that outlines the risk and references to existing relevant guidance (if there is one in place) and provides further details if needed.

Limitations and suggestions for research

This study was confronted with methodological limitations in that there were a few limited studies carried out under stringent movement and social distancing conditions. Citing prior research studies forms the basis of the literature review and helps lay a foundation for understanding the research problem under investigation. The period considered (December 2019–June 2020) was too short to have generated many studies related to cyberattacks and threats during the COVID-19 pandemic. Thus, with limited studies, the researchers could not extrapolate pertinent information regarding the impact of cybercrimes during the novel coronavirus. Depending on the currency or scope of the research topic, there may be little, if any, prior research on the topic (Saunders et al. 2019). For future research, the researchers recommend that a similar study be conducted after one year because there would be more studies, which might shed more light regarding cybercrimes during the pandemic. The researchers recommend that future studies should be conducted to analyse the success of cybersecurity interventions devised by firms. Furthermore, the study recommends the establishment of a proactive approach towards cybersecurity protocols, cybersecurity governance frameworks and a total paradigm shift in employees' behaviour.

Conclusion

It has been demonstrated that cyberattacks and threats during the COVID-19 pandemic are rising exponentially, creating another wave of challenges for the global economy which is already reeling under the novel coronavirus. The objective of this study was to analyse the impact of cybercrimes on the global economy. In addition, the study also analysed common cybersecurity threats, attacks and information systems security vulnerabilities during the pandemic. The findings from the study revealed that cybercriminals were targeting financial services, healthcare and government departments at a time when the whole world's attention was diverted towards the novel coronavirus. Healthcare organisations used many devices to share confidential patient information, and thus, it was difficult to keep abreast with latest cyberattacks and threats. In some instances, the use of outdated medical devices

created opportunities for cybercriminals because the devices were not compatible with latest security protocols. These interventions can only become effective if all stakeholders work together. In conclusion, firms should assess their security needs, requirements and shortfalls taking into cognisance that a one-size-fits all cybersecurity strategy does not address cyberattacks and threats.

Acknowledgements

The authors acknowledge their families for supporting them during the time of compiling and putting this research article together. Most of the discussions to brainstorm the ideas took place after normal working hours, which in most instances were family times. The families were very supportive.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this research article.

Authors' contributions

The authors contributed significantly to the development of the article. J.C. conceptualised the idea and shared it with R.M. J.C. developed the structure and key issues of the article. R.M. was responsible for identifying research articles that resonated with the study. In addition, R.M. did the write-up and handed it to J.C. for editing and final structure and submission of the article to the Journal.

Ethical consideration

This article followed all ethical standards for research. Secondary data was used in this study.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

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 and Engineering Research* 11(4), 1401–1407.

Aldawood, H. & Geoff, S., 2020, 'Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal, 2019–2020', *International Journal of Security* 10(1), 1–15.

Australian Institute of Criminology, 2020, 'Availability of COVID-19 related products on Tor darknet markets', *Statistical Bulletin* 24, viewed 09 June 2020, from https://ssm.com/abstract.

Babbie, E. & Mouton, J., 2012, *The practice of social research*, Oxford University Press, Cape Town.

Balsom, W. & Dixon, D., 2020, 'How COVID-19 shows the urgent need to address the cyber poverty gap', *World Economic Forum-Cybersecurity*, viewed 09 May 2020, from https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/.

Bayhack, J., 2020, 'Cybercrime continues during COVID-19', *Bizcommunity*, viewed 15 May 2020, from https://www.bizcommunity.com/Article/196/661/203999.html.

Binwal, P., 2015, *Creating a cybersecurity governance framework: The necessity of time, security intelligence and analytics*, viewed 29 January 2020, from https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/.

Centers for Disease Control, 2020, *Coronavirus disease 2019 (COVID-19)*, viewed 20 May 2020, from https://www.cdc.gov/media/dpk/diseases-and-conditions/coronavirus/coronavirus-2020.html.

Checkpoint Risk Intelligence, 2020, *27th April-Threat Intelligence Bulletin*, viewed 06 May 2020, from https://research.checkpoint.com/2020/27th-april-threat-intelligence-bulletin/.

Chigada, J., 2020a, 'Towards an aligned South African national cybersecurity policy framework', Unpublished PhD thesis, University of Cape Town, Cape Town.

