Impact of Information Security Threats on Small Businesses During the Covid-19 Pandemic

Inga Mzileni and Tabisa Ncubukezi
Information Technology Department, Faculty of Informatics and Design, Cape Peninsula University of Technology, Cape Town, South Africa
nizoinga6@gmail.com
ncubukezit@cput.ac.za

Abstract: Information is a significant asset of any organization. The increased information demand by all parties has gained attention and raised security concerns – especially in this digital era where everyone depends heavily on the Internet. The Internet and online platforms expose valuable information to various information threats. These pervasive threats compromise information privacy, safety, and security. Legitimate people and criminals compete to access information. Criminals use innovative ways to gradually increase information security threats, especially in the small business sector with only a minimal budget for proactive security measures. Due to the scarcity of academic research on information security threats for small businesses, this study presents the impact of security threats on businesses during the global Covid-19 pandemic. A qualitative survey within the interpretive approach was used to gather data from 20 small businesses in Western Cape, South Africa, to fill this gap. The study used judgmental sampling to select research participants who are business owners. Data were analyzed using thematic analysis. The results indicated the knowledge gap relating to information threats, even though most businesses are familiar with the costly and negative impact of threats on business operations, resulting in business discontinuity. However, some small business sectors showed minimal awareness a6nd understanding of information security threats, their impact, and proactive mitigation strategies. The study concluded with recommendations to protect against information security threats.

Keywords: cyber-attacks, cyber security, information security, information security threats, internet, small businesses

1. Introduction

Globally, all institutions possess valuable information related to assets, financial payments, customers, personal identification, and payment cards. The global Covid-19 pandemic forced all institutions to exchange information on the Internet, granting access to legitimate users and criminals. This process exposes information to threats that render the small business sector vulnerable (Ncubukezi & Mwansa, 2021). Small business exposure to information threats negatively impacts their daily activities, resulting in numerous business risks (Ncubukezi, Mwansa & Rocaries, 2020). The assets, information, and people associated with the small business sector become vulnerable and exposed to malicious attacks, compromising the state of a business. Examples of information security threats include software attacks, intellectual property theft, and sabotage (Holovkin, Tavolzhanskyi & Lysodyed, 2021).

Information security threats gradually increase, leading to data loss, corruption, and disruption of normal business operations (Whitman & Mattord, 2021). Consequently, the safety of business information and other assets is a substantial concern, especially when a business relies on the Internet. The presence of information security threats among small businesses can result in a significant data breach: loss, manipulation, or deletion (Biener, Eling & Wirfs, 2015).

Cyber security has escalated in the challenge, especially during the global pandemic, as opportunities for hackers, attackers, and scammers to take advantage of emergencies are prevalent, especially when people are frightened (Khan, Brohi, Zaman & 2020:2). This work, then, focuses on the impact of information security threats among small businesses during the Covid-19 pandemic. To achieve this, the paper:

- identifies the persuasive information security threats;
- determines the impact of information security threats on small businesses; and
- determines measures to protect against information security threats.

The entire paper is laid out as follows: the subsequent sections address the literature review, research methodology, results, and discussions, followed by recommendations and concluding remarks.

2. Literature review

The coronavirus pandemic (Covid-19) started in 2019 and quickly escalated into a global crisis, resulting in the mass quarantine of citizens worldwide. Global restrictions forced all institutions, including small businesses, to operate from homes (Georgiadou, Mouzakitis & Askounis, 2021), which increased Internet dependency on routine business activities (Ncubukezi, Mwansa & Rocaries, 2021). In recent times, as businesses globally face transformation, most have become increasingly innovative, competitive, and challenging, while concomitantly, security risks targeting information systems have also increased (Gerić & Hutinski, 2007). Small businesses are frequently receiving threats and attacks (Akpan, Udoh & Adebisi, 2020). Small businesses are presented below.

2.1 Overview of small business

'Small' in terms of qualifying for government support and preferential tax policy varies by country and industry. The business sector is determined by size, with small to medium-sized (SMEs) businesses employing fewer than 200 employees. Small businesses can be privately owned corporations, partnerships, or sole proprietors with fewer employees and lower annual revenue than a corporation or regular-sized company (Itliong, 2020). Small businesses generally employ a range of 50 to 60% of South Africa's workforce and contribute significantly to around 34% of the gross domestic product (GDP) (IFC World Bank Group, 2021). Small businesses contribute to GDP (Paulsen & Toth, 2016).

