Global Journal of Management and Business Research: G Interdisciplinary
Volume 24 Issue 1 Version 1.0 Year 2024
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4588 & Print ISSN: 0975-5853

Mitigating Cyber-Attacks and Threats in South African Commercial Banks

By Tlhologelo Mphahlele & Joel Chigada
University of South Africa

Abstract- The increasing incidence of cybercrimes has become a pressing issue for society, businesses, and governments. Responding to the growing demand for digitisation from customers and investors, South African institutions have become targets of sophisticated cyberattacks. The financial sector, considered part of the country's critical infrastructure, has not been immune. The frequency of attacks on commercial banks in South Africa has risen, with several successful cyberattacks causing substantial harm. This paper explores the interventions commercial banks use in South Africa through a qualitative research lens. The results indicate that while technical interventions provide value, there are still opportunities for improvement in the human and process elements of the interventions. This highlights the need for a holistic approach to cybersecurity, incorporating technology, people, and processes to mitigate the risks posed by cyber threats effectively.

Keywords: *cyber threats, cyber-attacks, commercial banking, cybersecurity.*

GJMBR-G Classification: *JEL Code: G21*

Strictly as per the compliance and regulations of:

Mitigating Cyber-Attacks and Threats in South African Commercial Banks

Tlhologelo Mphahlele [α] & Joel Chigada [*]

I. Introduction

The rapid advancements in Information and Communication Technologies (ICTs), multiple industries and the globalisation of economies have seen an influx of technological innovations. The global financial services sector has undergone significant changes with the rise of Financial Technology (FinTech), including mobile Internet, cloud computing, Big Data, search engines and blockchain technology (Cheng, Li, Wu, & Luo, 2017). The introduction of digital services such as digital government, digital commerce, digital education, digital health, digital environment, and digital banking has enabled commercial banks to reach a wider audience without needing a physical location, albeit against a rising scourge of cybercrime (Chigada & Naailah, 2021).As cybercrimes continue to escalate in complexity and severity, financial institutions have become prime targets for criminals. These institutions offer more significant attack vectors due to the increased online services provided to their clients, making them vulnerable to cyberattacks (Chigada, 2023). However, the growth of online financial services has also led to increased information security and data breaches, which threaten economic interests, national security, and intellectual property (Tisdale, 2015).

The increasing frequency of cyber threats and attacks on financial institutions has led to the need for commercial banks to adopt interventions to mitigate these threats and attacks. These interventions range from technical solutions, such as firewalls, antivirus software and encryption, to people-oriented interventions, such as cyber awareness and training, and process-oriented interventions, such as incident response planning, risk management and security governance. While the technical interventions provide a degree of protection against cyber threats, the people and process-oriented interventions build a culture of security within the organisation and ensure that the technological interventions integrate into the bank's overall approach to cybersecurity. Chigada (2020) avers that unacceptable human behaviour requires attention. Individuals operate in a space where they determine what, why, how, and when to act in a specific way. Nyasvisvo and Chigada (2023) state that firms may put in pace cogent measures to curb cyber-attacks and data breaches, but nefarious and threat-actors are always a step-ahead in their acts. Therefore, it is best to implement continuous measures that include a culture of awareness, training and development and others that would deter would be-cybercrime.

A review of literature demonstrates the abundance of studies on cybercrime and information security challenges in financial institutions (Mabunda, 2019; Khan et al., 2020; World Health Organisation, 2020; Chigada & Madzinga, 2021). Most of these studies were conducted during the Corona Virus Disease-2019 (COVID-19) period. Post the COVID-19 period, there have been studies on cyber-attacks and threats on financial institutions, forced to pay ransomware, but there is a dearth of reports that suggested how financial institutions in South Africa have mitigated these cyber-attacks and threats. A preliminary investigation showed that financial institutions were not keen to share information security and cybersecurity issues given the sensitivity of clientele information managed by these institutions. We discovered that the South African Bank Risk Information Centre (SABRIC) collated most of the cyber-attacks and threats information for all banks in the country. Other financial institutions such as insurance companies, medical aid schemes etc reported their data breaches to specific sectors other than SABRIC. After engaging some participants, we discovered that institutions preferred to operate in silos for fear of exposing their strategies or company information. It is against this background that the present study examined interventions that are deployed by South African commercial banks to mitigate cyber-attacks and threats. The following research questions guided us to address the study objectives:

- What are the main cybercrime typologies are targeted at South African commercial banks?
- What are the effects of cybercrime typologies on the performance of commercial banks?
- What interventions can mitigate cyber-attacks and threats in South African commercial banks?

Author α: PhD Student, Department of Information Systems, University of the Western Cape (UWC), Cape Town, South Africa.
e-mail: mphahleletk@gmail.com
Orcid Id: https://orcid.org/0009-0005-8670-511X
**Corresponding Author: Professor, Department of Information Systems, School of Computing, College of Science, Engineering & Technology, University of South Africa (UNISA), Florida, South Africa.*
e-mail: chigajm@unisa.ac.za
Orcid Id: https://orcid.org/0000-0002-7633-8345

II. Literature Review

a) South African Banking Landscape

The banking landscape in South Africa comprises a central bank (South African Reserve Bank), five large local banks and other smaller banks and financial institutions. The sector is considered well-developed and ranked relatively high compared to developed nations. In 2017, the South African banking sector ranked 11th out of 138 countries in market development in the global competitiveness report. It also ranked 2 out of 138 countries in terms of bank soundness; a sound banking system ensures the optimal allocation of capital resources and efficient management of risks to prevent costly banking system crises and their associated adverse feedback effects on the real economy (Schwab, 2017; Schwab, 2019). Simbanegavi, Greenberg, and Gwatidzo (2015) state that the South African banking sector is monopolistically competitive; however, this does not indicate a lack of efficiency or competitiveness within the market. Moyo (2018) further corroborates this by highlighting that the sector comprised 64 institutions as of 2017, which indicates competitiveness.

The five big banks have also started making significant changes to how they do business; in digital innovation, they have had to choose between becoming part of somebody else's ecosystem or becoming a destination. This has led to some of the banks embracing a platform banking approach, which allows banks to offer more than financial services to their customers. Commercial banks such as Nedbank, First National Bank, and Standard Bank have either started this offering or have expressed their intentions to become platform banks (Whateley, 2021; Brink, 2020; BusinessTech, 2021).

b) Cybercrime Typologies in the South African Banking Industry

Zhang, Yanping, Xiao, Ghaboosi, Zhang and Deng (2012) define cybercrimes as criminal activities that use modern information technology, such as computer technology, network technology, etc. The South African definition of cybercrimes further expounds on their definition to include cyber extortion, unlawful acquisition, possession, provision, receipt or use of a password, access codes or similar data or devices, attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit an offence, theft of incorporeal, penalties, and competent verdicts (Department of Justice and Constitutional Development, 2016). Brar and Kumar (2018) note that cybercrime's motivations include entertainment, hacktivism, financial gain, and revenge. South Africa has also seen a scourge of cybercrimes; critical infrastructure within the country has not been spared, and in 2021 South Africa ranked 7th globally in cybersecurity exposure and had one of the highest numbers of cybercrimes victims globally (Cyber Exposure Index, 2021)

c) Hacking

One of the cybercrime typologies to have gained popularity is hacking. According to Van Niekerk (2017), the first cybercrime incident against a commercial bank in South Africa occurred in 2003 when Absa Bank lost approximately ZAR500000 due to a hack. The threat actor, in this case, compromised the users by sending an email containing a trojan which obtained the banking details and PINs of the victims when opened. The hacker then used the victim's computers to access their bank accounts, bypassing security controls and making it seem like a legitimate session; they then proceeded to withdraw money from the victim's accounts (Mohan et al., 2020). Hackers can access systems through structured query language (SQL) injections, theft of file transfer protocol (FTP) passwords and cross-site scripting (Chigada, 2023).