Chigada, J., 2020b, 'A qualitative analysis of the feasibility of deploying biometrics authentication systems to augment security protocols of bank card transactions', *South African Journal of Information Management* 22(10), a1194. https://doi.org/10.4102/sajim.v22i1.1194

Chigada, J. & Hirschfelder, B., 2017, 'Mobile banking in South Africa: A review and directions for future research', *South African Journal of Information Management* 19(1), 1–9. https://doi.org/10.4102/sajim.v19i1.789

Chigada, J. & Kyobe, M.E., 2018, 'Evaluating factors contributing to misalignment of the South African National Cybersecurity Policy Framework', *International Conference on Information Resources Management (CONF-IRM 2018 Proceedings 4)*, viewed n.d., from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1012&context=confirm2018.

Cook, A., 2020, *COVID-19: Companies and verticals at risk for cyberattacks*, viewed 04 May 2020, from https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/.

Council of Europe Cybercrime Convention Committee, 2020, *Towards a Protocol to the Convention on Cybercrime: Additional stakeholder consultations*, viewed n.d., from https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations.

Crisanto, J.C. & Prenio, J., 2020, *Financial crime in times of COVID-19 - AML and cyber resilience measures, bank for international settlements*, viewed 15 October 2020, from https://www.bis.org/fsi/fsibriefs7.htm.

Cybersecurity Ventures, 2020, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', *Cybercrime Magazine*, viewed 13 June 2020, from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

Da Veiga, A. & Eloff, J.H.P., 2010, 'A framework and assessment instrument for information security culture', *Computers and Security* 29, 196–207.

Department of Health, 2020, *COVID-19 statistics*, viewed 12 June 2020, from www.health.gov.za.

Dewey, A. & Drahota, A., 2016, *Introduction to systematic reviews: Online learning module, Cochrane training*, viewed 10 October 2020, from https://training.cochrane.org/interactivelearning/module-1-introduction-conducting-systematic-reviews.

Dixon, W. & Balson, D., 2020, *How COVID-19 shows the urgent need to address the cyber poverty gap,* viewed n.d., from https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/.

Frost & Sullivan, 2016, *Artificial intelligence systems poised for dramatic market expansion in healthcare,* viewed 11 April 2020, from ww2.frost.com.

Fuentes, M.R., 2020, 'An investigation into the current condition of underground markets and cybercriminal forums', *Trend Micro*, viewed 09 June 2020, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark.

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*, viewed 08 February 2020, from https://www.martindale.com/industry-group/goldberg-segalla-llp-5000609/Cybersecurity-and-Data-Privacy/.

Gravrock, E.V., 2019, 'Here are the biggest cybercrime trends of 2019', *World Economic Forum*, viewed 19 April 2020, from https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/.

International Monetary Fund (IMF), 2020, *A crisis like no other, an uncertain recovery*, viewed n.d., https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020.

International Telecommunications Union [ITU], 2020, 'Regional cybersecurity forum for Europe and CIS', 27–28 February, Sofia Bulgaria, viewed 13 March 2020, from https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2020/CSF/SofiaBG.aspx.

Interpol, 2020, COVID-19 cyberthreats, viewed 24 May 2020, from https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

Isa, M., 2020, *SA suffers as cybercrime rises globally*, viewed n.d., from https://m.fin24.com/Finweek/Business-and-economy/sa-suffers-as-cybercrime-rises-globally-20200106.

Khan, N.A., Brohi, S.N. & Zaman, N., 2020, *Ten deadly cybersecurity threats amid COVID-19 pandemic,* IEEE, Researchgate publications, Berlin.

Lederer, A.L. & Mendelow, A.L., 2013, 'Issues in information systems planning', *Information and Management* 10(5), 245–254. https://doi.org/10.1016/0378-7206(86)90027-3

Magome, M., 2020, 'South Africa sees sharp rise in virus, part of African wave', *Associated Press*, viewed n.d., from https://www.usnews.com/news/world/articles/2020-12-10/south-africa-sees-sharp-rise-in-virus-part-of-african-wave.