Small businesses employ fewer than 50 employees in comparison to medium businesses, with some employing fewer than 20 depending on the industry and micro sizes. This study focuses on SMEs that operate as Internet cafés with 3 to 10 employees, depending on the number of services a manager undertakes. For example, Internet cafés typically provide Internet services, information and communication technology (ICT), and document services such as faxing, copying, and printing.

2.2 Impact of Covid-19 among businesses

In recent times, global businesses have grown increasingly competitive, with small businesses often on the receiving end. When the coronavirus pandemic (Covid-19) started in 2019 and quickly became a global crisis, the world saw the mass quarantine of hundreds of millions of citizens worldwide. Covid-19 pandemic-imposed lockdowns in most nations affected all industries and service sectors. The pandemic is anticipated to permanently normalize the Internet use and continue to force businesses to adopt online service strategies (Herath & Herath, 2020). The rapid and massive shift to online revealed a concern for small businesses. For the most part, they do not have sufficiently trained staff for the new and unfamiliar tools now necessary to remain competitive in these trying times. This inexperienced sector with minimal skills in technology usage has become easy target (Monteith et al., 2021), especially as many people, including businesses, perform their daily activities at home relying on a connection to the Internet, even though the small business sector does not have diverse IT and cyber security personnel compared to large enterprises (Ikpe et al., 2020). As a result, most small business managers have little understanding of information security and security threats.

2.3 Why information security?

As one of the main business assets, information should always be protected and guarded against pervasive, disruptive, intruding threats (Lundgren & Möller, 2019). Information security sometimes referred to as InfoSec, defends information from unauthorized access, use, disclosure, alteration, recording, inspection, or recording (Alhassan & Adjei-Quaye, 2017). Consequently, information security should be prioritized in all institutions. Information security practice prevents unauthorized access to information, unauthorized data modification, and deletion of data. The network and the computer are the main tools used to deploy data breaches, commonly coming as viruses, spam, phishing, and identity theft. These data breaches compromise the confidentiality, integrity, and availability (CIA) of business information, the fundamental information security principles (Zafar, Ko & Osei-Bryson, 2016).

Figure 1 shows the three primary components of the CIA triad – confidentiality, integrity, and availability – for guiding the sector's security procedures and policies (Moura & Serrao, 2016). The confidentiality component promotes data availability to those with the proper authorization, while the integrity principle focuses on information consistency, accuracy, and trustworthiness. Finally, the availability principle ensures easy access to

authorized recipients (Thapa & Camtepe, 2021). These principles protect a business's digital assets against ever-looming cyber-attacks.

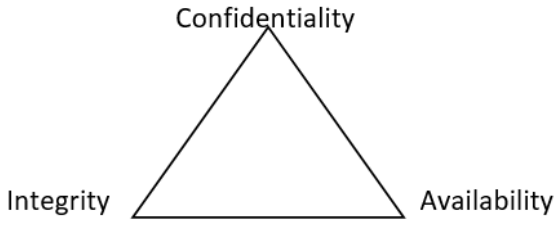

Figure 1: CIA triad security principles (Moura & Serrao, 2016)

As the key aspect of every business, information security aims to ensure business continuity and minimize unforeseen damages by limiting the impact of security incidents (Von Solms & Van Niekerk, 2013). Information security measures are required because the technology applied to information creates risk and is important to an organization's dependence on information technology. This is significant when an organization's information is exposed to risk. As failures of information security measures are adverse events that cause business losses, information security risk management is essential for every business (Blakley, McDermott & Geer, 2001).

2.4 Security threats

The global pandemic has revealed the state of safety and security of businesses. A successful business prioritises the security of the business at all levels, namely: personnel, network, systems, hardware and information. Improved safety and security includes the protection of sensitive data, personally identifiable information, protected health information, and governmental and industrial information systems from theft and damage attempted by criminals and adversaries. Increased Internet usage by businesses necessary for visibility in the market to attract new prospects, increase profit and improve communication has exposed all sectors to a diverse range of security threats, such that security threats are presently a major challenge within the small business sector.

But in these trying times, the overall security of small businesses is undeniably challenging. Hackers, attackers, and scammers take advantage of emergencies, primarily when people are frightened (Khan, Brohi & Zaman, 2020). Cyber-attacks result in a leakage of financial information, among other losses, which damage businesses. Therefore, the safety of business information is a critical and significant concern. Protecting computer operating systems, networks, and data from cyber-attacks requires special skills and knowledge. Heidt, Gerlach, and Buxmann (2019) confirm that most small institutions do not have a budget to hire IT specialists to secure their systems. This opens the door for crimes within the business sector that threaten security. Cybercrimes are human-generated and can be planned or unplanned (Ncubukezi, 2022).

2.5 Cybercrime

Cybercrimes are typically regarded as computer crimes because criminals use a computer as a tool to commit illegal actions such as fraud, identity theft, or privacy violation (Monteith et al., 2021). Cybercrime is often described as a crime triangle, which specifies that for cybercrime to occur, three factors must exist: a victim, a motive, and an opportunity (Lallie et al., 2021). In such a scenario, the victim is the target of the attack while the motive forces information threats and attack, and the opportunity presents a chance for the crime to occur (Lallie et al., 2021). Due to the valuable information possessed by small businesses, they are ready targets of cyber-attacks and crimes.

Cybercrimes corrupt the state of security of the business's hygiene at all levels of information. The Covid-19 pandemic gave both legit users and criminals equal chances to perform activities in the business space. As victims of criminal intentions, businesses are easy cyberspace victims (Ncubukezi, Mwansa & Rocaries, 2020). Some attackers select victims based on susceptibility to an attack; these attacks are called opportunistic attacks. Opportunistic attackers seek to maximize their gain and, therefore, wait for the best time to launch an attack where conditions fit.

3. Related work

The Covid19 global pandemic has caused a panic to many institutions. The global pandemic raised cybersecurity related issues especially during the "new normal." As a results there are a number of studies that have been conducted in relation to the impact of the global pandemic. A study conducted by Georgiadou, Mouzakitis and Askounis (2021) evaluated cyber security culture readiness among the organizations that are based on various countries. In year 2020, their study used online surveys with 23 questions to collect data from 264 employees working at home during the sudden Covid19 pandemic. The results of their study were discussed and recommendations addressed both vulnerabilities and needs for security culture.

Another study analysed the cyber-crime during COVID-19 pandemic focusing on the variety of cyber attacks. The study revealed cyber-attack modus-operandi of campaigns and steadily attacks which ultimately became prevalent resulting to a maximum of three attacks being reported a day (Lallie et al., 2021). In addition, Pranggono and Arabo (2021) studied cybersecurity issues that have occurred during the coronavirus (COVID-19) pandemic. Their paper addressed the correlation between the cyber attacks, their risks caused and the pandemic which increased anxiety and fear. In their study it came out that the healthecare sectros are mostly vulnerable to cyber attacks. The study recommended the practical approaches that proactively reduce cyber-attacks related risks among the sector. the impact of the information security threats among the small business sectors during the hitting global pandemic. The study is conducted in South Africa, Cape Town. A total of twenty small businesses were sampled and the results were reported and discussed.

4. Research method

While there are numerous research designs, the most prominent five are as follows: narrative research, phenomenology research, grounded theory research, ethnology research, and case study research. Phenomenology provides the best approach for this study. In the phenomenological approach, the focus describes the meaning for individuals of their lived experience of a concept. The study describes what all participants have in common as they experience the phenomenon. Phenomenology has two methods: hermeneutic phenomenology – the theory and methodology of interpretation; and empirical phenomenology – minimal focus on the interpretations of the research and more on describing participant experiences.

Qualitative approach: The study adopts a qualitative interpretation research paradigm to study the research participants in their natural setting and understand opinions and perceptions. The approach provides great value in relation to diverse environmentns and phenomena by describing events or experiences of the research participants from a wide range of sectors and different roles. So this study reports the information security threats among small businesses during the Covid-19 pandemic. This qualitative interpretive research gathers data from small businesses. The approach helps to develop concepts and visions for problems. For this study, the researchers were interested in the meaning and meaning-making process because qualitative data never speaks for itself but needs to be given meaning.

Research participants: The study focused on male and female small business managers and owners, between 23 and 30 years old, as research participants. Business owners and managers, knowledgeable about business systems, are responsible for overall business management. These participants were invited to participate in the study through emails. Only those who voluntarily responded to the communication request were part of the study. None of the participants were reminded or persuaded to participate in the study. The selection of the sampling method used in the study is presented below.

Sampling and data collection method: Twenty (20) participants were selected using judgemental sampling within the qualitative interpreting approach. The chosen sampling method helps researchers get more information on the collected data. In addition, it helps to describe the findings of the main impact based on the population. Information gathered will be used for research purposes to achieve the aim of the study. Due to national and global restrictions, this work used an online survey, created on Google Forms, as the data collection method. This was the most convenient data collection method available. The researcher sent email invitations to small business managers. Those willing to participate responded and were sent a link to complete a qualitative online survey. The study received an 85% response rate.

Data analysis: Data analysis provides theorized and interpretative accounts, socially located explorations of experiences (Braun et al., 2021), and sense-making of information security threats to small businesses. Data

gathered from the qualitative survey were analyzed using thematic analysis. The researcher examined the collected data to identify common themes relating to repeated topics, ideas, and patterns. The researcher further worked with the data collected during the analysis and assigned preliminary codes to describe the content. The researcher searched for themes in the codes across different responses. The themes analyzed in the study were as follows:

- participant background;
- common threats experienced by small businesses;
- impact of information security threats, and
- security measures to improve small business security.

Themes were reviewed, defined, and named to produce a report. These themes are clearly presented in the results and discussion section.

Ethical considerations: The researcher, having received ethical clearance from the departmental ethics committee, assured respondents of confidentiality, privacy, and anonymity. The information collected in this study is only used for research purposes. In addition, research participants were not forced to participate in the study and were given sufficient time to decide. The participation was voluntary, and the participants were made aware to withdraw at any time without fear of consequences.

5. Results and discussions

This section reports the experiences of the small business with the impact of information security threats. Results are presented according to the pervasive information security threats, their impact, and the measures used to protect against these information security threats in the small business sector.

5.1 Participant background

Data were collected from Internet café businesses in South Africa in Western Cape. The male and female participants were adults aged between 23 to 30 years. The participants were selected from the townships in the Western Cape. Most businesses have been operating for over eight (8) years, while others are still in the early years, just finding their feet in the business world. All participants use cyberspace to attract new prospects and engage in daily business activities, making them vulnerable to various information threats. Figures 2 to Figure 4 illustrate participant gender, participant age, and the number of years of each business.

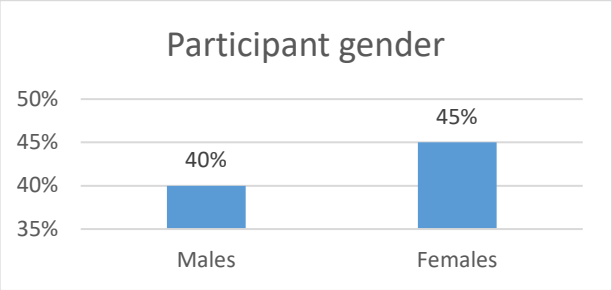

Figure 2: Participant gender

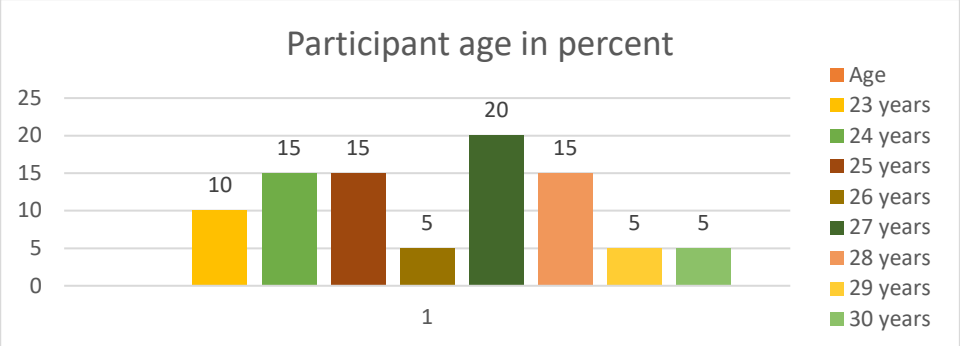

Figure 3: Participant age

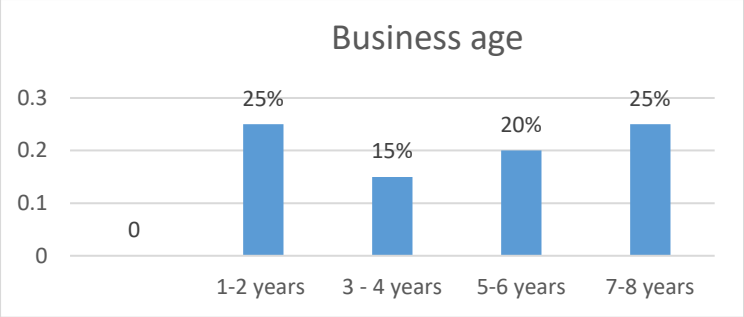

Figure 4: Business age

5.2 Common information threats

When asked about pervasive information security threats that the small business sector experiences, participants indicated that they are exposed to phishing, unauthorized access, modification of data, spyware, Trojan horses, and malware.

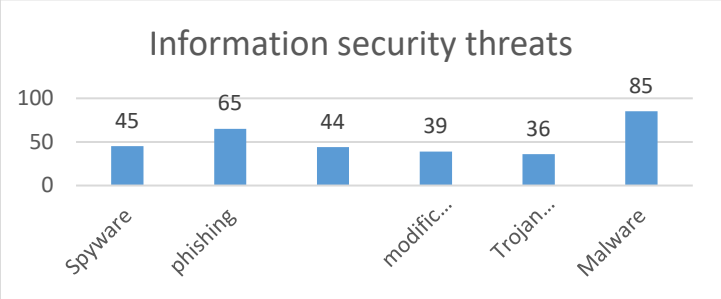

Figure 5: Information threats

Figure 5 shows information security threats that businesses experienced: 45% of the businesses experienced spyware, 65% phishing, 44% unauthorized access, 39% modification of data, 36% Trojan horses, and 85% malware attacks. The results show that all the selected businesses were victims of information threats. The impact of the information threats weakens business information confidentiality, integrity, availability, and authorized access. Information threats are intrusive and disconcerting attacks within the small business sector. All businesses need to identify the intruding information threats which increased during the global pandemic. Identifying the information security threats influences the strategies that can be used to mitigate the risks caused by information threats (Fedushko & Benova, 2019). Businesses experience these information threats through the use and access to ICT resources. Spyware, phishing, and Trojan horses result from connection to the Internet. Even though cyberspace brings convenience to businesses, equally this access opens channels for increased information threats. Dependency on the Internet and other information and communication technologies continue to expose all business sectors to threats (Ncubukezi & Mwansa, 2021).

In addition, the information threats can be caused by employee ignorance, resistance to change, mischievous behaviors, minimal awareness levels, and access to unknown websites (Safa et al., 2018). Likewise, other information threats are often caused by memory sticks and external hard drives. The following section presents the impact of these information threats (Ncubukezi, 2022).

5.3 Impact of information threats

When asked about the impact of information threats, participants shared their experiences that affect the business assets, people, systems, and information. Criminals intentionally exploit business systems to gain unauthorized access. Businesses experience data manipulation, which ultimately leads to data breaches. Even though some businesses have established mitigation strategies, other businesses experience denial of service, unavailability of data; unauthorized access; and compromised confidentiality, privacy, and integrity, which ultimately cause data breaches. These information security breaches are caused by insiders and outsiders (Ncubukezi, 2022). Insider information threats are often caused by employee ignorance, poor decision making, lack of skills, poorly enforced security strategies, understaffing, poor security guidelines, and a technological knowledge gap (Kluge, Sasse & Verret, 2022; Singh & Singh, 2022).

When security for business resources has not been appropriately implemented, businesses are vulnerable to various threats. Information security threats – software attacks, intellectual property theft, identity theft, equipment or information, sabotage, and information extortion (Deeks, 2020) – severely impact business information. The results of information security can diminish a business's reputation and hinder financial groups (Ncubukezi, 2022). Figure 6 illustrates the impact of information threats.

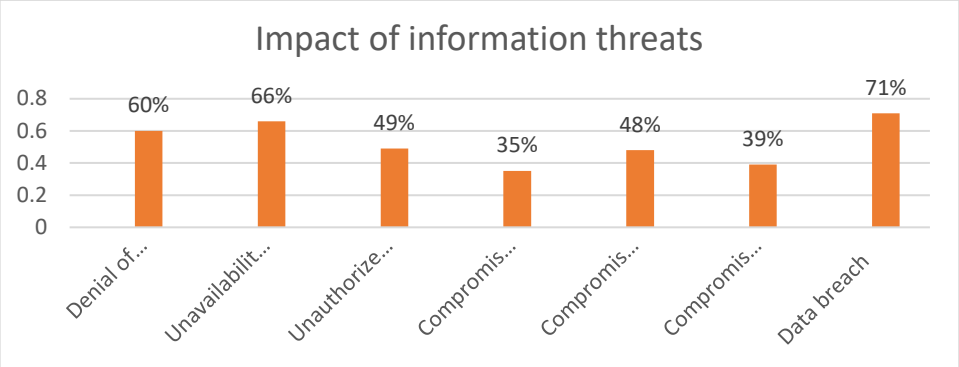

Figure 6: Impact of information threats

5.4 Measures to protect against the information security threats

When businesses were asked about security measures, participants indicated that they use passwords to protect sensitive information and resources. However, passwords are ineffective if they are not regularly updated or meet acceptable password criteria. Weak passwords cause a major loophole in the system (Jiow, Mwagwabi & Low-Lim, 2021). Firewalls detect information security threats penetrating the system (Emm, 2013). The lack of firewalls within the small business space increases the chances of unauthorized access to the system. An effective firewall filters both the incoming and outgoing traffic on the network. According to Okoye (2017), most managers are concerned about the confidentiality of an organization's operational data rather than protecting the firm's knowledge and information assets. Hutchings, Smith, and James (2013) suggest that "small businesses face several computer security threats and may lack the time and technological resources that enable software updates and patches that improve security." Due to the severity of risks caused by the global pandemic, software manufacturers improve their security by updating and edifying software patches; failure to run software updates exposes systems to a diverse range of threats.

The small business sector should invest in securing overall resources and information. They should adopt alternative and advanced strategies to detect early warning signs. In addition, businesses should adopt cloud storages that will serve as a secure backup system, as cloud storage has a high level of security which will heighten the safety and security of information. The idea is to back up data according to each business's need, especially free cloud storage, likely meeting small business needs (Hutchings, Smith & James, 2013). Businesses should also always have up-to-date antivirus and antispyware. When business devices are connected to the network, the devices with antivirus and antispyware will automatically run updates to detect abnormalities on the business network and system. In addition, device encryption is used to improve security.

Data can be protected in multiple ways. Small businesses need a security strategy to protect their own business, customers, and data. Information security threats always scope for ways to gain access into a system, detrimentally impacting businesses, resulting in data loss, device theft, breaches, and financial loss. All businesses encounter different information risks based on their services, but all are impacted negatively by information threats. Security threats include everything that protects sensitive data, personally identifiable information, protected health information, and governmental and industrial information systems from theft and damage attempted by criminals and adversaries. Protecting computer operating systems, networks, and data from cyber-attacks requires special skills and knowledge. It may be expensive for growing businesses to hire an IT specialist to secure their systems.

Table 1: Summary of research questions about mitigation strategies

Questions	Measures used	Business responses
What security measures do businesses implement?	Passwords	100% of the respondents indicated that they use passwords despite not complying with the accepted password criteria or regularly updating them.
	Firewall	60% of the respondents indicated that they have a firewall, and another 40% do not use a firewall to filter incoming traffic.
	Backup system and cloud storage	68% of the businesses back up their information on the cloud, while 32% do not back up their information. Instead, they trust their hard drives.
	Software updates and patches	56% of the businesses automatically run software updates which increase the safety and security of information. Some businesses do not run software updates, which creates a loophole for various information threats.
	Antivirus and antispyware	40% of the respondents operate on stand-alone devices which do not allow automatic antivirus updates and antispyware.

5.5 Recommendations and future research

The evident increase in cyber-attacks within small businesses in South Africa requires investment in proactive defensive technologies to reduce information risks and threats. Approximately 43% of cyber-attacks are aimed particularly at small businesses in the health, insurance, retail, financial and legal sectors (Ginindza, 2021). The research participants shared their experiences with information security threats and the impact on small businesses, especially Internet cafés. The study revealed a need to equip small businesses with ways to combat information security threats. Effective information security requires enforced policies, training management, and established security controls (Cheung, 2014). The small business sector should be aware of the information threats to effectively protect against their assets and infrastructure before deploying security measures (Anderson, 2003). Pranggono and Arabo (2021) suggest using a virtual private network continuous training for system end-users. Due to high exposure to information threats during the Covid-19 pandemic, the following are recommended for businesses:

- Implement security on information, systems, network, devices, and personnel.
- Always use firewalls to filter incoming and outgoing traffic.
- Use virtual private networks (VPNs) for secure Internet connections.
- Enforce strong password criteria.
- Regularly update software and restrict automatic installations, especially from unknown websites.
- Provide security training throughout the year, updated regularly.
- Use encryption and multi-factor authentication.

This study should include other business sectors in the future.

5.5.1 Contribution and significance

The global Covid-19 pandemic became a fertile season for information threats. It influenced the use of technology for reaching out to loved ones, other businesses, suppliers, and new business partners. The study's findings showed small businesses' current state of information security. First, this study gave insight into the current state of information security within the small business sector. Secondly, this study generated awareness about the current information security, its impact, and security measures in the small business sector. The more information available about information security, the better strategies can be established. And finally, this study challenged businesses to explore lasting and robust security strategies to strengthen information security.

6. Conclusion

The Covid-19 pandemic affected everyone and introduced new changes and rules, resulting in thousands of deaths, self-isolation, lockdown, and increased Internet dependency. Small businesses, in particular, have had to adapt and adopt new technologies, which have increased exposure and vulnerability to cyber-attacks and information threats. The study determined the nature of information security threats in the small business sector, threats that steal private and sensitive data, finances, and client information. The research revealed that

the small business sector is exposed to various information threats that negatively affect businesses. No business can avoid information threats. In addition, the study revealed the significant information security risks and the impact of intrusive information threats on the small business sector. In response, businesses shared their current security strategies for reducing business risks.

References

Akpan, I.J., Udoh, E.A.P. & Adebisi, B. (2020). "Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets, and lessons from the COVID-19 pandemic". *Journal of Small Business & Entrepreneurship*, pp. 1-18.

Alhassan, M.M. & Adjei-Quaye, A. (2017). "Information security in an organization." *International Journal of Computer (IJC)*, *24*(1), pp. 100-116.

Anderson, J.M. (2003). "Why do we need a new definition of information security." *Computers & Security*, *22*(4), pp. 308-313.

Biener, C., Eling, M. & Wirfs, J.H. (2015). "Insurability of cyber risk: An empirical analysis." *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), pp. 131-158.

Blakley, B., McDermott, E. & Geer, D. (2001). "Information security is information risk management." In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104).

Braun, V., Clarke, V., Boulton, E., Davey, L. & McEvoy, C. (2021). "The online survey as a qualitative research tool." *International Journal of Social Research Methodology*, *24*(6), pp. 641-654.

Cheung, S.K. (2014). "Information security management for higher education institutions." In *Intelligent Data analysis and its Applications, Volume I* (pp. 11-19). Springer, Cham.

Deeks, A. (2020). "Secrecy Surrogates." *Virginia Law Review*, *106*(7), pp. 1395-1477.

Emm, D. (2013). "Security for SMBs: Why it's not just big businesses that should be concerned." *Computer Fraud & Security*, 2013(4), pp. 5-8.

Fedushko, S. & Benova, E. (2019). "Semantic analysis for information and communication threats detection of online service users." *Procedia Computer Science*, *160*, pp. 254-259.

Georgiadou, A., Mouzakitis, S. & Askounis, D. (2021). "Working from home during COVID-19 crisis: a cyber security culture assessment survey." *Security Journal,* pp. 1-20.

Gerić, S. & Hutinski, Ž. (2007). "Information system security threats classifications." *Journal of Information and organizational sciences*, *31*(1), pp. 51-61.

Ginindza, B. (2021). "Work from home increases cyber-attack risks for SMEs" [Accessed on 13 March 2022] available from https://www.iol.co.za/business-report/companies/work-from-home-increases-cyber-attack-risks-for-smes-8991e5de-5bdc-48d5-afa0-3c8c56ff4a2a

Heidt, M., Gerlach, J.P. & Buxmann, P. (2019). "Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments." *Information Systems Frontiers*, *21*(6), pp. 1285-1305.

Herath, T. & Herath, HS (2020). "Coping with the new normal imposed by the COVID-19 pandemic: Lessons for technology management and governance." *Information Systems Management*, *37*(4), pp. 277-283.

Holovkin, B.M., Tavolzhanskyi, O.V. & Lysodyed, O.V. (2021). "Corruption as a cybersecurity threat in conditions of the new world's order." *Linguistics and Culture Review*, *5*(S3), pp. 499-512.

Hutchings, A., Smith, R.G. & James, L. (2013). "Cloud computing for small business: Criminal and Security threats and prevention measures." Tr*ends and Issues in Crime and Criminal Justice*, (456), pp. 1-8.

Itliong, J. (2020). Online Strategies For Small Businesses Affected By Covid-19: A Social Media And Social Commerce Approach. Masters Thesis California State University, San Bernardino.

Jiow, H.J., Mwagwabi, F. & Low-Lim, A. (2021). "Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education." *Journal of Media Literacy Education*, 13(1), pp. 67-78.

Kluge, A., Sasse, M.A. & Verret, I. (2022). "Why IT Security Needs Therapy." In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers* (Vol. 13106, p. 335). Springer Nature.

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

Lundgren, B. & Möller, N. (2019). "Defining information security." *Science and engineering ethics*, *25*(2), pp. 419-441.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P.C. & Glenn, T. (2021). "Increasing cybercrime since the pandemic: Concerns for psychiatry." *Current psychiatry reports*, *23*(4), pp. 1-9.

Moura, J. & Serrão, C. (2015). "Security and privacy issues of big data." In *Handbook of research on trends and future directions in big data and web intelligence* (pp. 20-52). IGI Global.

Ncubukezi, T. (2021). "Human errors: A cybersecurity concern and the weakest link to small businesses." *International Conference on Cyber Warfare and Security*, 17, pp. 395-403.

Ncubukezi, T. & Mwansa, L. (2021). "Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid19 Pandemic." *International Conference for Internet Technology and Secured Transactions* , 9, pp. 714–721.

Ncubukezi, T., Mwansa, L. & Rocaries, F. (2020). "Review of the current cyber hygiene in small and medium-sized businesses." *International Conference for Internet Technology and Secured Transactions,* 15, pp. 283–288.

Ncubukezi, T., Mwansa, L. & Rocaries, F. (2021). "An analysis of the cybercrimes within the Western Cape small and medium-sized enterprises." *International Conference on Cyber Warfare and Security*, 16, pp. 425-435.

Okoye, SI (2017). "*Strategies to minimize the effects of information security threats on business performance."* (Doctoral dissertation, Walden University).

Paulsen, C. & Toth, P. (2016). "*Small business information security: The fundamentals*." (No. NIST Internal or Interagency Reports (NISTIR) 7621 Rev. 1). National Institute of Standards and Technology.

Pranggono, B. & Arabo, A. (2021). "COVID-19 pandemic cybersecurity issues." *Internet Technology Letters*, 4(2), e247.

Safa, N.S., Maple, C., Watson, T. & Von Solms, R. (2018). "Motivation and opportunity-based model to reduce information security insider threats in organizations." *Journal of information security and applications*, 40, pp. 247-257.

Singh, I. & Singh, Y. (2022). "Cyber-Security Knowledge and Practice of Nurses in Private Hospitals in Northern Durban, Kwazulu-Natal. " *Journal of Theoretical and Applied Information Technology*, *100*(1).

Thapa, C. & Camtepe, S. (2021). "Precision health data: Requirements, challenges and existing data security and privacy techniques." *Computers in biology and medicine*, 129, p. 104130.

Von Solms, R. & Van Niekerk, J. (2013). "From information security to cyber security." *Computers & Security*, 38, pp. 97-102.

Whitman, M.E. & Mattord, H.J. (2021). "*Principles of information security*." Cengage Learning.

Zafar, H., Ko, M.S. & Osei-Bryson, K.M. (2016). "The value of the CIO in the top management team on performance in the case of information security breaches." *Information Systems Frontiers*, 18(6), pp. 1205-1215.