d) Internet Fraud

In 2006 in three months, account user details for clients belonging to three commercial banks in South Africa were compromised; the compromised credentials were then used to transfer money from the victim's accounts into either cell phones or Telkom prepaid accounts (IOL Media, 2006). The threat actor, in this case, found a way to hack into either business accounts or personal accounts belonging to the victims using malicious tools such as spyware, backdoor trojans and keyloggers; this breach cost an estimated USD80000 (Oiaga, 2006).

e) Unethical Employee Behaviour

An attack possibly aided by employees at Landbank and Absa Bank occurred in December 2010; a syndicate hacked into the Landbank's infrastructure and obtained secret passwords that only a select group of personnel had access to. The syndicate then proceeded to set up automated fund transfers to multiple companies. However, the attackers were unsuccessful, as bankers at Absa noticed the suspicious transactions and froze the accounts (Potgieter, 2011). Absa South Africa was a victim of an insider attacker after an employee illegally accessed and shared customer information with third parties; the data accessed by the employee contained a mix of sensitive information and marketing information (Thompson & Farber, 2020). Within the same year, Nedbank suffered a data breach through one of its third-party service providers (Computer Facilities (Pty) Ltd). The compromise involved the leaking of personally identifiable information of some Nedbank clients. The third-party breach affected approximately 1.7 million clients, with 1.1 million active clients (Nedbank, 2020).

f) ATM Fraud Attack

Standard Bank South Africa suffered a massive cyber-attack in 2016, leading to the bank losing ZAR300 million through an ATM fraud attack in Japan. In the coordinated attack, about one hundred people used forges Standard Bank credit cards to withdraw money from 1400 ATMs throughout Japan (Moyo, 2016). It was suspected that hackers broke into the bank's digital infrastructure and obtained about 3000 sets of personal data that were subsequently used in the attack (News24Wire, 2016).

g) Distributed Denial of Service Attack (DDoS)

In 2019 South African banks were hit by a massive Distributed Denial of Service Attack (DDoS), which targeted multiple banks in with country. Distributed Denial-of Service attack (DDoS) is perpetrated when threat actors and attackers clog the bandwidth denying legitimate users from access computing services (Chigada, 2020). This attack disrupted online and mobile app banking (McKane, 2019). The attack was ransom-driven, with the threat actors sending ransom notes to employee email addresses and unattended email addresses within the targeted banks (Fin24, 2019).

h) Phishing Emails

Banking clientele have been receiving Phishing emails purporting to be coming from legitimate source. Nyasvisvo and Chigada (2023) define email phishing as fraudulent messages which are designed to appear genuine in order to convince the recipient to believe the messages and act upon it. Burns et al. (2019) suggest that the use of well-known logos, brands and layout make these emails look real and this is what deceives victims. Chuma and Ngoepe (2021) state that South Africa has recently become of the top countries experiencing Phishing attacks.

i) Identity Theft And Bank Card Fraud

Chigada (2020) reports that identity theft and bank card fraud have the highest commission rate in the world. The South African Bank Risk Information Centre [SABRIC], 2020) reports that identity and credit card theft cases are on the rise. Attackers use the internet (online services) to commit fraudulent solicitations, transactions and transmit these fraudulent transactions to financial institutions. Internet fraud has similar trait as cyberstalking (Khan et al., 2020).

j) Complexity, Frequency and Severity of Cyberattacks

Over time, the increasing complexity, frequency, and severity of cyberattacks targeting financial institutions bring forth the inevitability and the impossibility of completely protecting the integrity of critical computer systems and data (Dupont, 2019). The fourth industrial revolution also adds a level of complexity as it represents a fundamental change in the ways humans live and work; it is enabling the merger of the physical, digital, and biological worlds, the combination of cyber-physical systems, the Internet of Things and the Internet of System, smart factories and fusing technologies in ways that create both promise and peril (Schwab, 2015; Marr, 2018).

k) Insufficient Information Security Expertise and Awareness

The European Union Agency for Cybersecurity (ENISA) (2021) identifies some of the challenges in cybersecurity as a lack of sufficient information security expertise and awareness, incomplete organisational policies, reluctance to fund security, lack of accountability, fragmentation of security technical standards, supply chain management complexity, interoperability of devices, platforms, and frameworks, and lack technical capabilities (Malatras, Skouloudi, &Koukounas, 2019). Blum (2020) adds to the list of challenges by identifying ineffective communication, hard-to-change culture, and the lack of solid leadership within organisations.

l) Lack of Confidentiality, Integrity, and Availability

An information security strategy should be employed to meet the requirements of the information security triad: confidentiality, integrity, and availability. Confidentiality is concerned with access controls around information and system permissions. Integrity is concerned with the authenticity of the information being viewed and accessed. Availability entails anyone authorised to access and modify data within an appropriate timeframe. When looking to secure information resources, organisations must balance the need for security with users' need to effectively access and use these resources (Bourgeios, Mortati, Wang, & Smith, 2019).

III. Interventions to Mitigate Cybercrime among Commercial Banks

a) Computer Security Incident Response Teams

The Security Operations Centre (SOC) comprises a Computer Security Incident Response Teams (CSIRT), and other functions form an effective cybersecurity architecture within any institution. The Security Operations Centre and the CSIRT are responsible for dealing with cybersecurity incidents within institutions; they do this by investigating, triaging, responding and remediating incidents (CompTIA, 2021; Cybersecurity & Infrastructure Security Agency, 2007). It has become imperative for firms to establish in-house cybersecurity management teams. In so doing, the teams should develop and implement a governance, risk and compliance framework (Chigada, 2023).

b) National Cybersecurity Policy Framework

Only recently, through the National Cybersecurity Policy Framework, Cybercrimes Bill, and Protection of Personal Information Act, firm cyber-

security policies were adopted in South Africa. The purpose of the National Cybersecurity Policy Framework was to create a secure, dependable, reliable, and trustworthy cyber environment that facilitated the protection of critical information infrastructure whilst strengthening shared human values and understanding of cybersecurity in support of national security imperatives and the economy (Republic of South Africa, 2015). The policy framework sets out to achieve this through centralising the coordination of cybersecurity activities and establishing relevant structures, policy frameworks and strategies in support of cybersecurity.

c) The Protection of Personal Information Act (POPIA)

The Protection of Personal Information Act (POPIA) had the objective of promoting the protection of personal information processed by public and private bodies; introducing certain conditions to establish minimum requirements for the processing of personal information; providing the establishment of an Information Regulator to exercise certain powers and to perform specific duties and functions in terms of the Act and the promotion of access to Information Act, 2000; regulating the flow of personal information across the borders of the Republic of South Africa as well as to provide for matters connected therewith (Republic of South Africa, 2013).

d) Adoption and use of Biometric Authentication

Chang and Coppel (2020) state that a good intervention strategy to mitigate credit card fraud is the adoption and use of biometric authentication. Customers do not need to carry credit cards or key-in personal identification numbers (PIN) when transacting. Merchants would have invested in biometric technologies that support biometrics authentication. Different biometrics usable in the authentication process are classified as physiological (fingerprint, face recognition, IRIS scan, hand geometry, deoxyribonucleic acid [DNA]) and behavioural (voice pitch, speaking style, typing rhythm, signature, breathe) (Pillay, 2020).

e) Cybersecurity Risk Assessments

Chigada (2023) states that firms should periodic cybersecurity risk assessments to identify security weaknesses and likely risks posed by third-party vendors (Galine et al., 2017). The cybersecurity risk assessment drive helps the firm to keep a detailed register of its assets which are authorised to access the corporate network. There is a proliferation of Bring Your Own Device (BYOD) approach where some organisations allow employees to use their personal devices for work purposes (Chigada & Daniels, 2021).

IV. Methodology

a) Research Design

The study employed a qualitative research design which enabled it to explore the social and human aspects of cybersecurity through a conversational approach provided by a qualitative research design. Creswell and Poth (2018) define qualitative research as a research activity that locates the researcher worldwide. It consists of interpretive, material practices that make the world visible. The authors expound on the definition by stating that qualitative research begins with assumptions and a theoretical framework that informs the study to address the meaning individuals or groups ascribe to a social or human problem.

Cleland (2017) postulates that qualitative research methods address the "how" and "why" of research questions and facilitate a deeper understanding of experiences, phenomena and context. It further makes it possible for the researcher to ask questions that cannot easily be put into numbers. Our focus was on how reality could be observed and our relationship with that reality (epistemology). By choosing the qualitative research methodology, the intention was to complement the subjective ontological stance and interpretivist philosophical paradigm (Nyasvisvo& Chigada, 2023). In order to address the research problem through direct interaction and personal conversations with participants, the ideal methodological choice was the qualitative one. We probed participants for clarity on issues that were not clear (Creswell & Creswell, 2018).

For this study, qualitative data collection was done through semi-structured interviews with employees from commercial banks in South Africa. No-probability purposive sampling was used in this study in the selection of participants from the respective IT departments. We used an inclusion/exclusion approach to select participants for the study. The prerequisite for employees to participate was to be employed in IT, Risk, Compliance, IT Security, or governance within the banks. The interviews were conducted using video conferencing software (Microsoft Teams and Zoom).

b) Data Analysis

As espoused by Kabir (2016) analysing data helps to summarise the findings but in a meaningful way so informed decisions can be made. We were actively involved and participated in the semi-structured interviews, therefore, we understood, described and interpreted the views from the participants' perceptions of events as they occurred in a natural setting. Within qualitative data, we used thematic data analysis (TDA) to identify, analyse and interpret themes which were invaluable to address the research questions (Maguire & Delahunt, 2017). Thematic analysis is a method used to identify and interpret meaning patterns across qualitative data (Clarke & Braun, 2014). Qualitative data analysis is simultaneously an iterative and sequential process that follows a set number of steps to assign meaning to pieces of data (Rossman & Rallis, 2017). This study employed thematic analysis to identify key

impediments to the challenges faced by commercial banks in South Africa regarding developing local cybersecurity frameworks. The use of ATLAS. Ti helped us to tease out emerging themes from the transcriptions. We deployed a six -step approach in analysing data and these were familiarisation; generation of initial codes; generating themes; reviewing themes; naming themes and write-up of this report. To ensure accuracy and error-free and easy to read responses, we used the Dragon speech transcription software. Findings were presented in text format.

V. Findings and Discussion

The data collected for the study was gathered from twenty-one participants, fourteen male participants and seven female participants. The disparity between the number of male and female participants is partly because males dominate the Information Communication Technology (ICT) sector within South Africa. This is supported by Padayachee and Pillay (2018) who state that females are under-represented within the IT sector in South Africa and further evidenced by Malinga (2021) who points out that out of the 236 000 ICT roles within South Africa, females only hold 23% of those roles. Due to this factor, the study has more males than females predominantly.

a) *Cybersecurity Challenges Faced by Banks from Internal and External Perspectives*

This question explored the challenges commercial banks face regarding cybersecurity, revealing one central theme raised by most participants. The main theme was the lack of IT and Cybersecurity skills. Participant MN14 stated that: "I don't think that we have an all-round. I don't think I don't think the industry has an all-around pool of skilled people that can effectively, you know, defend, to a certain extent, yeah." This was supported by participant HN07 who indicated that:

> "I think one of the challenges as well is kind of skills, because when it comes to IT security, I don'thave the skills and the knowledge"

Given the above perceptions, Participant MR11 added the following comments:

> "They will always face threats internally and externally for exploitation and resourcing. I think resourcing. It's a question of the right skills or the right level of skills to be able to protect the bank."

Participants explained how lacking such a fundamental skill is detrimental to an organisation's security posture. Kshetri (2019) mentioned the lack of cybersecurity skills and estimated that by 2020 there would be a shortfall of about 100000 cybersecurity personnel in Africa. The World Economic Forum (2022) and (ISC)2 (2021)stated that there is still a workforce gap of more than 2.72 million positions globally, and the cybersecurity workforce needs to grow by 65% to defend the critical assets of organisations effectively.

Participants also noted a lack of resources as one of the driving forces behind the challenges faced by commercial banks. Participant TM02 indicated that:

> "I think the budget would be one of the biggest challenges. And why I'm saying this is remembered, most of because the organisation is the bank itself. So, for them to properly ensure that the bank is protected, and such, so the question is, do they have enough budget?"

In support of Participant TM02's views, MR11 stated that "And under-resourcing leads to a plethora of issues in terms of they can't deal with the vulnerabilities in a timely manner. They can't keep up with technologies; they can't keep up with security training". While BN06 asserted that "And the other challenge or the underlying challenge was lack of resources. So, you have fewer analysts or engineers, looking at a SOC."

European Union Agency for Cybersecurity (2021) supports the participant's views by positing that a lack of information security awareness and expertise in organisations often leads to a lack of cybersecurity budget and inadequate staffing. Da Veiga, Astakhova, Botha, & Hersleman (2020) stated that resources are required for successful implementations or changes to information security, with organisations with budgeting and funding being crucial to implementing security practices within organisations.

Commercial banks' cybersecurity challenges are industry-wide and not specific to one commercial bank. The first response was obtained from Participant AA19 who stated that:

> "The second part of it, which is a lot around education and awareness and training for your staff, your staff need to be aware of the type of emails, they need to look out for the type of phishing emails that are being sent. It's very well crafted these days."

Participant JP16 further pointed out that in support of Participant AA19:

> "Yes, we put controls in place to ensure they cannot remove that sensitive data information. But they are our first line of defence. I think of the word now that the attackers use a syndicate, Syndicate, and that's always going to be the main thing."

Participant KS12 averred and indicated that "The biggest vulnerability, according to me, right? It's people. Yeah, it's people. And, and by people, I mean end-users, because those are where most of the breaches stemmed from, you know, your phishing and all that."

Some of the major cyber incidents that have occurred recently were partly due to incompetent, negligent or users who did not know better. This was evidenced by Van Niekerk (2017) who stated that one of

the first successful cybercrime incidents against a commercial bank was a threat actor compromising a user's account by sending malicious mail to the user. Mitnick, Simon, & Wozniak (2002) ultimately state that employees and end-users are the greatest threat to corporate information security, intentionally or through negligence or often due to lack of knowledge.

Participants identified the deprioritisation of cybersecurity as one of the contributors to the challenges commercial banks face regarding cyber-security. Participant JB15 stated that: "The first issue is that executive is primarily focused on generating revenue, as opposed to implementing security controls". This was echoed by Participant SD17 who had this to say:

> "I think it's because I'm in, I've been put in a position where it's not emphasised, cybersecurity. And when you're given a title, you stick to the title and like expectations, and our theory to sort of know or understand it and things."

Participant NM21 asserted that "I mean, a long time ago, not maybe not a long time ago, not a long time ago. But if I were to wrap it up, I'd say it before, it wasn't something that banks traditionally focused on".

Security prioritisations help organisations identify the potential risks affecting them and subsequently prioritise the defence of their digital assets (Blum, 2020). Although the participants might occupy high positions of influence, security was still not emphasised in their role, implying that their subordinates also did not see the importance of safety. Keman and Pearlson(2019) state that an organisation's lack of a strong cybersecurity culture can make them less resilient against cyberattacks.

b) Misalignment of Security and Business

The response from Participant JB15 was that "If you have too many security controls in place, you're slowing down business and stopping business from happening."

Participant KS12 provided a detailed response by stating that:

> "But remember, security is actually a deterrent to business. To a certain extent. That's why you can't. We can just put encryption on everything because it then degrades the performance of applications and stuff."

A different perspective was shared by Participant JP16 who indicated that "You know, and this is the big kind of the elephant in the room with security is that security is always seen to business and project drivers as a blocker."

Blum (2020) states that misalignment of security and business could negatively affect any project's security touch. Edwards (2020) notes that a disconnect exists between how businesses understand and manage cyber risk, driven by organisations failing to view cybersecurity as a business strategy rather than an IT problem. To overcome this misalignment Boehm, Curcio, Merrath, Shenton, and Stähle(2019)assert that organisations need to move towards a risk-based approach to cybersecurity.

c) Cybersecurity Frameworks within your Bank

From the question asked, one central theme emerged of the framework employees were most familiar with in their organisation. Three other subthemes emerged from the interview with the participants.

Theme 1: NIST Cybersecurity Framework

Multiple participants mentioned the NIST Cybersecurity framework as one of the frameworks used within their organisations. Participant MR11 was succinct with the response by stating that "So, the NIST I know we are we just at the company that I'm working, for now, we just did NIST, NIST review." An equally precise response from Participant AM09 stated that "Okay. All right. So, what I know is okay, this is the NIST framework." Whereas Participant JB15 weighed in by outlining that "So, for most of everything I've based everything on NIST compliance. Okay. The reason I've chosen NIST is that the American government takes federal law very, very seriously"

The National Institute of Standards and Technology's cybersecurity framework is a set of cybersecurity activities that are common across the critical infrastructure sector (Alexander & Panguluri, 2017). With estimates stating that almost 50% of all enterprises use NIST, the framework being the most mentioned by participants shows the popularity and widespread adoption of the framework (Banga, 2020).

Theme 2: ISO Frameworks: Participants also cited the International Organization for Standardization (ISO) standards as frameworks they were aware of within their organisations. Short and precise responses were received from three participants. For instance, Participant NT03 said that "Like sort of standard, like, for example, the one that I'm aware of. It's ISO 2700 something". Participant KM05 had this view that supported Participant KM03, "The ISO 27001 That is the only internationally accepted framework. So, meaning that it's an ISO standard, it's accepted everywhere is used everywhere, and that is the accepted norm." While Participant AM09 indicated that "Then your ISO to 27001 And 27002, and then. Yeah, but then now also, with the cloud. This standard is an ISO standard for security in the cloud."

The ISO 27001/ISO 27002 these frameworks/ standards describe an Information Security Management System (ISMS) and detail the steps involved in the establishment of such a system, with the ISMS aims to minimise risk and ensure business continuity by limiting the impact of security breaches through creating policies and procedures to manage a business's sensitive information.

Theme 3: Do not know: A subtheme from the interview with the participants was that few were unaware of the frameworks utilised within their organisations. Participants gave reasons ranging from cybersecurity not being in the direct scope of the roles to the organisations they are employed within not emphasising cybersecurity enough in day-to-day operations. Participant SD17 outlined that "I'm not really familiar with. I think it's because I'm in, I've been put in a position where it's, it's not emphasised". This was also supported by Participant DM01 who said that "I actually don't know. It's not in my scope. And then I've not really seen or heard anything shared along if the exact frameworks or tools that are being used within the bank." There was concurrence from Participant AB10 who also did not know and stated that "Zero, sorry. I guess more I don't know if I should call front-end or client-facing software; those layers might integrate more directly into our cybersecurity framework. But we are the absolute back end."

d) *Interventions to Mitigate the Threats Faced by the Banks*

Various interventions that informed the themes of the question emerged during the study; these included implementing controls within the banks, building a more robust culture and awareness around cybersecurity, and continuously monitoring and maintaining the organisation's security posture. The themes identified during the analysis of the captured responses are below.

Theme 1: Security Controls: Many of the participants indicated that having controls in place is one of the most effective ways to mitigate the threats and attacks faced by the bank. These controls comprise the three common cyber control types: physical controls, technical controls, and administrative controls (Chapple, Tittel, & Stewart, 2021).

> "So we had initiatives around secure perimeter and network. And then so obviously, making sure that we don't have any high-risk vulnerabilities that externally facing, conducting pen test remediating vulnerabilities during the configuration. These views were shared by Participant MR11."

These views by Participant JP16 differed from what was stated by Participant MR11 above in that:

> "But, you know, as I said, we have controls in place to ensure that we monitor data flow, and we understand what's happening in the environment."

Participant AA19 bridged the gap between what was said by Participants MR11 and JP16 by stating that

> "You look at the type of access governance that you also have in place, which means only certain individuals are allowed to have access to certain data at any given time."

IBM Cloud Education (2019) describes security controls as "parameters implemented to protect various forms of data and infrastructure important to an organisation. Although participants stated that having controls in place is one best ways of mitigating the threats the organisation faces, inadequate controls or control failures are usually the reason behind successful breaches. To adequately put in controls to defend against attackers, organisations need to undertake a risk analysis to determine the necessary controls to be implemented.

Theme 2: Security Tools and Assessments: The various initiatives that institutions need to ensure that they are secure to some extent and that they continuously monitor their security posture include the responses. What was considered secure yesterday would not necessarily be considered secure today. Participant MN14 stated that:

> "You know, interventions are definitely buying the latest and greatest technology, the bank, the banking institutions, or the sector, if you may, they, they hardly spare any expenses when it comes to tools. "

While Participant AA19 was succinct in their answer by stating that "We do a lot of simulation, penetration testing, continuous routine testing."

Comprehensive posture of security tools and assessments was obtained from Participant JB15

> "We use IPS, IPS and IDS technologies to do like virtual patching. They using vulnerability scanners to pick up vulnerabilities that exist in the networks and in the infrastructure."

From the responses above, it was clear that the organisations use vast and varying tools from different vendors to protect them. Comments from participant MN show that the organisations spare no expense when securing the best tools out there. These tools may be a collection of technical processes and practices designed to protect the institution (Möller, 2020; Sheikh, 2020).

Theme 3: Awareness and Training: It was evident from the participants that security awareness and training programs are crucial in educating end-users and employees in organisations to be better aware of security threats and respond appropriately. In view of training and awareness Participant AA19 stated that

> "There so that it's really important awareness education with the customers as well, ensuring that they know that, you know, ever, if there's any communication that comes from a bank, that they verify that they trust in the source that it actually comes from."

Participant VS18 summarised one's response by stating that "We constantly have to do what is this cybersecurity trainings to just make sure that we are aware of, you know, is out there." However, a mode

detailed response was obtained from Participant KM05 who indicated that:

> "The people aspect, I would say the interventions have also been implemented there to ensure that you put people in those processes, that that that they understand their recommendations, that they understand they are role in protecting themselves and their organisations."

Awareness programmes further assist in disseminating an organisation's security policy to its employees with the hope that these programmes will encourage a security-aware culture so that good security practices will become the de facto approach to everything in an organisation (Gundu, Flowerday, & Renaud, 2019)

Theme 4: Risk Assessments: These assessments were critical drivers to understanding the overall risk the organisations were exposed to and tools for calculating and understanding the risk they would be exposed to when integrating with third-party service providers.

Participant BN06's views regarding risk assessments were that:

> "So, when I can think of taking that high-level risk assessment, being able to understand the risk faced by the bank, and through the process of risk assessment, you then need to make sure you have the right controls or tools, which mitigates those specific risk, and ultimately, threats as well."

Risk assessment in terms of contracts was a major issue with Participant KM05 who indicated that "For every third party that we contract, we need to make sure that we do risk assessment, including a cybersecurity risk assessment". A different posture was obtained from Participant MR11 who stated that "Also risk management effective proactive for thinking looking risk management. I think banks have done a pretty good job in terms of trying to resource the risk management department"

Participant JP16 had this to say regarding risk assessments:

> "Like I say, you're always going to have attacks and breaches, but this is exactly why we, we build in our risk appetite into these projects and how we implement controls, and we understand what is material to the bank."

Blum (2020) posits that risk management can be a keystone within an organisation's security culture and governance model. Wang, Ding, Sui, and Gu (2021) also support the participants' views by stating that risk assessments are essential to effectively responding to cyberattacks. Their paper demonstrates how risk assessments assist in quantifying and identifying cybersecurity risks and finding attack paths with high cybersecurity threats.

e) Impact of Cyber-Attacks and Threats on the Operations of the Bank

The themes below served to answer the question above about the impact cyber-attacks and threats have on commercial banks. They also sought to meet the research objective of assessing cyberattacks and threats' impact on commercial banks. Four themes were identified from the interviews, and the themes were:

Theme 1: Stop Operations: One of the other subthemes from the participants was the impact cyberattacks had on the CIA triad mentioned earlier in this study. Multiple participants noted how attacks could impact either of the triad's pillars, leading to a halt in operations. Participant MR11 stated that "I think from an attack perspective if an attack is successful, the bank cannot operate at all. So, transactions cannot take place. People cannot transact, which leads to a financial impact on the bank."

While more detailed responses were obtained from Participants JB15 and A119 respectively:

> "They, I mean, it can really shut down the bank. You know, if the threat of the attack is big enough, yeah, you know, if you, if you're a small bank, and you get a distributed denial of service, and you're very centralised, the entire bank could be offline you cannot operate"(Participant JB15).

> "We know ransomware is a massive issue. As you can imagine, you get different types of ransomware, you get ransomware, that encrypts files, and you get ransomware. That encrypts hard drives and systems" (Participant AA19).

Theme 2: Reputational Damage: This was summarised by Participant AA19 who stated that "And then obviously, the big elephant in the room is the reputational damage that comes from that because As you know, if your customer doesn't trust you anymore, your customer is 95% of the time going to go somewhere else."

Participant NM21 argued in that data breaches caused reputational damage to the brand by stating that:

> "Reputational damage reputation itself obviously is terrible, this type of attacks and the times will go out to the media."

The above extract was supported by Participant TM02 who stated that:

> "So the implications could be catastrophic for the bank, you know, in a nutshell. And with that said, I think the manner in which the bank would respond to such attacks."

Reputational damage and trade name devaluation are real consequences of cyberattacks. Trust between clients and investors is usually eroded when organisations are victims of cyber incidents. Hollard (2017), which is an insurance provider in South

Africa, states how a cyber incident that occurred at Standard Bank South Africa, which cost the bank around ZAR 300 million, had an impact on the organisation's reputation, not only because of the attack but the downtime associated with these attacks. Agrafiotis, Nurse, Goldsmith, Creese, and Upton (2018) identify reputational harm as one of the cyber-harms that results from cyberattacks; they state that reputational harm adversely affects how the public perceives the organisation, and this might, in turn, an effect on how the media portrays the organisation and the relationship between the organisation and its stakeholders.

Theme 3: Financial Losses: It was also evident that participants knew that financial losses faced by commercial banks when dealing with cyber-attacks were not only from the cybercriminals carrying out the attack but from the regulators who could impose fines on the banks for those material breaches. Participant KS12 indicated that "I mean, quoting the words of our CEO, cyber threats, have the potential to bankrupt the bank. And probably even make us shut down in a very short space of time."

While Participant OO04 directly pointed that financial losses were highly likely to occur by stating "There is a potential for financial losses, there is a potential for regulatory losses in terms of fines from the regulatory body when there is if it is determined that sufficient controls were not put in place to prevent the incident from happening"

A different perspective was shared by Participant VS18 who spoke about investors pulling out of the hacked bank:

> "If the bank were to be hacked, shame, god forbid, and your traders don't have access to the market, the bank would lose millions because then you won't be able to bid in the market like wouldn't be able to participate."

The participants' views are corroborated by an Accenture report (2019), which showed that the annual costs of all types of cyber-attacks are increasing, with the average cost of an attack totalling US$13.0 million in 2018. Within South Africa, the fines are imposed by the South African reserve bank and the Information Regulator depending on the type of infringement. Examples of these fines include a ZAR 1 million to Habib Overseas Bank Limited for inadequate internal controls for detecting suspicious and unusual transactions; Investec Bank Limited was fined R20 million for a similar transgression as Habib Overseas Bank (South African Reserve Bank, 2020). Recent examples of such fines include a possible penalty to the credit bureau TransUnion for a cyber breach that affected data belonging to South African citizens. The credit bureau was facing a potential fine of ZAR 10 million for the breach (My Broadband, 2022).

Theme 4: Loss of Investor and Customer Confidence: The last subtheme that emerged from the participants was how suffering cyberattacks could result in the financial institution losing investors and how customers' confidence in the institution might suffer.

Their views are supported by an expanse of literature that cites that the announcement of cybercrime often negatively impacts the market value of the stock prices (Smith, Jones, Johnson, & Smith, 2019). EY Global (2019) asserts the participants' views by stating that a cyberattack can destroy trust between organisations and their customers. This is because, in recent times, customers have been providing more data to organisations. Concurrently, concerns around data privacy and cybersecurity have been growing among customers.

Participant VS18 Stated that:

> "And shareholders would not have faith, you know, in the bank itself. Because if you're unable to protect your systems against cyber-attacks, then they cannot trust that the interests are protected in the bank, and they feel very vulnerable. So you can do a lot in terms of the share price."

Participant DM01 was clear how the loss of information could be consequential to the bank by stating that "You could lose, number one, some very important information of your clients, which in turn will result in a loss of trust with the clients in the bank. And, you know, you could lose market share"

VI. Conclusion

This paper examined the mitigations available to commercial banks in South Africa with dealing with cyber threats and attacks. The results evidenced multiple contributors to the success of attacks by threat actors. It would take a concerted effort by all stakeholders to mitigate the threats faced by the banks. From the responses, it emerged that to mitigate the threats; efforts would need to be applied to improving the cybersecurity culture within organisations and provisioning more resources, including skilled security professionals and the financial resources required to obtain the necessary tool and security assessments to identify and mitigate threats. Security needs to be viewed as an enabler of business. This would enable security to widen its scope within organisations and actively analyse and prioritise risk. The overall theme that emerged from the findings was that the issue of security needs novel approaches that would employ a three-pronged approach of people, process, and technology.

The study's limitations were the adoption and implementation of POPIA, which limits the sharing of personal information without the express consent of the data subjects; the implications were that identified participants and respondents to the study could not

share details of potential respondents and participants without first acquiring their consent. Furthermore, the participants of the semi-structured interviews were employees from the big five commercial banks in South Africa. Due to this, the study's findings portray views mainly of the big five banks.

Future research may be performed to investigate the impacts they have on commercial banks and to determine if the regulations have had a positive effect on cybercrimes and cybersecurity within the country. To gather a more comprehensive picture of the threats and patterns of attacks faced by banks, further studies could focus on obtaining the necessary permissions and clearance to study this nature within the banks. This will enable better data collection and access to information that is not publicly available due to its sensitivity.

Acknowledgements

The authors acknowledge with gratitude the University of the Western Cape for allowing this study to take place. The financial institutions and participants to the study are acknowledged for their time and invaluable contributions towards the completion of the project. We acknowledge our families and friends for their support towards this study.

References Références Referencias

1. (ISC)². (2021). A Resilient Cybersecurity Profession Charts the Path Forward: (ISC) 2 Cybersecurity workforce study, 2021. (ISC)².
2. Accenture and Ponemon Institute LLC. (2019). Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. Accenture Security. Accenture. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
3. Accenture South Africa. (2020). Insight into the cyber threat landscape in South Africa. Accenture. Retrieved October 31, 2021, from https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa
4. Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4 (1).
5. Albert, B., Tullis, T., & Tedesco, D. (2009). Beyond the usability lab: Conducting large-scale online user experience studies. Morgan Kaufmann.
6. Albert, D. (2020, October 5). Why Security Can't Live In A Silo. Retrieved June 16, 2022, from Forbes.com: https://www.forbes.com/sites/forbestechcouncil/2020/10/05/why-security-cant-live-in-a-silo/?sh=708372023819
7. Alexander, R. D., & Panguluri, S. (2017). Cybersecurity Terminology and Frameworks. In R. M. Clark, & S. Hakim (Eds.), Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level (pp. 19–47). Cham: Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-32824-9_2
8. Alvarez, M. (2017). Security trends in the financial services sector. IBM Security. Retrieved from https://www.ibm.com/downloads/cas/QWYWABVG
9. Armstrong, R. C., & Mayo, J. R. (2009). Complexity Science Challenges in Cybersecurity. Argonne.
10. Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. Software Quality Journal, 987-1018.
11. Banga, G. (2020, November 4). How To Ensure Your NIST Cybersecurity Framework Implementation Isn't Too Little, Too Late. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2020/11/04/how-to-ensure-your-nist-cybersecurity-framework-implementation-isnt-too-little-too-late/?sh=3e3ae4e6364d
12. Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | NIST. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | NIST.
13. Bert, A. (2018). 3 reasons gender diversity is crucial to science. Elsevier Connect.
14. Blum, D. (2020). Rational Cybersecurity for Business the Security Leaders' Guide to Business Alignment. Apress.
15. Blum, D. (2020). Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment (1 ed.). Berkeley, California: Apress. doi:10.1007/978-1-4842-5952-8
16. Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019, October 8). The risk-based approach to cybersecurity. Retrieved April 17, 2023, from Mckinsey.com: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/
17. Bote, D. (2019). The South African National Cyber Security Policy Framework: A critical analysis. Potchefstroom: North West University.
18. Bourgeios, D., Mortati, J., Wang, S., & Smith, J. (2019). Information Systems for Business and Beyond (2019 ed.). Saylor Foundation. Retrieved from https://opentextbook.site/exports/ISBB-2019.pdf
19. Bramwell, L. (2017, August 21). Parliament of the Republic of South Africa. Retrieved from https://static.pmg.org.za/170822Cybersecurity.pdf
20. Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. Journal of Computer Networks and Communications, 2018. doi:10.1155/2018/1798659

21. Buthelezi, L. (2022, January 24). Hawks arrest Absa engineer for alleged theft of R103 million. Retrieved June 2022, from Fin24: https://www.news24.com/fin24/companies/hawks-arrest-absa-engineer-for-alleged-theft-of-r103-million-20220124
22. Cabrera, D., & Cabrera, L. (2018). CONNECTING SILOS: Solving the problem of organizational silos using a simple systems thinking approach. Cornell University.
23. Carter, W. (2017). Forces Shaping the Cyber Threat Landscape for Financial Institutions. SWIFT INSTITUTE. Retrieved from https://ssrn.com/abstract=3047730
24. Catota, F. E., Morgan, G. M., & Sicker, D. C. (2018, April 30). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4 (1). doi:10.1093/cybsec/tyy002
25. Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018, 4). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4. doi: 10.1093/cybsec/tyy002
26. Chapple, M., Tittel, E., & Stewart, J. M. (2021). CISSP: Certified Information Systems Security Professional Study Guide. Sybex.
27. Cheng, Z., Li, Y., Wu, Y., & Luo, J. (2017). The transition from traditional banking to mobile internet finance: an organizational innovation perspective - a comparative study of Citibank and ICBC. Financial Innovation, 12(3).
28. Chigada, J. (2023). Towards an aligned South African National Cybersecurity Policy Framework. Published PhD Thesis: Cape Town.
29. Chigada, J. (2020). 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 (1), 1-9. https://doi.org/10.4102/sajim.v22i1.1194
30. Chigada, J., & Kyobe, M. E. (2018). Evaluating Factors Contributing to Misalignment of the South African National Cybeersecurity Policy Framework. CONF-IRM 2018 Proceedings. 4. Retrieved from http://aisel.aisnet.org/confirm2018/4?utm_source=aisel.aisnet.org%2Fconfirm2018%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages
31. Chigada, J., & Ngulube, P. (2015). Knowledge-management practices at selected banks in South Africa. South African Journal of Information Management, 17(1), 10.
32. Chigada, J., & Madzinga, R. (2021, February 19). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23, No 1(a1277). doi: https://doi.org/10.4102/sajim.v23i1.1277
33. Chigada, J., & Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financialservice firm, Business Information Review, 38(3), 1-12. https://doi.10.1177/02663821211036400
34. Cleland, J. A. (2017). The qualitative orientation in medical education research. Korean Journal of Medical Education, 61-71.
35. Copan, W. G. (2020, February 19). A Conversation on the NIST Privacy Framework. Washington, D.C, Washington.
36. Cram, W. A., ProudFoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. MIS Quarterly Executive, 19(3), 183-198. doi:10.17705/2msqe.00032
37. Creswell, J. W., & Plano Clark, V. L. (2017). Designing and Conducting Mixed Methods Research (Third Edition ed.). SAGE Publications, Inc.
38. Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry & Research Design (Fourth ed.). Sage.
39. Creswell, J. W., & Tashakkori, A. (2007, January). Editorial: The New Era of Mixed Methods. Journal of Mixed Methods Research, 1(1), 3-7. doi: https://doi.org/10.1177/2345678906293042
40. Cyber Exposure Index. (2021). Country statistics. Retrieved November 14, 2021, from Cyber Exposure Index: https://cyberexposureindex.com/country-statistics/
41. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92. doi:10.1016/j.cose.2020.101713
42. Da Veiga, A., Astakhova, L. V., Botha, A., & Hersleman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92 (101713).
43. Dekkers, R. (2017). Applied Systems Theory (2nd ed.). Glasgow: Springer.
44. Deloitte. (2022). Beneath the surface of a cyberattack A deeper look at business impacts. Deloitte.
45. Deloitte. (2022). Privacy by Design Setting a new standard for privacy certification. Deloitte.
46. Department of justice and constitutional development. (2016, December 9). Cybercrimes bill[B 6-2017]. Cybercrimes and cybersecurity bill, Government Gazette No. 40487. Republic of South Africa: Government Gazette No. 40487 of 9 December 2016. Retrieved from https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000
47. Dupont, B. (2019, September 7). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 1-17. doi: 10.1093/cybsec/tyz013

48. Edwards, M. (2020, August 5). Facing the Challenge of Aligning Cybersecurity and Business. Retrieved April 17, 2023, from gca.isa.org: https://gca.isa.org/blog/facing-the-challenge-aligning-cyber-security-and-business
49. European Union Agency for Cybersecurity. (2021). Cybersecurity for SMES Challenges and Recommendations. ENISA.
50. European Union Agency for Network and Information Security. (2016). Review of Cyber Hygiene practices. ENISA.
51. EY Global. (2019, April 09). Cybercrime. What does the most damage, losing data or trust? Retrieved June 16, 2022, from ey.com: https://www.ey.com/en_za/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust
52. Fin24. (2019). SA banks hit by ransom attacks. Retrieved July 25, 2021, from https://www.news24.com/fin24/companies/financial-services/sa-banks-hit-by-ransom-attacks-minor-disruptions-expected-20191025
53. Gerhardt, M. W., Nachemson-Ekwall, J., & Fogel, B. (2022, March 8). Harnessing the Power of Age Diversity. Retrieved from Harvard Business Review: https://hbr.org/2022/03/harnessing-the-power-of-age-diversity
54. Grant, C., & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House". Administrative issues journal, 4(2).
55. Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver Security Awareness Training, then Repeat: {Deliver; Measure Efficacy}. 2019 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-6). IEEE.
56. Hollard. (2017, January 23). The new word in insurance: cyber insurance. Retrieved June 18, 2022, from Hollard.co.za: https://www.hollard.co.za/brokers/news/short-term-broker-news/the-new-word-in-insurance-cyber-insurance
57. i-SCOOP. (2023, March 25). The CIA triad of confidentiality, integrity and availability . Retrieved April 2023, from i-SCOOP: https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/
58. IBM Cloud Education. (2019, December 4). What are Security Controls? Retrieved June 19, 2022, from ibm.com: https://www.ibm.com/cloud/learn/security-controls
59. IBM. (2022). Cyber Resilient Organization Study 2021. Retrieved June 16, 2022, from IBM.com: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/
60. International Organization for Standardization. (n.d.). ISO/IEC 27001 Information Security Management. Retrieved June 07, 2022, from iso.org: https://www.iso.org/isoiec-27001-information-security.html
61. IOL Media. (2003). How Absa hacker targeted clients' home PCs. Retrieved July 21, 2021, from https://www.iol.co.za/news/south-africa/how-absa-hacker-targeted-clients-home-pcs-110109
62. IOL Media. (2006). Bank admits to hacking attacks. Retrieved July 21, 2021, from https://www.iol.co.za/news/south-africa/bank-admits-to-hacking-attacks-284319
63. Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers & Security, 67, 267-279. doi:https://doi.org/10.1016/j.cose.2016.12.012.
64. Kaspersky Lab. (2015). Carbanak Apt the Great Bank Robbery. Kaspersky Lab.
65. Kaspersky Labs. (2022). Top Tips for Cyber Hygiene to Keep Yourself Safe Online. Retrieved June 15, 2022, from Kaspersky.com: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits
66. Keman, H., & Keri, P. (2019, 1). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Practice-based IS Research. doi:10.24251/hicss.2019.769
67. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792
68. Kosutic, D., & Federico, P. (2020). Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 43(1).
69. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22 (2), 77-81. doi: 10.1080/1097198X.2019.1603527
70. Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to Do Qualitative Data Analysis: A Starting Point. Human Resource Development Review, 19 (1), 94-106.
71. Li, L., Xu, L., He, W., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24. doi: https://doi.org/10.1016/j.ijinfomgt.2018.10.017
72. Lockheed Martin Corporation. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (E. M. Hutchins, M. J. Cloppert, & R. M. Amin, Eds.) Retrieved from https://www.lock-heed-martin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
73. Mabunda, S. (2019, June). Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill. Statute Law Review, 40 (2), 143-154. doi:10.1093/slr/hmx028

74. Malatras, A., Skouloudi, C., & Koukounas, A. (2019). Industry 4.0 cybersecurity: challenges & recommendations. European Union Agency for Network and Information Security (ENISA). European Union Agency for Network and Information Security (ENISA): European Union Agency for Network and Information Security (ENISA). doi: 10.2824/143986
75. Malinga, S. (2021, September 03). SA tech firms strive to disrupt gender status quo. Johannesburg, Gauteng, South Africa: ITWeb.
76. Mbelli, T. M., & Dwolatzky, B. (2016, 6). Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), (pp. 1-6). doi: 10.1109/CSCloud.2016.18
77. McBride, N. (2005, May 26). Chaos theory as a model for interpreting information systems in organizations. Information Systems Journal, 15(3), 233-254.
78. McKane, J. (2019). South African banks hit by massive DDoS attack. Retrieved July 25, 2021, from https://mybroadband.co.za/news/banking/324881-south-african-banks-hit-by-massive-ddos-attack.html
79. McLeod, A., Dorantes, C. A., & Dietrich, G. (2008). Modeling Security Vulnerabilities Using Chaos Theory: Discovering Order, Structure, and Patterns from Chaotic Behavior in Complex Systems. 7th Annual Security Conference.
80. Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
81. Morse, J., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. International Journal of Qualitative Methods, 1(2), 13-22.
82. Moyo, A. (2016). Standard Bank heist modus operandi 'not new'. Retrieved July 25, 2021, from https://www.itweb.co.za/content/nkLgB1MeNZGq59N4
83. Moyo, B. (2018). An analysis of competition, efficiency and soundness in the South African banking sector. South African Journal of Economic and Management Sciences, 21(1) (a2291). doi: https://doi.org/10.4102/sajems.v21i1.2291
84. My Broadband. (2022, March 20). Trans Union faces R10-million fine for hack. Retrieved June 18, 2022, from mybroadband.com: https://mybroadband.co.za/news/security/438098-transunion-faces-r10-million-fine-for-hack.html
85. Nedbank. (2020). Nedbank warns clients of potential impact of data incident at Computer Facilities (Pty) Ltd. Retrieved August 14, 2021, from https://www.nedbank.co.za/content/nedbank/desktop/gt/en/info/campaigns/nedbank-warns-clients.html
86. News24Wire. (2016). Standard Bank computer was hacked in R300 million ATM fraud hit. Retrieved July 25, 2021, from https://businesstech.co.za/news/banking/128602/standard-bank-computer-was-hacked-in-r300-million-atm-fraud-hit/
87. Nielsen, M. W., Alegria, S., Börjeson, L., Etzkowitz, H., Falk-Krzesinski, H. J., Joshi, A., . . . Schiebinger, L. (2017). Gender diversity leads to better science. Proceedings of the National Academy of Sciences, 114, 1740-1742.
88. Nyasvisvo, B. & Chigada, J.M. (2023) "Phishing Attacks: A Security Challenge for University Students Studying Remotely," The African Journal of Information Systems: 15(2), Article 3. Available at: https://digitalcommons.kennesaw.edu/ajis/vol15/iss2/3
89. Ocholla, D. N., & Le Roux, J. (2011). Conceptions and misconceptions of theoretical frameworks in library and information science research: a case study of selected theses and dissertations from eastern and southern african universities. Mousaion: South African Journal of Information Studies, 61-74.
90. Oiaga, M. (2006). Three South African Banks Hit by Hackers. Retrieved July 21, 2021, from https://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml
91. Open Group Standard. (2017). Open Information Security Management Maturity Model (O-ISM3), Version 2.0. The Open Group.
92. Padayachee, R., & Pillay, V. (2018, April 18). Women remain under-represented in emerging tech. PwC South Africa.
93. Payment Card Industry Data Security Standard. (2022). Requirements and Testing Procedures, v4.0. PCI Security Standards Council.
94. Petersen, F. (2019). Determinants for the acceptance and use of mobile health applications: Diabetic patients in the Western Cape, South Africa. University of the Western Cape.
95. Potgieter, D. W. (2011). Absa intercepts Land Bank swindle. Retrieved July 21, 2021, from https://www.iol.co.za/business-report/companies/absa-intercepts-land-bank-swindle-1009423
96. Ramluckan, T., van Niekerk, B., & Leenen, L. (2020). Cybersecurity and information warfare research in South Africa: Challenges and proposed solutions. Journal of Information warfare, 19 (1), 80-95. Retrieved October 31, 2021, from https://www.jinfowar.com/journal/volume-19-issue-1/cyber-security-information-warfare-research-south-africa-challenges-proposed-solutions
97. Raphael, J. J., Célestin, J. C., & Djiethieu, E. R. (2019, September 9). A Key to Strengthening IT Security? Chaos.

98. Republic of South Africa. (2013, November 26). No.4 of 2013: Protection of Personal Information Act, 2013. Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/20140 9/3706726-11act4of2013popi.pdf
99. Republic of South Africa. (2015, December 4). National Cybersecurity Policy Framework. Retrieved October 22, 2021, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
100. Republic of South Africa. (2015, December 4). National Cybersecurity Policy Framework. Retrieved October 22, 2021, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf
101. Republic of South Africa. (2021, June 1). Cybercrimes Act 19 of 2020. Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf
102. Rossman, G. B., & Rallis, S. F. (2017). An Introduction to Qualitative Research (Fourth Edition ed.). Sage.
103. Salim, H., & Madnick, S. (2016). Cyber Safety: A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack. Massachusetts: Massachusetts Institute of Technology.
104. SANS Institute. (2019). 2019 SANS Security Awareness Report. SANS Institute.
105. SANS. (2021). 2021 Security awareness report managing human cyber risk. sans Institute.
106. Saunders, M. N., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students (Eighth ed.). Pearson Education Limited.
107. Savage, S., & Schneider, F. B. (2009). Security is Not a Commodity: The Road Forward for Cybersecurity Research. Washington: Computer Science & Telecommunications Board of the National Research Council.
108. Simbanegavi, W., Greenberg, J. B., & Gwatidzo, T. (2015). Testing for Competition in the South African Banking Sector. Journal of African Economies, 24 (3), 303-324. doi: 10.1093/jae/eju022
109. Sinnot, J. D., & Rabin, J. S. (2012). Sex Roles. In Encyclopedia of Human Behavior (Second Edition ed., pp. 411-417). Academic Press.
110. Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17 (1), 42-60. doi:10.1108/JICES-02-2018-0010
111. South African Banking Risk Information Centre (SABRIC). (n.d.). Cybersecurity. Retrieved April 18, 2023, from Pmg.org.za: https://pmg.org.za/files/170228SABRIC-Cybersecurity.pptx
112. South African Reserve Bank Prudential Authority. (2020). Prudential Authority Annual Report 2019/20 20. Pretoria: South African Reserve Bank Prudential Authority. Retrieved October 5, 2021, from https://www.resbank.co.za/en/home/public-cations/publication-detail-pages/reports/pa-annual-reports/2020/10227
113. South African Reserve Bank. (2020, October 8). South African Reserve Bank imposes administrative sanctions on banks. Retrieved June 18, 2022, from Resbank.co.za: https://www.resbank.co.za/en/home/publications/publication-detail-pages/media-releases/2016/7425
114. Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic Cyber Hygiene: Does It Work? Computer, 52(4), 21-31.
115. Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. The African Journal of Information and Communication (AJIC), 20, 83-112.
116. Swart, W., & Wa Afrika, M. (2012). It was a happy New Year's Day for gang who pulled off...R42m Postbank heist. Retrieved July 21, 2021, from https://www.timeslive.co.za/news/south-africa/2012-01-15-it-was-a-happy-new-years-day-for-gang-who-pulled-offr42m-postbank-heist/
117. The information regulator of South Africa. (2021, April 1). Protection of Personal Information Act, 2013 (Act No. 4 of 2013). Retrieved October 21, 2021, from https://www.gov.za/sites/default/files/gcis_document/202104/44383gon297.pdf
118. Thompson, W., & Farber, T. (2020). Absa says 'some sensitive customer information' stolen by employee. Retrieved August 14, 2021, from https://www.timeslive.co.za/sunday-times/business/2020-12-01-absa-says-some-sensitive-information-leaked-by-employee/
119. Tisdale, S. M. (2015). Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. Issues in Information Systems, 16 (III), 191-198. Retrieved from https://www.semanticscholar.org/paper/ Cybersecurity%3A-Challenges-From-a-Systems%2C-Knowledge-Tisdale/5e0bb009f7b87 d3fff87b20e156a56a726f891fb
120. Turner, J. R., & Baker, R. M. (2019, January 10). Complexity Theory: An Overview with Potential Applications for the Social Sciences. Systems, 7 (1).
121. Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021, October). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109. doi: Developing a cyber security culture: Current practices and future needs
122. Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. The African Journal of Information and Communication (AJIC), 20, 113-132. doi: https://doi.org/10.23962/10539/23573
123. Vecchiatto, P. (2003). Hack not to blame in new Absa fraud case. Retrieved July 21, 2021, from https://www.itweb.co.za/content/mYZRX79PaepvOgA8

124. Wang, S., Ding, L., Sui, H., & Gu, Z. (2021). Cybersecurity risk assessment method of ICS based on attack-defense tree model. Journal of Intelligent & Fuzzy Systems, 40(6), 10475-10488.
125. Wilkinson, L. A. (2011). Systems Theory. Encyclopedia of Child Behavior and Development, pp. 1466-1468.
126. Winjit. (2021, March 31). Why SA businesses need to consider cyber security. Why SA businesses need to consider cyber security. Retrieved October 31, 2021, from https://www.itweb.co.za/content/Kjlyr7w14BEqk6am
127. World Economic Forum. (2022, 03 10). Can closing the cybersecurity skills gap change the world? Retrieved from Weforum.org: https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/#:~:text=Despite%20the%20headlines%20we've,year%2C%20it's%20simply%20not%20enough.
128. World Health Organisation (WHO), (2020). Beware of criminals pretending to be WHO, viewed 24 May 2023, from https://www.who.int/about/communications/cyber-security.
129. Xu, S., Yung, M., & Wang, J. (2021, April 28). Seeking Foundations for the Science of Cyber Security: Editorial for Special Issue of Information Systems Frontiers. Information Systems Frontiers, 263-267.
130. Zetter, K. (2015, 8). Hackers Finally Post Stolen Ashley Madison Data | WIRED. Hackers Finally Post Stolen Ashley Madison Data | WIRED. Wired. Retrieved from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
131. Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. Security and Communication Networks, 5, 422-437. doi: 10.1002/sec.331