Munn, Z., Peters, M., Stern, C., Tufanaru, C., McArthur, A. & Aromataris, E.C., 2018, 'Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach', *BMC Medical Research Methodology* 18(1), 143. https://doi.org/10.1186/s12874-018-0611-x

National Institute of Communicable Diseases [NICD], 2020, *Latest confirmed cases of COVID-19 in South Africa (10 June 2020)*, viewed 10 June 2020, from Replace with: https://www.nicd.ac.za/latest-confirmed-cases-of-covid-19-in-south-africa-10-june-2020/.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T. & Kagaya, T., 2009, 'Information security governance framework', *Proceedings of the First ACM Workshop on Information Security Governance* (WISG '09, 1), Chicago, USA, November 13, 2009, pp. 1–5.

Palmer, D., 2020, 'DDoS attacks are getting more powerful as attackers change tactics', *ZDNet*, viewed n.d., from https://www.zdnet.com/article/ddos-attacks-are-getting-more-powerful-as-attackers-change-tactics/.

Payne, G. & Payne, J., 2004, *Key concepts in social research*, Sage Publications, London.

PwC, 2020, *Impact of COVID-19: The World has changed and so have we*, viewed n.d., from https://www.pwc.co.za/en/about-us/integrated-report-2020/impact-of-covid-19.html.

Quade, P., 2020, 'A deep dive into the universe of cybersecurity: The digital big bang', World Economic Forum COVID Action Platform, viewed 08 February 2020, from www.weforum.org.

SABRIC, 2020, *Identity theft*, viewed n.d., from https://www.sabric.co.za/stay-safe/identity-theft/.

Saunders, M., Lewis, P., Thornhill, A. & Bristow, A., 2019, *Research methods for business students,* 8th edn., Pearson Publishers, Harlow.

Simonovich, L., 2020, 'Are utilities doing enough to protect themselves from cyber-attack?', *World Economic Forum*, viewed 09 May 2020, from https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/.

SonicWall, 2020, *Cybersecurity threat report*, viewed n.d., from https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/.

Stein, S. & Jacobs, J., 2020, 'Cyber-attack hits U.S. Health Agency amid COVID-19 outbreak', *Bloomberg*, viewed 20 March 2020, from https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

Stevens, T., 2018, 'Global cybersecurity: New directions and methods', *Politics and Governance* 6(2). https://doi.org/10.17645/pag.v6i2.1569

SwivelSecure, 2020, *9 reasons why healthcare is the biggest target for cyber-attacks,* viewed 10 June 2020, from https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

Takahashi, Y., Uchida, C., Miyaki, K., Sakai, M. Shimbo, T. & Takeo, N., 2009, 'Potential benefits and harms of a peer support social network service on the Internet for people with depressive tendencies: Qualitative content analysis and social network analysis', *Journal of Medical Internet Research* 11(3), e29.

Tranfield, D., Denyer, D. & Smart, P., 2003, 'Towards a methodology for developing evidence-informed management knowledge by means of systema review', *British Journal of Management* 14, 207–222.

United Nations Conference on Trade and Development (UNCTAD), 2019, *World investment report*, viewed 30 April 2020, from https://unctad.org/webflyer/world-investment-report-2020.

Vlachos, V., 2011, 'The landscape of cybercrime in Greece', *Information Management and Computer Security* 19(2), 113–123. https://doi.org/10.1108/09685221111143051

White, K., 2020, *Life healthcare reports hacking attack*, viewed 14 June 2020, from https://www.businessday.co.za.

World Bank, 2019, *World development report: The changing nature of work,* viewed 19 May 2020, from https://www.worldbank.org/en/publication/wdr2019.

World Economic Forum, 2020, *COVID-19 risks outlook: A preliminary mapping and its implications*, viewed n.d., from https://www.weforum.org/global-risks/reports.

World Economic Forum, 2019, *Global risks report: Global risks perception survey 2018–2019*, viewed 09 March 2020, from https://www.weforum.org/reports/the-global-risks-report-2019.

World Health Organization (WHO), 2020a, *Beware of criminals pretending to be WHO*, viewed 24 May 2020, from https://www.who.int/about/communications/cyber-security.

World Health Organization (WHO), 2020b, *Modes of transmission of virus causing COVID-19: Implications for IPC precaution recommendations*, viewed 24 May 2020, from https://www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations.

World Health Organization (WHO), 2020c, *Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019- nCoV)*, 2020, viewed 14 May 2020, from https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov).