A CRIMINOLOGICAL ANALYSIS OF THE COMMISSION OF CYBERCRIME IN THE SOUTH AFRICAN BANKING INDUSTRY: A CASE STUDY OF CYBERCRIME IN BANKS IN DURBAN, KWAZULU-NATAL

by

Perushka Pillay

Student Number: 213562910

This dissertation is submitted in fulfilment of the requirements
for the degree of
Master in Social Science: Criminology
in the
School of Applied Human Sciences
(Discipline of Criminology and Forensic Studies)
at the
University of KwaZulu-Natal (Howard College)
South Africa

Supervisor: Ms. Precious Nolwazi Ntuli

2022

DECLARATION

I, Perushka Pillay, declare that:

(i) The research reported in this dissertation, except where otherwise indicated, is my original research.

(ii) This dissertation has not been submitted for any degree or examination at any other university.

(iii) This dissertation does not contain other persons' data, or other information, unless specifically acknowledged as being sourced from them.

(iv) Where other written sources have been quoted, then:

a) Their words have been re-written but the general information attributed to them has been referenced;

b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) This dissertation does not contain text copied and pasted from the Internet, unless specifically acknowledged and the source being detailed in the dissertation and in the References sections.

……

Student

…….

Supervisor

DEDICATION

This study is dedicated in memory of my late brother, Thaveshan Pillay. You are always remembered and dearly loved.

This study is also dedicated to my husband (Mr Shannon), my parents (Mr Michael and Mrs Priscilla), and members of my family (Mr Selvan and Mrs Sarah). You have collectively shown me that I am stronger than I ever believed. Without your ongoing love, encouragement, and support, this research would not have been possible.

ACKNOWLEDGEMENTS

First and foremost, I want to express my gratitude to God. I am sincerely grateful for everything that has been bestowed upon me and for his blessings throughout my life. He has given me the strength and fortitude to persevere and finish my dissertation on time.

I also want to express my gratitude to the following people for their support and assistance throughout this project:

My Supervisor, Ms Precious Nolwazi Ntuli: Thank you for your unwavering support, guidance, and tremendous efforts. Your guidance has been invaluable and I consider myself fortunate to have had the opportunity to learn from you. You have provided me with critical and constructive input at every level of my research and I could not have asked for a better supervisor. This research would not have been possible without your assistance and guidance. Thank you for always having faith in me.

I am grateful to the **South African Police Service** for allowing me the opportunity to conduct this research and for their assistance during this project. Thank you so much Colonel Narayan, Lieutenant Colonel Joubert, Lieutenant Colonel Jacob, Lieutenant Colonel Didi, Lieutenant Colonel Olga, and Warrant Officer Zama for always being so helpful and willing to assist me with any questions I had during my research study.

To the South African Police Service (SAPS) officials who have participated in this study: Thank you so much for your co-operation and for taking the time out of your busy schedule to accommodate me. I appreciate all your efforts and contributions to make this study a success. Thank you for taking the time to share your input. It is greatly appreciated.

To My Husband Shannon Alastair Nair: Thank you so much for always standing strongly by my side and for motivating, encouraging, supporting, and pushing me to my limits. At times when I felt like giving up, you were always there to help me pick up the pieces and assist me in confronting the challenges that came my way. You helped me accept the things I could not change and to look at things in a positive light. Thank you for being exceptional.

I would also like to express my gratitude to my amazing parents, **Mr and Mrs Pillay**. You have both sacrificed much to help me through every part of my life and I am grateful for who I am today because of you. Thank you for your continuous love and encouragement throughout my studies.

I also sincerely thank all my family and loved ones who supported, encouraged, and cheered me on through this process.

Additionally, Mrs Linda Coertze deserves my sincere gratitude for the outstanding technical editing of this dissertation.

ABSTRACT

As expenditures in broadband infrastructure in developing countries have increased and barriers to internet access have decreased, this infrastructure has rapidly become a target for cybercrime. Developing countries such as South Africa, Kenya, and India have become the preferred destination for cybercriminals owing to their lack of cyber regulations and the prevalence of cybercrime illiteracy. Cybercrime has plagued numerous sectors in the South African landscape, one of which is the banking industry. This industry has experienced multiple types of cybercrime such as phishing, vishing, spams, identity theft, hacking, and malware. As all banks now rely on digital networks for their business operations, the risk of becoming a cybercrime victim has increased for both the banking industry and its clients.

The focus of this study was to establish and analyse the causes of the increased rate of cybercrime in banks and to determine the effectiveness of legislation in addressing the threat posed by cybercrime to the banking industry. The study explored selected South African Police Service (SAPS) detectives' experiences regarding cybercrime and ascertained these detectives' views on factors that contribute to cybercrime within the banking industry.

The researcher utilised a qualitative methodology as this approach allowed the elicitation of the view of various participants. The study could therefore focus on actual issues associated with cybercrime rather than on statistical significance. Ten detectives who investigated cybercrime in Durban, KwaZulu-Natal were interviewed and some intriguing findings concerning cybercrime were uncovered. The study revealed the prevalence of internal fraud within the banking industry, poor internal controls, ineffective processes and systems, banking clients' lack of knowledge and awareness of the looming threat of cybercrime, low conviction rates for cybercriminals; and SAPS officials' lack of skills in policing cybercrime in KwaZulu-Natal as some of the key factors that exacerbate cybercriminal activities in the banking industry. Based on the transnational character of cybercrime, it had been concluded that majority of the banks in South Africa and many other countries are under threat of cybercrime, and therefore they need to coordinate and implement a unified effort to tackle the growing threat of cybercriminal activities in the banking industry.

Keywords*: banking industry, crime, cybercrime, cybercriminal, internet and South African Police Service.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

KZN	KwaZulu-Natal
SAPS	South African Police Service
SABRIC	South African Banking Risk Information Centre
ABSA	Amalgamated Banks of South Africa
FNB	First National Bank
ECTA	Electronic Communications and Transactions Act
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
FICA	Financial Intelligence Centre Act
ICT	Information and Communications Technology
ATM	Automated Teller Machine
IP	Internet Protocol
SALC	South African Law Commission
POCA	Prevention of Organized Crime Act
NCPF	National Cybersecurity Policy Framework
DTPS	Department of Telecommunications and Postal Services
SSA	State Security Agency

CHAPTER ONE
INTRODUCTION AND THE BACKGROUND

1.1 Introduction and Background of the Study

This chapter introduces the reader to the study's research topic and includes an overview of the project by explaining what it is about, why it is important, and who will benefit from it. The first section of the chapter outlines the study's intention and background. The discussion then moves to what prompted this research by elucidating the problem that it sought to understand and the new insights that were gained to better understand the dynamic nature of cybercrime. The study's aims, objectives, and the research questions are also outlined. Definitions of key concepts are provided, such as the internet, cybercrime, cyberspace, online, and the banking industry. The chapter also presents an overview of the approaches the study employed to collect and analyse the data to draw conclusions that support the study's objectives. In addition, an outline of each chapter for the entire research study is presented.

Technological and social change has increased significantly in the twenty-first century and there has been an emergence of new criminal activities that were not present historically, and therefore could not be prosecuted by authorities (Sissing, 2013). Attacks on digital technologies are referred to as cybercrime, or online crime, which is committed in the cyber-environment using technological systems that may involve computers, mobile phones, and credit-card machines (De Angelis & Sarat, 2000). Cybercrime can be referred to as any illegal action whereby the internet and/or computers can be used as a primary method of committing a crime (Booysen, 2011). According to Obeng-Adjei (2017), the existence and use of internet tools to commit a crime render individuals, corporations, and countries powerless against cybercrime-related attacks, while the risk of the exposure of information, confidentiality, data integrity, and accessibility increases. South Africa has presented some of the highest cases of cybercriminal activities globally (Von Solms, 2015), and according to the SAPS Directorate for Priority Crime Investigation (DPCI), cybercrime has steadily risen in banks in Durban, KwaZulu-Natal (Cole, 2013). Unlike conventional crimes, cybercrime leaves no visible evidence and can be carried out from afar, which adds to the difficulty of policing this crime effectively. As indicated by Oladipo (2015:2), “South African banks, businesses, government agencies, and internet service providers (ISPs) prioritise the performance and features of their

websites to entice consumers, yet measures to police the internet are of a low standard and quality".

The escalation of cybercrime has had a negative effect on the use of digital infrastructure and information technology. Cybercriminals are devising increasingly advanced forms of hacking and counterfeiting to gain access to information regardless of technical security advancements. According to a former Chief Executive of the South African Banking Risk Information Centre (SABRIC), Kalyani Pillay, cybercriminals are highly skilled in utilising social engineering to force their individuals into revealing their confidential information (Malinga, 2019). Cybercriminals capitalise on the idea that digital customers are not all technologically savvy and therefore they exploit the victim's weakness. Through the use of technology, together with social engineering, criminals are able to collect sufficient data to impersonate a victim and bypass bank security protocols (Naidoo, 2018). Mugari, Gona, Maunga, and Chiyambiro (2016) indicate that cybercrime poses a significant threat to all aspects of the economic activities of every nation, which is a threat that is more pronounced in banking than in most other industries. In November 2002, the South African government introduced a cybercrime section into the Electronic Communications and Transactions Act (hereafter the ECT Act) of 2002 to create the first legislative framework against cybercrime (Van der Westhuizen, 2019). Critics have argued that the section on cybercrime in the ECT Act is too broad and that it does not properly legislate cybercrime codification and related punishments to effectively prosecute cybercriminals. The key concern of the Regulation of Interception of Communications and Provision of Communication- Related Information Act (RICA) of 2003, however, is that it acts as a violation of the constitutional right to privacy (Van der Westhuizen, 2019), which is addressed in the Protection of Personal Information Act of 2013, commonly known as the PoPI Act.

Van der Westhuizen (2019) states that cybercrime caused severe losses to the South African business sector in 2015. The World Economic Forum (cited in Ikdal, 2017) estimated the value of these losses to be around R5,8 billion. As indicated in a report by SABRIC (2014), 75% of fraud that occurred in South African banks was attributed to cybercrime schemes. According to SABRIC, 13 438 incidents occurred across banking applications, online banking, and mobile banking facilities in 2017, resulting in the loss of R250 million. Kgosana (2018) mentions that, between January and August of 2018, cyber and digital crimes resulted in a loss of over R183

million, while mobile banking increased by 100%. Furthermore, in 2018 online banking scams resulted in the loss of R89,3 million (Kgosana, 2018).

The banking sector in South Africa is the main target for cybercrime operations and banks have to spend three times more on cyber security than other organisations (Van der Westhuizen, 2019). In traditional crimes, criminals were found to leave a trail of traceable evidence that could be utilised to ascertain a crime, however criminals who attack from cyberspace are very difficult to trace and therefore difficult to apprehend. Van der Westhuizen (2019) mentions that the government has adopted various forms of legislation since the early 2000s to counter the ever-evolving problem of cybercrime. However, regardless of all these efforts, it still remains difficult to enact legislation to combat cybercrime and ensure data protection.

The exponential growth of cyberspace in South Africa is not balanced by the provision of the needed skills to combat crime in this sphere. The United Nations Economic Commission for Africa (2014) states that broad-based internet safety and security education programmes are required to resolve the issue of social security and protection for users. In addition, enabling safe access to information and communication technology (ICT) is of vital importance for users. It is important to note that no individual or institution has the mandatory capacity to deal with cybersecurity as it is not a mechanism but a process, therefore it is not just a matter of passing legislation. The United Nations Economic Commission for Africa (2014) enlists parliamentarians, attorneys, the judiciary, the military, civil society, the media, the youth, and the public as key stakeholders, arguing that they should all be active in efforts to address cybersecurity. This organisation urges that it is crucial to have all the necessary stakeholders involved to ensure the requisite understanding of processes and concerns associated with cybercrime.

Although research has been conducted on cybercrime, a paucity of literature exists on cybercriminal activity in the banking industry within South Africa, particularly in KwaZulu-Natal. Even though the globe is now more technologically connected than it has ever been, the prevalence of cybercrime persists, and there seems to be a lack of proactive strategies to curb this crime. When a 2014/2015 crime statistics report (South African Police Services, 2015) was perused, no information on cybercrime could be traced. This prompted the researcher's intention to create awareness among relevant role-players such as the banking industry, the SAPS, and internet users regarding the threats this crime poses. As cybercrime has almost no

consideration for national borders, investigations and prosecutions are complicated by the fact that criminals, victims, and technical infrastructure are spread across numerous jurisdictions, which is a fact that adds to the many challenges associated with cybercrime. Against this background, it was deemed urgent to create awareness of this crime among the public and to enlighten all affected parties about the current situation, as well as potential concerns, regarding cybercrime. This could be a positive step towards curbing the impact of this crime on unsuspecting and innocent citizens.

1.2 Problem Statement

SABRIC states that South Africa is rated the third highest when it relates to individuals being victim to cybercrime activities and this makes up a total of around R2,2 billion a year that was a result of cyberattacks (Naidoo, 2018). According to Sizwe Cakwebe, cyber risk manager at SHA Risk Specialists, South Africa loses roughly R2,2 billion each year as a result of cybercrime (Craig, 2021). According to the annual crime statistics of SABRIC in 2020 (Craig, 2021), identity theft and phishing, which is when emails and SMSs are modified to look legitimate in order to deceive victims, are the top issues associated with cybercrime. Because financial institutions are pivotal to secure and accessible financial systems, their failure to curb cybercrime will have a detrimental impact on the financial stability of this country in the medium and long term. Despite this threat, banks have failed to implement strategies to counteract cybercrime, which enhances the appetite of cybercriminals even when they are challenged from the highest levels and by the most proficient specialists. Information technology (IT) specialists in South Africa have had minimal success in developing systems to control the risks associated with cybercrime, and it is argued that this is due to a lack of comprehensive empirical research on this topic. This gap in knowledge has also resulted in the failure of the banking industry to appropriately detect and manage cyber-risk and the detrimental impact it has on their operations. The limited body of literature on criminal cyber activities, particularly in the context of the South African banking industry, thus prompted the researcher to explore cybercrime in a delimited area. One focus was on identifying the factors that contribute to cybercriminal activity in South African banks in Durban, KwaZulu-Natal. In light of the limited controls in the South African banking industry to curb cyberattacks, their control strategies and the legal framework to map and dynamically manage the banking industry's IT system architecture were viewed as critical in mitigating cybercrime.

1.3 Aim of the Study

With the ever-evolving progress in digital technologies, societies have witnessed an increase in the number of individuals who have devices and smartphones that are connected to the internet. Therefore, most South Africans who use digital banking platforms are targets for savvy cybercriminals (Mungadze, 2019). At present, there is a paucity of data on cybercrime in South Africa, and specifically on the banking industry. The increasing number of cybercrime activities that occur within the banking industry in South Africa needs to be documented so that an enabling policy can be ratified to protect banking clients against this crime. This study therefore analysed the causes of cybercrime activities that target banks, and specifically looked at the provision of qualified technicians and fraud experts within the industry.

Another aim was to examine the legal framework that guides financial institutions such as banks to determine if any weaknesses could be rectified to strengthen banks' legal position with regards to cybercrime prevention. The banking industry is required to evaluate existing cybercrime activities to better identify and mitigate the risks they face. The study thus critically analysed the effectiveness of legislations and their practical implementation to determine if they protect banks in the study area against cybercrime. Based on the findings, it is envisaged that this study will contribute to knowledge in the field of cybercrime as, prior to the study, very limited research was conducted to generate data regarding cybercrime in banks, particularly in the study area.

1.4 Research Objectives

The objectives of the study were to:

- Establish the causes of the increased rate of cybercrime in banks;
- Identify pieces of legislation that address cybercrime in South African banks;
- Examine legislations and policies that guide the implementation of cybercrime countermeasures in South African banks to determine if they are effective.

1.5 Research Questions

The questions that needed to be answered were:

- What are the causes of the increased rate of cybercrime in South African banks?

- What cybercrime legislations have the government implemented to support financial industries in South Africa?
- Are policies that guide countermeasures against cybercrime effective in the banking industry?

1.6 Significance of the Study

As the banking industry trades in money and data, it is a major target for cybercriminals. Moreover, weaknesses in banking systems make their data relatively easy to obtain. While the banking industry is vigilant and utilises various security measures, cybercriminals that target them are always a step ahead and this results in a large percentage of successful attacks by these criminals. Today's banking industry is completely reliant on computer technology, thus it is startling that some information systems have not been effectively adjusted to combat the ever-changing technological environment to deal with the threats that banks face. The significance of this study is that it will raise awareness of these threats in the banking industry, and among SAPS law enforcers and public internet users.

It is this researcher's contention that we can close the loopholes that cybercriminals exploit in the context of the fourth industrial revolution if South Africans are better informed about the ever-changing modus operandi of these criminals and if banks adopt a more intensive approach to advanced protection and attack detection methods. It is critical to raise awareness of this threat even as banks continue to invest enormous sums of money in decreasing the negative effects of cybercrime. The banking industry and its clients should be aware that there is a lack of implementation of active strategies. Cybersecurity risk management must thus be addressed as a matter of urgency and on a constant basis as cybercriminals seem to stay abreast of any newly implemented measures to curb their activities. This research will extend the knowledge base on this phenomenon and will offer insight into what factors allow cybercrime to occur and flourish in the banking industry and how they affect banks' overall performance. This research is significant because it highlights the need for all banks to protect themselves against a variety of sophisticated cyberattacks and to effectively address the risks they face in this regard.

1.7 Definitions of Key Concepts

Internet: The internet can be referred to as a global collection of computers that utilise the communication protocol Transmission Control Protocol (TCP)/ Internet Protocol (IP). A subset of such computers is known as the World Wide Web (Hitchcock & Page, 2006).

Cybercrime: Verdegem, Teerlinck, and Vermote (2015:1) state that cybercrime is an "umbrella term to describe different online threats such as malware, scams, and hacking". The use of a computer to advance illicit goals such as fraud, trafficking in child pornography and intellectual property, stealing identities, or invading privacy is known as cybercrime, which is also sometimes referred to as computer crime.

Cyberspace: This is an umbrella term for the World Wide Web, which is a virtual reality that is accessible only by computers, mobile devices, or any device with internet connectivity (Cambridge Dictionary, n.d.).

Online: This is the state of being when a person is linked to an Internet Service Provider (ISP), an American web portal and online service provider (AOL), and is e- or Earthlink connected (Sissing, 2013). Everything performed when linked to an ISP is considered to be online such as e-mails, browsing blogs, and when chatting or reading news bulletins online (Hitchcock & Page, 2006).

Banking industry: According to Amadeo (2021:1), "banking is an industry that handles cash, credit, and other financial transactions for individual consumers and businesses alike".

1.8 Methodology

This research adopted a qualitative approach and the overall objective is to describe the social world, through comprehending, explaining, and discovering individuals experience and feelings in a great depth, from a human standpoint. Shuttleworth (2008) mentions that a qualitative research design has the advantage of being versatile and allowing for a wide variety of techniques for data collection and analysis.

1.8.1 Research design

Leedy (1997) describes a research design as a study plan that outlines the overall structure for data collection. Burns and Grove (2001) state that a clearly specified framework within which a study is implemented is referred to as its research design. This researcher used an exploratory study design which was embedded within the qualitative approach to provide a full criminological analysis of the commission of cybercrime in the South African banking industry. Burns and Grove (2001:374) define exploratory research as "research that is performed to gain new insights, find new ideas, and increase knowledge of the topic under investigation". The reason why data were collected from selected SAPS officials in the current study was that these individuals were responsible for investigating cybercrime.

1.8.2 Sampling

In this study, purposive sampling technique was utilised to select the research participants. This method of sampling is appropriate when the researcher wishes to concentrate on a relatively small sample and in this case, the researcher selected a sample of ten (10) SAPS officials. The researcher recruited these participants from two police stations and two detective units. The sample from the two police stations comprised of three research participants, while seven research participants were recruited from the two detective units. Sampling involves selecting a subset of the data population, to be used for participation in a study, based on a set of criteria (Polit & Beck, 2004; Uys & Basson, 1991).

1.9 Structure of the Dissertation

Chapter one: Introduction and the background

This chapter provides the background to the South African cybercrime landscape. It also presents the purpose (or aim) of the study as well as its objectives and the research questions. It briefly refers to the study approach, provides insight into the cybercrime phenomenon, and acquaints the reader with the research topic in general.

Chapter two: Literature review

In this chapter the phenomenon of cybercrime is discussed based on a review of scholarly literature and the South African legal framework that aims to address this crime. The discourse focuses on definitions of cybercrime, the impact of cybercrime on the banking industry and its

clients, legislation that addresses cybercrime in South Africa, and South African and global views of cybercrime.

Chapter three: Theoretical framework

The theoretical framework within which this study was located is discussed. The theories that underpinned this study were the routine activity theory, the rational choice theory, and the space transition theory. These theories were utilised as each contextualizes a different component of cybercrime.

Chapter four: Research methodology and methods

This chapter discusses the research methodology that was utilised in detail. Due to the nature of the study, the qualitative research approach was supported by an exploratory research design. This chapter also discusses the methods of data collection and analysis as well as the ethical considerations that were adhered to.

Chapter five: Data presentation and interpretation of the findings

This chapter presents a summary of the results that emerged from the data analysis process. These results are in line with the research questions and objectives that directed the study. The discourse refers to findings from the literature and determines if the current study supported or refuted these results.

Chapter six: Conclusion and recommendations

This chapter presents concluding remarks about the findings and offers some recommendations for future study.

1.10 Conclusion

The dilemma that motivated this research is that individuals are becoming increasingly dependent on internet and computers, as digital technology progresses, however, millions of individuals are vulnerable to cybercrime because information can be easily and instantly transmitted in cyberspace. This emphasises the importance of implementing effective and efficient cybercrime detection and policing systems in South Africa. Internet banking has introduced a new age in the banking service industry which constantly seeks new horizons of growth and advancement to improve its business operations. Unfortunately, evidence from the

field has shown that this innovation comes with a certain level of exposure to cybercrime and data security breaches, both of which have resulted in a negative view of the banking industry globally, but particularly in South Africa.

This chapter explained the purpose of this study as well as its epistemological position. A criminological analysis of the commission of cybercrime in the South African banking industry, with particular reference to Durban, KwaZulu-Natal, was undertaken and this chapter explained the study's context. The researcher paved the way for the reader to grasp the logic for this undertaking by raising the issues of insufficient literature and flaws in the current banking system. It was explained that the high and escalating rates of cybercrime in South Africa pose a serious threat. Moreover, this country ranks third in the world in terms of incidences of cybercrime. The research objectives and questions that guided the study were presented, and it was explained that members of the SAPS, who were knowledgeable of cybercrime in KwaZulu-Natal, had been recruited as participants. A review of the literature that was consulted will be presented in the following chapter.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

In the past few years, statistics have demonstrated that cybercrime is on the ascendency in South Africa, with digital banking fraud across all platforms increasing from 13 389 reported incidences in 2017 to 23 466 in 2018. This was a 75.3% increase (Spyridon, 2012; SABRIC, 2018). As indicated by Obeng-Adjei (2017), the advent of the internet has changed the manner in which we converse with one another, as well as the systems that are utilized to accomplish activities on a day-to-day basis. Newman and Clarke (2003) explain that internet activities allow one to shop, bank, and network across a wide spectrum using social media without having to physically leave a specific location.

As cybercrime has no physical borders and is not subject to import/customs or currency restrictions, it is easily accessible for anyone from anywhere in the world, particularly for those who nefariously wish to access banking credentials (Gordon, 2002). Obeng-Adjei (2017) and Leukeldta & Yar (2016) mention that examples of cybercriminal activities include computer hacking, identity theft, phishing, denial of service, the misappropriation of malignant programming, media and software piracy.

The Norton Cyber Security Insights Report (cited in Yedaly, Amazouz, & Yankey, 2016) states that 8.8 million South Africans were victims of online offences, while there were 602 million cybercrime victims internationally in 2015. Some of the main reasons why financial institutions have switched to electronic banking are that it is less expensive due to lower administrative and labour costs, more stable (it is generally easier to protect electronic money than physical money), and offers new opportunities for easy banking access such as smart cards. However, while it is legal to use digital signatures under the ECT Act, the risk of fraud, the lack of personal contact, and the security threats associated with internet banking remain a major roadblock that needs to be overcome.

2.2 Conceptualising Cybercrime

According to Brush, Rosencrance, & Cobb (2021), Aghtise (2014), and Brady & Heinl (2020), cybercrime is a computer-based crime which usually connotes crimes committed using a computer network. With growing advancements in digital technologies, the essence of cybercrime has changed dramatically over the years. The nature of this crime and the complexities associated with it make the enforcement of laws and policies to combat cybercrime extremely challenging for policymakers as well as government and law enforcement agencies (Obeng-Adjei, 2017). Moreover, the complexity of this crime weakens international cooperation and endeavours. Nevertheless, several government departments and law makers have agreed to collaborate in an effort to enact legislation and measures to counter its effects (Holt, Bossler, & Seigfried-Spellar, 2015).

What is cybercrime? It is described by the Council of Europe as "any criminal activity against or with the aid of a computer network" (United Nations Office on Drug Crime, 2013:18). Cybercrime is also defined as "computer-mediated activities that are illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Thomas & Loader, 2000:5). Other sources describe cybercrime as the unauthorised access to a computer system for the purpose of removing, altering, or harming computer data (Sarrab, Aldabbas & Elbasir, 2013; Broadhurst, 2006). These multiple definitions suggest that it is a dynamic type of crime because it has multiple types and motivations (Sarrab et al., 2013).

2.2.1 The complexity of cybercrime

Cybercrime detection and prosecution are made more difficult by the pace of advancement and the strength of modern information technology. For example, communications networks now cover the globe, and even a small personal computer can be linked to sites in various hemispheres with ease. This poses serious issues in terms of jurisdiction, evidence availability, investigative coordination, and the legal framework(s) that can be applied to cybercrime (Ibikunle & Ewemiyi, 2013). The ease with and degree to which digital knowledge can be converted and interpreted are related. For instance, a piece of knowledge can be interpreted using software or text (source code), executable code (binaries), or it can be converted in a number of ways, including mathematically, through encryption, or by conversion to a holographic picture or music (Okonigene & Adekanle, 2009). The latter authors state that, as a result, the format in which information is stored could one day lose its legal status. This information malleability has consequences in terms of device break-ins, where information

cannot be lost but is temporarily rendered unavailable. Such activities are difficult to classify as fraud or a data breach, which makes dealing with cybercrime and data security breaches difficult (Ibikunle & Ewemiyi, 2013).

It is essential to highlight two primary elements of cybercrime, namely computer-assisted and computer-focused crimes. Obeng-Adjei (2017) states that computer-assisted crimes can be referred to as unlawful acts that are performed in cyberspace, and money laundering is an example of this. The software systems, as well as the internet can be seen as enablers to cybercriminal activities. Furnell (2002) states that computer-focused crimes are attacks that target IT systems, arguing that this crime would not have existed without it. Hacking and virtual attacks are examples of these type of crimes, and it is evident that technology plays a major role in how these crimes are executed. Accordingly, technology plays an unforeseen (computer-assisted) or a necessary (computer-focused) role in characterising how a crime is committed (Yar, 2013). Rosewarne (2012) indicates that the multiplication of cybercrime is ascribed to two components which are underpinned by people reacting to financial and psychological gains. Rosewarne (2012) proposes that the common utilisation of the internet and the low punishment enforced on the cybercriminal once detected are the key drivers of cybercrime multiplication in South Africa.

2.2.2 South African and international views of cybercrime

With the increased use of computer technology, cybercrime has escalated and has become a serious problem on a global scale. A major drawback from the standpoint of crime prevention is that the perpetrator may not be situated in the same location, or is not even a member of the same nation, as the banking industry being targeted. Due to the pervasive nature of cybercrime, effective cooperation from all domains is required to garner the attention of governments from other nations as well as private and public sector organisations to combat and prevent cybercrime. In 2011, alongside terrorist threats and natural disasters, the United Kingdom government placed cybercrime as a top priority and pledged £650 million over a four-year period to combat it (Rosewarne, 2012). Across major economies such as the USA, China, Japan, and a number of African countries (such as Botswana, Kenya, Nigeria, Papua New Guinea, and Uganda) the same pattern is seen. Cybercrime is transnational and permeates all businesses across the world (Obeng-Adjei, 2017), and the South African landscape is no exception.

The Cyber Security Framework was adopted by the South African Cabinet to resolve national security threats, promote private and public investments in research and development, counteract cybercrime and cyberwarfare, raise cybersecurity awareness, encourage participation in trusted forums to exchange knowledge on cybercrime, build trust and confidence in the use of information technology, establish a security curriculum, and update existing cybersecurity regulations (Obeng-Adjei, 2017). As indicated by Rosewarne (2012), cybercrime proliferation is due to two factors: individuals who desire monetary gain, and psychological benefits for perpetrators. Rosewarne (2012) postulates that the widespread use of the internet and the low punishments levied on convicted cybercriminals exacerbate the proliferation of cybercrime in South Africa.

2.3 The Impact of Cybercrime on the Banking Industry and its Clients

2.3.1 The advent of information communication technology

Information communication technology (ICT) has revolutionised and streamlined our lives. Raghavan and Parthiban (2014) state that ICT has been implemented in various industries and has been used to streamline business processes by means of coding, customising, categorising, and summarising facilities and applications. However, it has also launched an unintended repercussion in the form of cybercrime. Cybercrime has plagued numerous sectors; one of these is the banking industry that has experienced multiple types of cybercrime such as phishing, vishing, spams, identity theft, hacking, and malware. History has demonstrated that innovation is accompanied by disruption, which is particularly true in the banking industry where cybercrime is rife.

The banking sector has seen the introduction of digital platforms that facilitate self-service for banking clients who no longer have to physically go into a bank branch. According to the South African Banking Risk Information Centre (2018), innovative and current banking platforms also generate new ways for criminals to use social engineering to target unsuspecting bank clients. Banks have responded by introducing various digital platforms to enhance their customer base, and transactions can now be accomplished without much effort (Vrancianu & Popa, 2010). By utilising these technologies, customers can access their bank finances through ATMs and smartphones while online banking is available 24/7 all year round.

2.3.2 Cybercrime victims in the banking industry

As mentioned by an Organisation for Economic Co-operation and Development (OECD) (2007) report, victims in the banking sector can be divided into two categories: the bank, and bank users. The users or clients may be individuals, small- and medium-sized companies, or major multinational firms. Individual users and small- and medium-sized businesses are the most targeted groups as they engage in risky online behaviour or do not use security measures during transactions (Asghari, 2010; Mannan & Van Oorschot, 2008).

The rise in fraud as criminal's access banking apps can be attributed to increased use by bank clients of these facilities. SABRIC (2018) mentions vishing is being used as a method by fraudsters to obtain transactional authentication tokens in the form of one-time passwords (OTPs) and random verification numbers (RVNs). Raghavan and Parthiban (2014) state that financial services have spread to the masses because of the development of IT and the penetration of mobile networks that have become central to people's daily lives. Cyber criminals use various means to steal information from customers' banks, and eventually also their money (Choo, 2011). In banking app fraud, the most common modus operandi is vishing, whereby a fraudster makes contact with a potential victim, impersonating a bank official and using their expertise in social manipulation to persuade the individual to reveal confidential data, and this data is used to deceive the victim (SABRIC, 2018).

2.3.3 The impact of COVID-19 on criminal activity in the banking industry

During the COVID-19 pandemic, the banking industry experienced a spike in criminal activities. This coincided with the establishment of disaster management restrictions, but financial crime trends escalated in this period (Majola, 2021). The South African Banking Risk Information Centre's annual crime statistics for 2020 (SABRIC, 2020) mentions that the pandemic prompted changes in human behaviour and movement as well as in policing, and this resulted in new prospects for criminals and a considerable increase in the number of criminal cases in this sphere. While certain crime types declined, others soared as criminals sought to profit from conditions during the COVID-19 pandemic. According to data produced on behalf of the banking industry, digital banking fraud climbed by 33%, debit card fraud jumped by 22%, and credit card fraud declined by 7% (Majola, 2021).

According to SABRIC CEO, Nischal Mewalall, as customers shifted to online shopping and making payments through their banking application (or app), fraudsters increased their efforts to phish clients in order to gain their personal information and scam them on digital and online platforms (Majola, 2021). In addition, Shabir Chohan, the Chief Executive of Al Baraka Bank, issued a strong warning to consumers, particularly those new to online transactions of any kind, and urged that they should be vigilant in protecting their personal information against cyber criminals now and in the future. His warning came in the wake of events involving bank consumers who had been the targets of actual and attempted scams (alBaraka Bank, 2021).

According to Mewalall (cited in Majola, 2021), cybercrime and data breaches will pose an enormous threat to customers and banks in the future as even the strongest security measures and technology can be compromised when criminals illegally acquire and use legitimate data to commit their crime. Mewalall also advises bank clients not to click on links in unfamiliar emails, as these links are often used in phishing emails to direct consumers to spoof websites that appear to be legitimate online merchants, complete with appealing graphics and persuasive taglines. However, criminals utilise these deceptive websites to steal bank card information and use an account to make online purchases.

Furthermore, Chohan (cited in alBaraka Bank, 2021) mentions that consumers must ensure that their personal information and data are secure to avoid identity theft and deceiving actions on various online platforms as a result of the shift in public behaviour. Chohan highlights that, while electronic innovation is to be embraced, the era of technology has the power to entrap the unwary. It is crucial to be aware that with technology, one's personal data are at risk unless adequately safeguarded to prevent cybercriminals from obtaining access as a way to defraud one of one's money (alBaraka Bank, 2021).

A TransUnion study that was released in June 2021 states that, as more and more people use the internet for banking and other financial transactions, fraudsters are increasing their efforts in the financial services business (Majola, 2021). The percentage of suspected digital fraud attempts in South Africa in financial services climbed by 187% during the last four months of 2020 (1 September to 31 December 2020) and the first four months of 2021 (1 January to May 2021), while financial services fraud attempts grew by 149% globally (Majola, 2021).

2.4 Digital Banking Fraud

2.4.1 Banking app fraud

The increased use of digital platforms by bank customers is to blame for the rise in banking app fraud. Vishing is a way for fraudsters to acquire transaction verification tokens, also known as OTPs and RVNs. Vishing is the most popular form of bank app fraud (SABRIC, 2018). It is a type of fraud in which a fraudster impersonates a bank official or a service provider and uses social engineering techniques to entice the victim to disclose sensitive information. The victim is then defrauded using the knowledge received. As indicated in the diagram below, there was an 82,1% increase in this crime from 2017 to 2018.

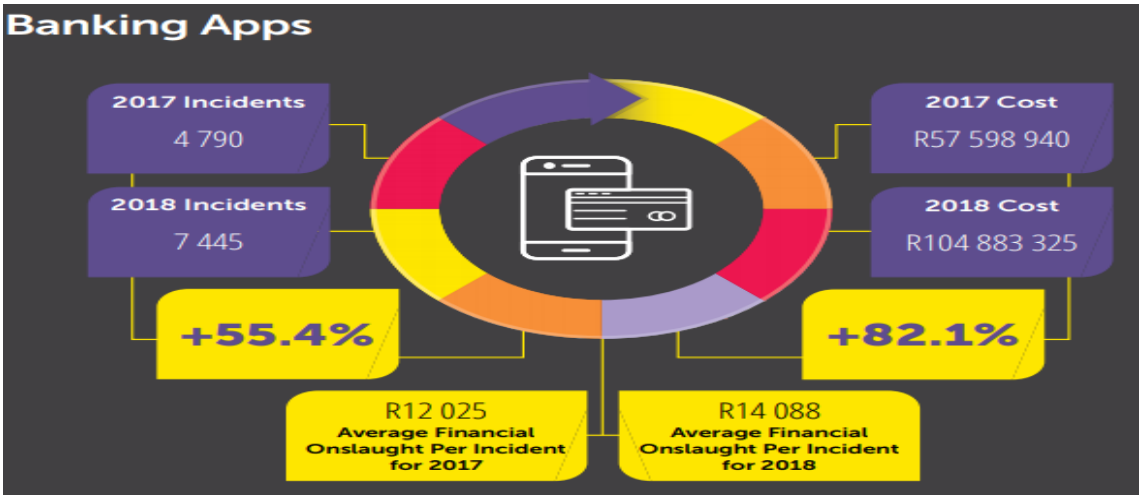

Figure 2.1: Rates of onslaughts on banking apps

Source: SABRIC Annual Crime Statistics (2018)

2.4.2 Online banking

Phishing emails are also the most powerful tool for collecting client banking login credentials for fraudsters. According to SABRIC (2018), phishing emails ask users to click on a connection in an email that takes them to a spoof website that pretends to be their legitimate bank's website in order to obtain, check, or update contact details or other sensitive financial information. A monthly average of 325 new cases has been registered since October 2018. As indicated in the comparison graph below, there was an increase in the number of cases from 2 837 in 2017 to 3 900 in 2018.

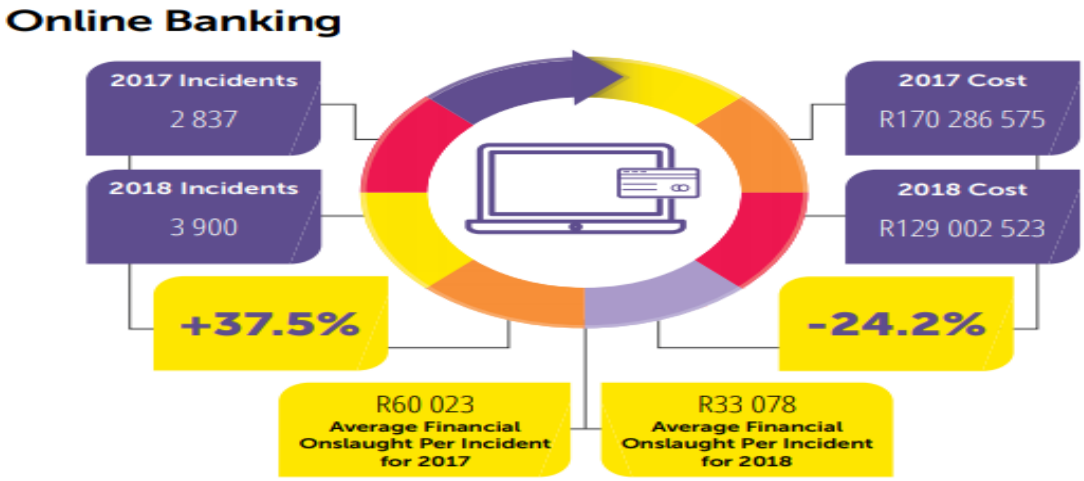

Figure 2.2: Rates of onslaughts on online banking

Source: SABRIC Annual Crime Statistics (2018)

2.4.3 Mobile banking

After a drastic rise between January and September 2018, reported fraud on the mobile banking channel stabilised in the fourth quarter of 2018. From October to December 2018, there was an average monthly gross loss of R700 000 (SABRIC, 2018). In the mobile banking fraud sphere, 'smishing' (short for SMS phishing) is the preferred method used by fraudsters to obtain confidential information. It is similar to phishing, but instead of emails, text messages are sent that instruct the user to call a number or click on a connection which entices them to disclose their personal information. As indicated in the comparison graph below, there was a 100% increase in the number of cases from 2017 to 2018.

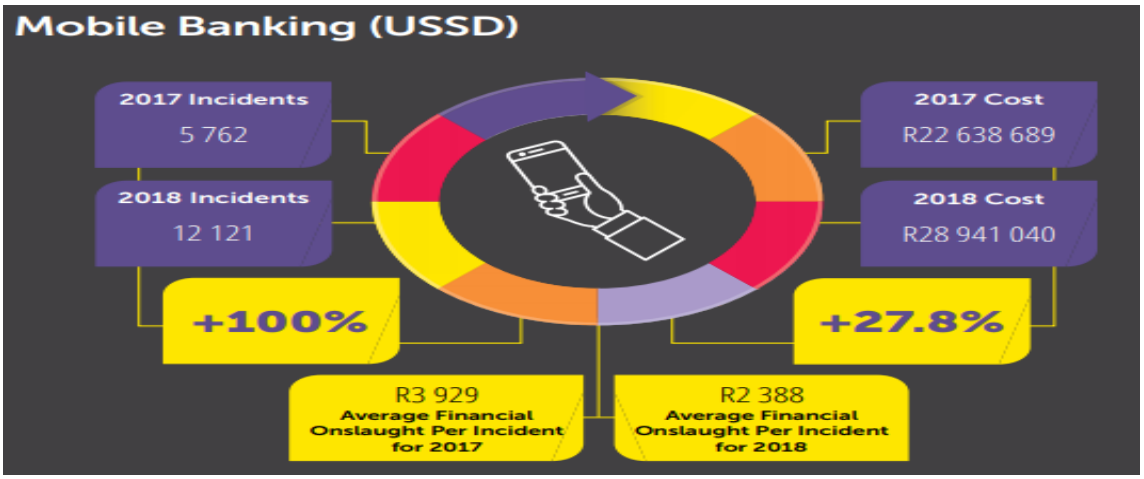

Figure 2.3: Rates of onslaughts on mobile banking

Source: SABRIC Annual Crime Statistics (2018)

2.4.4 Distributed denial of service (DDoS)

According to Brindley (2020:1) "the increased focus on South Africa by cyber threat actors is due to interconnected factors such as lack of investment in cybersecurity, developing cybercrime legislation, law enforcement training, [and] poor public knowledge of cyber threats". In 2021, ransomware paralysed the network of Johannesburg agency City Power. The City of Johannesburg was targeted by a group known as the Shadow Kill Hackers who demanded a bitcoin ransom payment (Brindley, 2020). Hackers conducted distributed denial of service (DDoS) attacks on local banks shortly after, flooding them with bogus traffic. A ransom was also requested by the perpetrators. DDoS attacks on financial institutions still pose a significant threat to companies and government agencies all over the internet. The need to protect financial institutions from the security risks associated with DDoS attacks is a crucial business necessity, and curbing such attacks on application and network layers has long been a priority of the financial industry.

Due the advent of newer financial industries such as bitcoin and the continued increase in crypto-currency assaults, the financial sector remains vulnerable. Lambert (2019) mentions that customers are unable to access their online banking and trading websites due to targeted and botnet attacks that trigger slow website response times. As indicated by Lambert (2019), criminals who search for ways to compromise confidential data, commit fraud, or steal private and financial data can use attacks as a diversionary tactic. These malicious programs lay the groundwork for a potentially crippling DDoS attack against a financial institution. DDoS attacks can render banking websites inaccessible, and this results in lost revenue, reputational harm, and a loss of customer confidence. A financial institution can face liquidity and capital risks if a bad actor's intent is fraud.

2.4.5 Social engineering

The science of using social interaction to induce a person or an organisation to comply with a request from a computer-related entity is known as social engineering. A social engineering attack consists of a social engineer, an aim, a goal or more enforcement principles, and one or more techniques that use either direct or indirect communication (Van Rensburg, 2017). According to Maan (2008), social engineering is the method of obtaining useful and sometimes sensitive and private information by illegal means, or the accomplishment of some other illegal

goal, through deception and coercion of individuals. However, Mouton, Leenan, Malan, and Venter (2014) indicate that a distinction can be made between social engineering as an art of persuading people to reveal confidential information and the practice of doing so as a social engineering attack.

A social engineer identifies the weakest link in a security model that is based on logic and subject to human nature's inclinations. According to Van Rensburg (2017), social engineering hackers rely on people inside a targeted organisation to either willingly share private information or the fact that they are unaware of the importance of information they have access to, and are thus careless about protecting it. According to Kaushik (2019), posting personal information on social media is discouraged in a news article reported in *The Cape Times*. A representative from SABRIC (2018) endorsed this report, stating that banking clients should exercise extreme caution when sharing personal information as criminals are continuously inventing new ways to commit fraud. Furthermore, social engineering techniques are described as methods for exploiting victims by obtaining personal information such as passwords over the phone or by e-mail. The extent of the impact of cybercrime, according to the Global Economic Crime Survey (2016), includes reputational harm, legal and compliance costs, service interruption, theft or loss of personal information, regulatory costs, and actual financial loss. As the cyberspace sphere enables the transfer of information, the exposure of millions of people to data security breaches is a harsh reality.

2.5 Challenges in Policing Cybercrime

Cybercrime policing entails investigating, identifying, and preventing cybercrime. These tasks will be discussed below.

2.5.1 Investigating cybercrime

Investigations involving computers often fail as a result of errors made early in the process or when crucial digital evidence was ignored, damaged, corrupted, or improperly treated (Dlamini & Mbambo, 2019). Essentially, there should be no delays in reacting to the crime during a cybercrime investigation as delays compromise the investigation's efficacy, rendering the information useless in efforts to apprehend the cybercriminal. As mentioned by Dlamini and Mbambo (2019), responders to cyberattacks have previously been unable to act quickly

because they feared they would not provide enough proof or fair justification to prosecute a crime. Also, the presumption exists that “an intrusion may be triggered accidentally by the perpetrator when looking around a computer system without the purpose of compromising the organization's data” (United Nations Office on Drugs and Crime, 2013:17).

2.5.2 Detecting cybercrime

Cybercrime is a problem that many businesses face. According to Kader and Minnaar (2015:69), "organisations have taken to launching their own counter-attacks and, even though this can be construed to be in self-defence, it could be illegal in the eyes of the law or even labelled as an illicit act of cyber vigilantism". This type of counter-attacking seems to be becoming more common as a way for large multinational corporations and organisations to detect and prevent data breaches (Dlamini & Mbambo, 2019). It is used to secure company records and ensure that confidential client information is not fraudulently obtained by cybercriminals. The establishment of a stronger cooperative policing policy by the police, the private sector, and the community is deemed necessary for an effective response to these acts.

2.5.3 Combating cybercrime

As security threats develop and diversify, businesses and organisations must upgrade their security strategies and reinforce their defences to aid in the launch of counter-attacks to fight cybercrime. Widsup, Spitter, Hylender, and Basset (2018) mention that regular cybercrime risk assessments can be conducted by a number of financial organisations and businesses − particularly those with sufficient financial resources − while advanced cybersecurity technologies, safe firewalls, digital evidence protection, content recognition, intrusion detection, cyber intelligence collection, cyber surveillance of all incoming online traffic, and network system monitoring can be implemented. Organisations that can afford to incorporate such security policies aid cybercrime experts in responding quickly to cybercrime. The majority of businesses and individuals believe they are not a priority worthy of cyber criminals’ attention. According to UNODC (2013), many government agencies face this issue because they lack the resources to implement these strategies. However, it remains a fact that, as a result of the lack of resources available to the public and private sectors, cybercrime is difficult to combat.

2.6 Cybercrime Legislation in South Africa

As demonstrated in the tabling of the Cybercrimes and Cybersecurity Bill (Sabinet Law, 2017) for comment at the National Assembly on 22 February 2017 (Republic of South Africa, 2016; Kilian, 2017), South African legislation was revised to tackle emerging cyberspace intimidation. It is said that South Africa is currently waiting for the new Bill to become law, which will then identify aspects such as defrauding an individual through fake websites (Kilian, 2017). However, South Africa has common law offences that are described in a body of laws that covers corruption by the falsification of invoices using computers. Similarly, regulation is also in force covering the electronic transfer of money. This is protected by the ECT Act that additionally deals with illegal access to information and data damage (Kilian, 2017). However, finding the location of the cybercriminal for an arrest and determining where and by whom a cybercrime was committed are not necessarily easy as cybercriminals bound their signal from country to country, making policing cybercrime in KwaZulu-Natal and South Africa very challenging.

Shinder (2011) points out that online crime offers a safe space for the prospective criminal. A cybercriminal can hide his or her identity as different services mask or hide the IP address, thus making it difficult to follow the criminal's trail (Ahmed, 2019). Even if the attacker might be identified, digital evidence may be hard to prove. Consequently, the successful prosecution of a cybercriminal is challenging. Using the example of child pornography, Shinder (2011) states that it is not easy to ascertain or confirm whether an internet user was personally aware of accessing illicit content because someone else may have broken into the network and stored data without the original computer user's knowledge or consent if the device was not properly protected.

Likewise, as noted by Von Solmes (2015), although the number of data protection laws in South Africa has increased, these laws need to be thoroughly investigated once enforced to assess their effectiveness. The African Union adopted the African Union Convention on Cyber Security and Personal Data Protection (African Union, 2018; Von Solmes, 2015). However, the Bill has clear drawbacks as some experts have expressed the opinion that it leaves unanswered some important questions, such as whether South Africa has cyber experts who will be able to effectively enforce the Bill (Du Toit, Hadebe, & Mphatheni, 2018). Von Solmes (2015) argues that, as cyber-capacity skills are global, South Africa is not familiar with these

scarce skills yet. Von Solmes (2015) states that, for South Africa to effectively and expertly enforce the Bill, a huge number of individuals must be trained to acquire the necessary skills. From the standpoint of the banking industry, banks must make sure that their digital security systems are strong enough to deter intrusion both internally and externally to limit the risk of cybercrime. This mandates the banking industry to continually upskill its engineers and cyber/IT specialists. On the other hand, the SAPS is required to keep abreast of sophisticated and continuously evolving threats posed by cybercriminals, thus law enforcement and cyber experts in the law enforcement field must be regularly upskilled to combat the most recent trends and tactics used by cybercriminals.

Von Solmes (2015:n.p.) states that, to transfer and acquire these skills, "there needs [*sic*] to be political will and financial resources". Therefore, the Bill will look good on paper but without the requisite skills it will not yield the desired results. Another challenge, according to Von Solmes (2015:n.p.), is "the decentralisation of cyber-related responsibilities to a number of government departments, which in all probability will create a silo-based approach to cyber governance". This, in fact, will eventually contribute to job ineffectiveness and repetition. Von Solmes (2015) therefore proposes combining some of the various configurations in the Bill, if not all of them, so that limited functional assets can be used more efficiently. The National Cybersecurity Centre, mandated by the National Cybersecurity Policy Framework and passed by the South African Cabinet in March 2012, was launched in 2015 as a key element in building awareness of cybersecurity as well as promoting the exchange of knowledge and technology that will ensure that South African business and personal internet users remain secure online (Du Toit, Hadebe, & Mphatheni, 2018).

2.6.1 The position of common law

Cybercrime is distinct from crimes that are committed with the use of a physical medium, hence the laws that guide the use of a physical medium are challenged when electronic media are used (Watney, 2012). This means that, in certain cases, regulations governing violent crimes cannot be applied to crimes committed by electronic means (Watney, 2012), as cybercrime does not require a physical component for its commission. Online offenses have no bounds and cannot be confined within a country's national boundaries (Watney, 2012). According to Njotini (2016), the South African criminal law is in the fortunate position of still having and evolving a common law system. This system can reasonably be expected to adapt quite easily

to new phenomena due to its reliance on versatile and adaptable general concepts rather than a multiplicity of rigid laws. However, whether or not South African common law has effectively adapted to the arrival of the computer is a contentious issue. For instance, as some types of theft are now dealt with by statute, Van Der Merwe (2016) asserts that the fundamental common law crime of theft exists and must be enforced even in cases of computer-based theft.

One thing that has changed, with reference to Section 35 of the Constitution, is that the definitional spectrum of such crimes can no longer be easily extended. This is due to the legality principle, *nullum crimen sine lege*, which has been enshrined in South Africa's Constitution as an inalienable civil right. Prior to the passage of the ECT Act in South Africa, both common and criminal laws of the time were broadened to allow for the arrest and active prosecution of certain online criminals (Schultz, 2017). When it comes to cybercrimes, however, the common law's applicability has certain limits and is narrowed considerably (Snail, 2009). The South African Law Commission (SALC) worked in two stages to resolve the shortcomings of common and statutory law. The first stage considered whether unauthorised access to computers and unauthorised alteration of computer data and software applications could be adequately dealt with under South African common law and, if not, the second stage considered whether new legislation was needed (Schultz, 2017). The SALC determined that courts would be reluctant to extend current common law offenses and concluded that legislation was necessary (Van Der Merwe, 2008). A number of South African scholars looked into the adaptability of common law in South Africa and found a legal loophole in the area of computer crimes and related fields (Sulfab, 2014). They questioned whether legislation would be required to effectively address the issue. Prior to 2002, it was clear that legislation was woefully inadequate to cope with the rapid advancement of information technology (Sulfab, 2014).

2.6.2 Criminalising cybercrime in the Electronic Communications and Transactions (ECT) Act

After years of legal ambiguity, Parliament passed the Electronic Communications and Transactions Act (ECT) in 2002 (Republic of South Africa, 2002). Chapter XIII is devoted to cybercrime and brings legal clarity to what constitutes and does not constitute cybercrime (Snail, 2009). However, it is important to note that Section 3 of the ECT Act (the interpretation clause) does not preclude the application of any statutory or common law from understanding or accommodating electronic transactions. In other words, when applicable, the common law

or other laws remain in effect and binding, resulting in the application of such laws where the ECT Act does not make explicit arrangements for criminal sanctions. Section 85 describes cybercrime as the behaviour of an individual who, after taking notice of data, realizes that he or she is not supposed to access that data but proceeds to do so anyway (Gereda, 2006). Therefore, an individual who knowingly accesses or intercepts any data without authority or consent is guilty of an offence, according to Section 86(1) of the Interception and Monitoring Prohibition Act No. 127 of 1992 (Republic of South Africa, 1992).

The Court held that a screen printout was inadmissible under the Civil Procedure and Evidence Act No. 25 of 1965 (Republic of South Africa, 1965) in the case *Narlis v. South African Bank of Athens* (1976 (2) SA 573 (A)) (Snail, 2009). It was apparent that the legislation governing the value of electronic data in legal proceedings needed to be amended as soon as possible. As a result, the Computer Evidence Act No. 57 of 1983 (Republic of South Africa, 1983) was enacted, but unfortunately prematurely. An authentication affidavit was needed to authenticate a machine printout under Section 142 of the said Act. The Computer Evidence Act seemed to be more geared toward civil cases than criminal cases. It raised significant concerns and fell short of the mark when it came to complementing existing laws and expanding universal standards (Kufa, 2008). Cybercrime is not restricted to the activities mentioned in the ECT Act, and there are also other statutes that may be used to prosecute cybercriminals (Snail, 2009). The prevention of all cybercrimes mentioned is highlighted under the Prevention of Organized Crime Act (PoCA) No. 121 of 1998 (Republic of South Africa, 1998) and the Financial Intelligence Centre Act (FICA) No. 38 of 2001 (Republic of South Africa, 2001), but in a more organised fashion. Money laundering and other financial crimes are also regulated by the latter Act, as these crimes are increasingly being committed online and may also be in violation of exchange control regulations.

2.6.3 The Protection of Personal Information Act No. 4 of 2013

In South Africa, cybercrime has had, and continues to have, a major impact on companies, which has a knock-on effect on individuals. According to Pillay (2016), between 70 and 80% of South Africans have been victims of cybercrime at some point in their lives. As a result, the state passed its first piece of legislation aimed at protecting personal information in the Protection of Personal Information Act No. 4 of 2013 (commonly known as the PoPI Act) (Republic of South Africa, 2013). This Act, which took a long time to develop, incorporates

best practices from around the world. By enacting minimum information security provisions, the PoPI Act aims to protect and safeguard personal information by regulating how it is treated, retained, secured, and destroyed. In essence, the Act mandates the protection of records, including the collection and application of data pertaining to identifiable natural or social persons. As a result, under the PoPI Act individuals have the right to contest such applications on practical grounds and to request that their data be removed (Opland & Moodley, 2013).

According to Anderson (2015), personal information includes, but is not limited to, contact information, demographic information, biography, biometric information, personal opinions of and about an individual, and private communications such as e-mail or text messages. Prior to this, any information minimum requirements were only used as a general guideline rather than being made mandatory (Pillay, 2016). Cybercriminals and social engineers may need access to personal information to carry out an illegal activity, so laws like the PoPI Act may help to reduce cybercrime. Notably, the PoPI Act gives effect to Section 14 of the South African Constitution (Republic of South Africa, 1996), which guarantees citizens' right to privacy. This right to privacy includes the right to confidentiality, which means that personal information must be protected from unauthorized collection, possession, dissemination, and use (Republic of South Africa, 2013).

The Personal Information Act (PoPI Act) protects citizens against harm such as emotional distress, time loss, and information change as a result of data breaches (Opland & Moodley, 2013; Republic of South Africa, 2013). It should be noted, however, that the true scope of cybercrime under this Act is not determined, giving individuals and businesses a false sense of security. The fundamental weaknesses in the Cybercrime and Cybersecurity Bill, on the other hand, are clearly evident. Van Rensburg (2017) argues that the Bill should be split into two different pieces of legislation; the first should concentrate on cybercrime while the second should focus solely on cybersecurity and the digital vulnerabilities and inadequacies of cyberspace. Furthermore, the current Bill does not discuss the technological aspects of cybercrime, cyberattacks, and hacking vulnerabilities in any depth.

2.7 Inadequacy of South Africa's Cybersecurity Initiatives

Despite the time and effort put into designing the policy structure that governs cybersecurity, the implementation process is still not complete (Grobler & van Vuuren, 2007). According to

Gwala (2016), this failure can be attributed to a variety of reasons, the majority being administrative in nature. This gap often results in a lack of sufficient resources to carry out policy implementation effectively. The National Cybersecurity Policy Framework (NCPF) stated that the computer security incident response team (CSIRT) and community security emergency response team (CSERT) would be established by the end of March 2012; however, due to a lack of political will, this did not occur and adjustments were not mandated, and thus the mandate was handed over to the Department of Telecommunications and Postal Services, which was equally inefficient (Grobler & Bryk, 2010). Later, the State Security Agency was granted this mandate. As a consequence of this mandate being sent from pillar to post, there was a time lag between policy formulation and policy implementation, and some of the NCPF's proposed policies have actually not been implemented as planned.

Another issue that South Africa is grappling with is the absence of effective legislation for apprehending and prosecuting cybercriminals. According to Cassim (2015), police authorities cannot prosecute such criminals unless countries have sufficient laws in place that outlaw any such illegal activity. Clearly, South African cybercrime laws are enacted with lofty ideals but they are failing because law enforcement officers lack a thorough understanding of cybersecurity and the various laws that apply to this crime form (Gwala, 2016).

Moreover, South Africa has adopted the European Convention on Cybercrime (CECC) but has yet to ratify it. Linked to this is the fact that cybercriminals are actually subjected to lax law enforcement and punishment. Many revised criminal codes demand insufficient sentences, and this fact offers little deterrent for crimes with large-scale economic and social implications (McConnell International, 2000). This is exacerbated by the fact that there are no successful mechanisms in place to prosecute a cybercriminal. These criminals thus commit cybercrime knowing that they will face only minimal or no punishment at all, which is a phenomenon known as immunity. Because of the complex nature of cybercrime, policymakers' cybersecurity policies are often obsolete, leaving them unable to keep up with the ever-changing cybercrime landscape. This point is emphasised by Pieterse (Mashiloane, 2015), who believes that rapid technological developments and computer manipulation will continue to intensify, and that this will result in an increase in cybercrime threats and incidences. As a result, cybercriminals are becoming more sophisticated as they produce new malicious software and devise new ways of infecting computers and networks.

Cybersecurity is also hampered by a lack of knowledge, especially among government agencies. At this point, understanding these threats and how to reduce them does not appear to be spreading as rapidly as the escalation in the use of cyber-technology (Goredema, 2012). South African government officials are exposed to cyberspace on a daily basis, but they are unfamiliar with such applications and are thus ignorant of the risks they face and the numerous counter measures currently in place. As a result, these users often unintentionally disclose confidential information that is used by adversaries who then commit cybercrime with impunity.

Although the consequences of cybercrime and all cyber-related threats have been widely recorded around the world, there is currently very little research available in South Africa, especially research that is based on the government sector. This is emphasised by Herselman and Warren (2010:256), who state that "research is needed to determine how badly (if at all) South African businesses are affected by cybercrime and whether the newly promulgated laws will help in the prevention of and enhance the prosecution of these crimes". Clearly, there is often a lack of cybersecurity awareness among officials and the public alike. A lack of capacity among stakeholders charged with implementing cybersecurity policies is also a dire threat. For instance, collaboration across national boundaries to investigate and prosecute crimes is complex and sluggish, and this is exacerbated by an inefficient law enforcement system that is complicated by the transnational existence and diversity of cybercrime (McConnell International, 2000).

Cybercriminals are well aware of this flaw. They often defy the traditional jurisdictional realms of sovereign nations and launch attacks from almost any device on the planet while crossing numerous national borders, or they launch attacks that appear to come from international sources (McConnell International, 2000). The technological and legal challenges of detecting and prosecuting cybercrime are significantly enhanced by such techniques. Another issue is that performing a cyber-related investigation frequently necessitates a considerable amount of conventional forensic work as well as highly specialised skills, which are often lacking in a country like South Africa (Mashiloane, 2015). There are very few organisations available to train such investigators so the service is often procured from foreign firms, but this is prohibitively costly for the country and, as a result, there is little quality (Allen, 2021).

2.8 Conclusion

It is apparent from the literature review that cybercrime will continue to pose an almost insurmountable threat to financial industries and that the problem will only get worse due to how rapidly digital technology is developing. The financial services industry is undoubtedly the foundation of the economy, which is a fact that highlights the urgency to address this issue. The literature review demonstrated that cybercriminals' ability to conceal their identities, which are typically removed from the real world, further reinforces the complexity of cybercrime. The capacity of cybercriminals to preserve their anonymity through disguise in cyberspace makes it difficult for law enforcement agencies to trace the offenders, and this makes it easy for fraudulent individuals to engage in cybercrime operations and to target the financial and banking industries. A case in point is that the percentage of suspected digital fraud attempts originating from South Africa in the financial services sector increased by 187% over the final four months of 2020.

The literature clearly shows that cybercrime is growing rapidly in South Africa due to public unawareness and a lack of appropriate legal frameworks to address it at both national and regional levels. Therefore, despite the fact that laws are being passed in South Africa to curb cybercriminals, they are ineffective because law enforcement officers are not well-versed in cybersecurity and the many applicable laws contained in diverse Acts. Therefore, international collaboration and general uniformity are necessary given the borderless nature of the internet and the difficulties posed by jurisdictional issues. It is thus crucial that governments learn from one other's attempts to combat cybercrime. The international nature and diversity of cyberspace make it difficult for an effective law enforcement system to investigate and punish crimes across national boundaries, as these processes are slow-moving and complex. It is important to note that implementing successful preventive strategies across all target groups is crucial for effectively combating the problem of cybercrime. Therefore, education and training need to be ongoing to enhance users' knowledge and to motivate them to incorporate preventive measures when utilising the internet and any device linked to cyberspace. The next chapter reflects on the theoretical framework based on where the study was located.

CHAPTER THREE
THEORETICAL FRAMEWORK

3.1 Introduction

A theoretical structure is necessary to underpin any research project because these theories help to explain the study's research problem and its underlying concepts. To understand crime and deviance and to devise suitable crime prevention efforts, various theories have been developed in the Criminology field. Essentially, the application of a theory (or theories) creates a better understanding of the reasons why and how offences are committed. According to Tibbetts & Hemmens (2009:12), a theory can be defined as "a set of concepts linked together by a series of statements to explain why an event or phenomenon occurs". The theories that will be clarified in this chapter frame phenomenon of cybercrime in financial industries, which was the central theme of this study.

For a cybercriminal to engage in cybercrime activities that target a financial industry, there must be motive, and the primary motivation is undoubtedly financial gain. To explain this in more depth, theories were employed to support our understanding of cybercrime in the social context of financial entities. The study was guided by three theories, namely the rational choice theory of Beccaria (1765, cited in Acheson, 2002), the routine activity theory (Cohen & Felson, 1979), and the space transition theory (Jaishankar, 2008). To summarise:

- The routine activity theory (commonly referred to as RAT) examines crime as a series of events. As indicated by Kodellas, Fisher, and Wilcox (2015), crime is a product of the confluence of time and space involving the potential criminal (in this study the cybercriminal), a suitable target (i.e., the financial industry), and the absence of capable guardians (i.e., the lack of technical, formal, and informal controls to prevent cybercrime).
- The rational choice theory, according to Acheson (2002), contends that individuals are motivated by selfish desires and they seek to maximise their gains and therefore their own interests. This is relevant to cybercrime as potential offenders are motivated by personal financial rewards.
- The space transition theory (Jaishankar, 2008) describes and understands the causes of crime as well as the types of behaviour that exist in both cyberspace and the in the

physical world. It thus describes and explains the role of conforming and non-conforming behaviours. For instance, this theory contends that, because of the anonymity of a perpetrator who is connected online, potential offenders will participate in cybercrime with impunity.

The theoretical framing that was selected was important as it elicited understanding from a theoretical point of view how and why cybercrime is perpetrated. It is noteworthy that the banking industry is a primary target for cybercriminals as the financial sector is driven by money, while it is also fraught with flaws that allow data to be relatively easily accessible. Therefore, the selected theories will serve to explain the cybercrime phenomenon in the financial industry in general.

3.2 The routine activity theory

The routine activity theory (RAT) was developed by Cohen and Felson (1979). This theory is based on the notion that a crime is not committed randomly but that three integral conditions exist for crime commission: a suitable target, the absence of a capable guardian, and a likely or motivated offender (Figure 3.1). According to RAT, victimisation is largely explained by the potential victim's suitability as a target for a motivated criminal. This means that a person or organisation is a suitable target based on availability and they appealing to the perpetrator (Cohen & Felson, 1979). Therefore, to avoid victimisation, a guardian's required. Guardianship thus refers to the capacity of people and other targets to prevent a crime from being committed, and it can manifest in both social and physical ways (Cohen & Felson, 1979). A motivated offender is therefore someone who is ready and prepared to commit a crime when the opportunity arises due to the existence of a suitable target and the absence of a guardian.

According to Leukfeldt and Yar (2016), the routine activity theory has been well established in the analysis of a variety of criminal behaviours. For instance, it was a crucial theoretical approach in Criminology in the late 1970s and has since been utilised to predict street and other forms of crime. More recently, it has been modified to explain and understand cybercrime (Kigerl, 2012) as it has important implications for crime control policy that aims to curb internet fraud. "RAT can be viewed as a situational crime theory i.e. a criminal-friendly situation/setting where offenders choose to commit crime based on their perceptions of available opportunities" Govender, Watson & Amra, 2021: 4). This theory is thus relevant in

determining how and why crimes are committed in the spatial domain of cyberspace compared to that of conventional crimes, as it is premised on the routine cyberspace activities of an individual which invite possible attack. So, when individuals operate online but are not technologically savvy, they are very likely to become the victims of cybercriminals.

With reference to the three components referred to above, Cohen and Felson (1979) state that they create a premise for the commission of most crimes. They propose that, in the absence of these three conditions, most crimes will not be committed as it is spatial and temporal convergence that opens the door for a criminal. This theory underpins cybercrime which can be related to the virtual nature of the internet and computer systems that are used for the commission of this crime. Kodellas, Fisher, and Wilcox (2015) argue that, by virtue of the routine activities that individuals perform, they expose themselves to potential offenders who then plan their attack. Obeng-Adjei (2017) mentions that the applicability of this theory to online activities may be moot as cybercrime generally occurs in the absence of the victim, however, it is contended that vicinity does not play a major factor when it relates to cybercrime activity, due to the fact that routine activities of the victim places him/her at risk of victimisation. It is this nature of the crime that the routine activity theory addresses and that makes it applicable to cybercrime in financial industries.

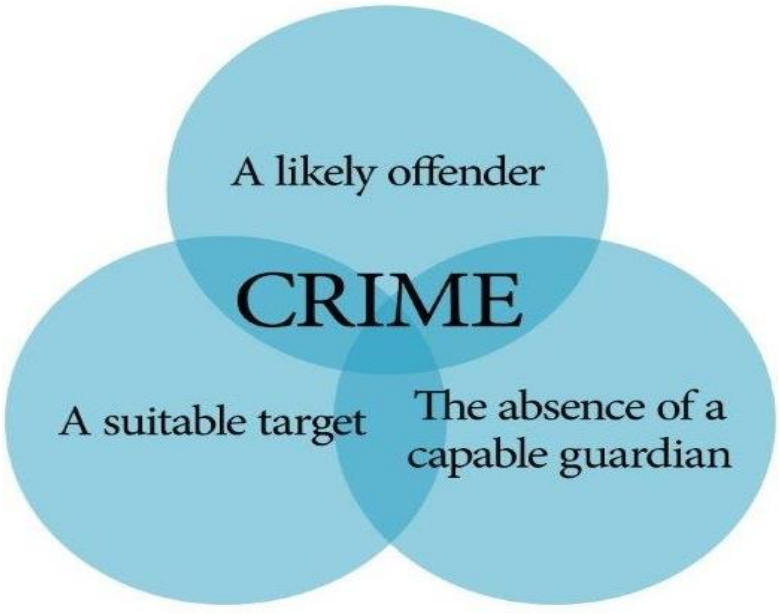

Figure 3.1: Components of the routine activity theory

Source: Adapted Cohen and Felson (1979) and Criminology theories (2022)

3.2.1 A motivated offender

Cohen and Felson (1979) state that motivated offenders have both criminal intention and a capacity to carry out that intention if they meet in space and time with unguarded targets. Leukfeldt and Yar (2016) indicate that, with reference to motivated offenders, there is no short supply of such people in the online environment which is fraught with numerous fraudsters, hackers, pirates, and so forth. Hinduja and Patchin (2001) state that the use of high-speed computers makes it possible for an individual to be exposed to online attacks, as a result of the speeds in which remote users can download, and have malicious software install on computer systems. As indicated by Cornish and Clarke (2014), the affinity of a person to commit a crime is frequently exacerbated by positive experiences after some time. Such a person is driven by decisions, experience, and the inclination to commit a crime, and this could lead to a high recurrence of the crime of choice. The rational choice theory indicates that potential offenders perform risk assessments prior to them executing an attack.

3.2.2 A suitable target

Leukfeldt and Yar (2016) argue that various targets are suitable for the theft of predation-proprietary data, personal information, online payment, and purchasing services. Moreover, computer systems themselves might be undermined and disrupted by unapproved interruption and interference. The utilisation of computer systems presents inherent risk exposure which may emerge as various threats. Cohen and Felson (1979) mention that a suitable target that is the object of an attack may be a computer system, an individual, or a property. Research has indicated that, when a crime occurs in real time and space, it essentially happens because perpetrators estimate the wealth of an area and then assumes the value of items in each individual household (Coupe & Blake, 2006). Conversely, all users of the internet are subject to an attack despite their geographical location, age, gender, race, and economic and social standing (Newman & Clarke, 2003). Cohen and Felson (1979) suggest that value, visibility, and access are characteristics of a target and that suitability is the result of a combination of these qualities. With regards to value, the potential offender may relate the value or perceived value to the target based on the surroundings where it is located. The relative weight of the target for theft also plays a role in rendering the target suitable for an attack in that it makes removal possible. Likewise, what is visible is more likely to appeal to a potential offender for a possible attack than an abstract or imaginary target, and the ease with which the target is

accessible is a contributing factor for the suitability of that target. In terms of cyberattacks, visibility on the internet is a primary factor, whereas the weight and size of the targeted loot are immaterial as the transfer occurs immediately and invisibly in cyberspace.

3.2.3 The absence of a capable guardian

Cohen and Felson (1979: 4) define guardianship as "the capacity to keep the perpetrator from causing malicious harm or injury to an individual or object". For this reason, there is a similarity between safeguarding a home and safeguarding a computer system (or smartphone) against malicious attacks. Grabosky and Smith (2001) indicate that offenders rather target a household with no physical security such as locks and burglar guards than houses with some visible physical security. In the same way, cybercrime occurs because of the absence of physical measures such as antivirus software (Grabosky & Smith, 2001). Another type of guardianship that has been investigated is social guardianship, for example the presence of some form of control or the perceived presence of an object/person with the innate capability of warding off the offender (Coupe & Blake, 2006). Leukfeldt and Yar (2016) point out that, in the cyberspace context, a capable guardian may take numerous forms, including network administrators, forum moderators, users, as well as an array of automated protection measures such as firewalls, virtual private networks, and anti-virus and anti-intrusion software. ID authentication and access management systems may also serve as capable guardians.

Databases that contain personal information such as names, addresses, passwords, and different banking information have become the focus of cybercriminals who exhibit the traits that Clarke (1999) refers to as CRAVED. The length of time spent online, an increase in Internet banking, and online transactions are all behaviours that have become highly likely to be targeted by cyber offenders (Kigerl, 2012). Therefore, to lower the contextual and situational opportunities for cyber criminals, this theory can be applied to inform policy that will prevent such crimes in the future instead of focusing on rehabilitating or isolating the offender. This means that the goal of policies informed by this theory is to alter society as a whole so that there are fewer opportunities for the commission of cybercrimes (Wickert, 2020). According to RAT, a crucial element for minimising victimization is to enhance the impact of capable guardianship (Leukfeldt & Yar, 2016), as the likelihood of offences being committed depends critically on whether a guardian is present or absent when potential offenders and desirable targets meet at a precise moment in time and space.

To shed light on the causative mechanisms that underpin both cybercrime in general and the many forms of offense-specific online cybercrimes, the researcher employed RAT as an appropriate theoretical framework. Moreover, as fraudulent access to cyberspace information is a major threat, using this model to describe cyberspace and Internet crimes could prevent victimization (Newman & Clarke, 2013). This choice was based on the notion that, even though internet cyberattacks have been studied in depth, the prevention of such crimes could be improved by learning more about the manner in which particular victims are targeted.

3.3 The rational choice theory

Cesare Beccaria introduced the rational choice theory in the 18th century, and it has evolved to underpin wide areas in Criminology such as situational crime prevention, the routine activity theory, deterrence, and crime analysis (Wright, 2009). According to the rational choice theory of Criminology, humans are reasoning individuals who weigh the benefits, disadvantages, and costs before making the decision to commit a crime. The basis of the rational choice theory is behaviour, which includes the decision to commit a crime with the knowledge or premeditation that the potential rewards will outweigh the risks (Bond, 2015).

The rational choice theory was initially developed by economists, while Criminology studies adopted it in the late 1970s. The rational choice theory in criminology and the notion of deterrence both originated in the classical school of Criminology and are based on Cesare Beccaria's utilitarian philosophy (Bond, 2015). The concept of the calculus of pleasure, sometimes referred to as the ‘hedonistic calculus’, is discussed by Jeremy Bentham using the classical school of Criminology and the utilitarian theoretical framework (Bond, 2015). According to the hedonistic calculation, people will make crime commission decisions based on how much pleasure the crime might evoke against how painful the punishment might be. The rational choice theory has a long history but is essentially credited to the philosopher Adam Smith as its creator. Sociologists George Homans, Peter Blau, and James Coleman advanced the rational choice theory in relation to social exchange in the 1950s and 1960s, moving from economics to the social sciences (*Introduction to Rational Choice Theory*, 2022). These social theorists claimed that a rational analysis of the exchange between costs and rewards determines social behaviour, and in particular criminality.

For this study, the rational choice theory was of fundamental importance. The tenets of this theory regarding human behaviour are useful in the study of Criminology (Wright, 2009). The reason for using the rational choice theory in this study was that it attempts to identify and explain the social phenomenon of cybercrime and explains how perpetrators are driven by cost and effect. The theory indicates that a crime will be committed when the offender has weighed the possible benefits and losses of his actions. In the case of cybercrime, financial industries are attacked due to their large number of customers; the benefits are thus much higher than when a single target is attacked.

Wright (2009) suggests that the fundamental features of the rational choice theory are human desires, values, and constraints. The expectations associated with the commission of a crime include the potential criminal's positive or negative perceptions of the consequence that can result from any planned attack. Thus the value derived from an attack will be considered rationally to determine the cause-effect relationship that will translate into the perceived benefit of perpetrating a certain crime. The limitations will thus also be considered rationally. Accordingly, Bransen (2001) argues that the rational choice theory stipulates the moral actions that are acceptable for achieving specific goals, given the limitations imposed by a certain situation.

Acheson (2002) argues that the rational choice theory is predicated on the tenet that human beings are motivated by selfish interests when they make choices, and that the goal is to maximize their rewards. It applied to this study because cybercriminals are driven by their ego, which becomes bigger and bigger as they achieve success upon success (Bocij, 2004). In addition, the rational choice theory posits that selfish, opportunistic acts lead individuals to violate laws only if their aims are achieved. This holds true for cyber attackers who breach a plethora of laws while attempting to achieve their goal of causing their victims financial loss, pain, and humiliation. In addition, the rational choice theory is based on the idea that human beings do certain things to maximise their advantage. Such criminals are greedy, egocentric, and brutal (Siegel, 2011). Bransen (2001) argues that the purpose of the rational choice theory is to understand and forecast human behaviour when criminals break the law for their own selfish purpose and without regard for the harm and pain they cause. This theory is thus applicable to the economic sector where individuals and companies, that try to maximise their income with marginal losses, are targeted by ruthless, faceless cybercriminals who behave in a manner that suits their own nefarious interests (Ahmed, 2019).

The rational choice theory assumes that there are many individuals who could commit crimes but, depending on the circumstances, many potential offenders will not actually commit a crime as, based on a process of rationalisation, they conclude that the disadvantages will outweigh the advantages. However, if the advantages outweigh the disadvantages, they will make the rational decision to go ahead and commit the crime (Criminology Web, 2022). Essentially, the commission of a crime is based on how and when an opportunity presents itself.

However, regardless of its high rate of applicability to criminal studies, the rational choice theory is frequently criticized. For instance, although the theory is founded on the notion of bounded rationality rather than pure rationality, critics argue that aspects like emotion and impulsivity are not given enough consideration in this theory (Criminology Web, 2022). These critics contend that irrational considerations sometimes motivate a criminal act such as in a crime of a crime of passion. This means that, although the rational choice theory recognizes the importance of personal characteristics, it does not consider impulsive action and a particular disposition that erupt impulsively in the commission of a crime.

Despite these objections, the rational choice theory is and will continue to be crucial in Criminology and criminological theory because it emphasizes a feature of crime that many other theories overlook, namely the situation. Some criminologists even contend that the rational choice theory serves as an effective framework for incorporating other theories of crime as those other theories can shed light on the background conditions that restrict free will, while the rational choice theory concentrates on the choices criminals make (Criminology Web, 2022). In summation, the rational choice theory differs from many other criminological theories in that it does not concentrate on the reasons why criminals commit crimes, but focuses on how opportunities affect crime and how offenders decide to commit crime.

3.4 The space transition theory

The space transition theory was developed by Jaishankar (2008). According to the space transition theory, people behave differently as they transition between different types of spaces (Jaishankar, 2008). Therefore, based on the advent of crimes in cyberspace, the space transition theory was advanced by Jaishankar (2008) who describes how and why cyberspace crimes are caused, arguing that the escalation of cyberspace crimes has become the new centre of criminal activity globally. Ahmed (2019) states that the theory attempts to clarify the causes of crime

and the essence of criminal actions that occur in cyberspace and that are related to conforming and non-conforming behaviour. Jaishankar (2008) argues that the theory of space transition describes the actions of individuals who exert conforming and non-conforming behaviour in their real, physical space and in cyberspace.

This theory has gained widespread interest in the Criminology field since its inception in 2008. Today it is a theory that is widely cited in cyber Criminology. Jaishankar (2008) states that the introduction of the theory of space transition introduced a modern definition of cybercrime that has helped to improve comprehension of this crime and how it can be tackled. The theory of space transition was promoted when no other scientist could describe the cybercrime phenomenon as a whole. This theory was first presented as a chapter in a Prentice Hall book titled "Crimes of the Internet" (Schmalleger & Pittaro, 2008). Since then, a number of empirical studies have been conducted to evaluate the usefulness of this theory, and several academics have praised Jaishankar's insights on combating cybercrimes.

In a bid to explain the research topic, the space transition theory was deemed suitable. The reason for utilising the space transition theory was that cybercriminals believe that, due to their anonymity on online platforms, they feel free to commit their planned offence. It can be argued that these individuals, who drift in cyberspace, do not act out impulsively but in a well-planned manner to disrupt, take, and damage data and to steal large sums of money. This theory was thus deemed relevant to cybercrime and its impact on financial industries, particular South African banks.

The theory's first premise is that an individual with repressed criminal behavioural tendencies might be more likely to commit a devious act in cyberspace than in a real, physical space because of the need to maintain the status quo and their place in society. Jaishankar (2008:6) borrows his premise from Arbak's (2005:5) model of crime and social standing to justify that:

- "Individuals feel varying degrees of self-reproach when they engage in criminal activity.
- They are generally concerned with their social status in society based on others' perception of their values.
- In making their decision, they calculate the social and material risks of being a criminal against the comfort of living as a law-abiding citizen".

The space transition theory's second premise is that versatility of identification, dissociative anonymity, and a lack of a deterrent factor prompt these people to commit a cybercrime. Jaishankar (2008) opines that anonymity often leads individuals to behave unpleasantly, such as committing a criminal offence in cyberspace. Suler (2005) stipulates that, while individuals are under the veil of anonymity, they are motivated to commit acts of crime which they believe are not going to be traced back to them. Conversely, one of the main factors that encourage most members of society to conduct themselves in an honest/non-violent manner is the fear of being caught, which is a powerful deterrent. However, this deterrent is increasingly absent in cyberspace which contributes to cybercrime.

The third premise in the space transition theory is that, if an offender in the physical space engages in activities that are criminal in nature, then he/she will most likely be committed to behave in a criminal manner in cyberspace as well. This is evident when offenders begin to boast of their actions online and in the physical world (Jaishankar, 2008). For example, most cybercriminals worked individually when preparing and conducting cybercrime in the early 2000s, but there has been a rise in organisations and conspirators that use cyberspace to make money. This notion is supported by the fact that cyberspace promotes and conceals cybercriminals' illegal activities. Today, the simplicity and ease with which cybercriminals move money from one account to another make it very challenging and difficult for law enforcement agencies to track these criminal gangs' financial transactions.

However, various scholars have criticized the theory for being difficult to test and being specific to only certain types of cybercrime. This is because gathering information on cybercrime perpetrators is a difficult task that makes it challenging to test the space transition theory (Holt, Bossler & Spellar, 2015; Holt & Bossler, 2016). Kethineni, Cao and Dodge (2017:13-14) state that, "although the case studies provide some support for space transition theory, more data is [sic] needed to test all of the propositions empirically". Currently, it is challenging to identify a sizable population of cyber offenders, but this problem might be resolved in the future. What is clear, however, is that cybercrimes will increase in the future and the barrier between offline and online offenders will become increasingly blurred. This may see the advent of an increasing population of cybercriminals which will render the application of the space transition theory much more realistic than it is at the moment (Jaishankar, 2018).

3.5 Conclusion

It is clear that cybercrime will remain a major threat to financial institutions. As digital technology advances, the challenges associated with such crimes will become more complicated. According to the routine activity theory, there are certain aspects of information that are available online, and this renders the financial and banking industries suitable targets. The rational choice theory posits that financial crimes are driven by cost and rewards, and the cybercriminal thus regards financial industries as fertile ground for their perceived reward which will be much higher than when a single individual is targeted. Moreover, the space transition theory suggests that cybercriminals believe that, due to their anonymity on online platforms, they feel free to commit an offence as they can infiltrate the infrastructure of the banking industry with impunity. The following chapter discusses research methodology and the methods utilised to conduct this study.

CHAPTER FOUR
RESEARCH METHODOLOGY AND METHODS

4.1 Introduction

In the field of Criminology, as in the Criminal Justice System (CJS), sound and verified information is critical. According to Higgins (2009), research facilitates the discovery of new information or the replication of prior findings. The latter author further asserts that research is scientific as it employs precise methods that can be replicated by other researchers to obtain the same results. Moreover, in the field of Criminology and Criminal Justice, there are three main research approaches that provide this scientific logic, namely the quantitative, qualitative, and mixed-method designs. In the current study, it was critical to select the appropriate research design and methodology to meet the study's aims and objectives.

A research methodology is a collection of ways for conducting research and reaching conclusions about the study topic. According to Neuman (2003), research methodology is a tool that transforms social research into scientific information; hence it is critical in making decisions about the research processes that should be used. This chapter will demonstrate how the researcher utilised a qualitative approach to meet the aims and objectives of the study. According to Maxfield and Babbie (2008), every research project requires a well-defined research design that outlines how data will be collected and analysed. This is covered in more detail in section 4.4 below.

The benefit of social science research is that it provides contextualised and accurate interpretations of the topic being examined by employing a variety of methods that systematically develop new social discoveries (Bhattacherje, 2012; Bachman & Schutt, 2011). The study's objectives and research questions were met by obtaining data gathered from SAPS officials. The non-probability sampling method was employed and the participants were recruited by means of purposive sampling. Purposive sampling entails selecting cases that are representative of the population under study (Terre Blanche and Painter, 2006). This sampling technique was used to ensure that knowledgeable SAPS officials were recruited to address the objectives of the study. Any research methodology should promote the validity and reliability of the results through the methods that are utilised to collect the data (Crow and Semmens, 2008). Data were thus collected by interviewing SAPS officials and detectives and access was

granted by the SAPS National and Provincial offices. The researcher assured the participants that the data would be used for academic purposes only and that the information they provided would be untraceable to them as individuals. To analyse the data, the six phases of thematic analysis as proposed by Braun and Clarke (2006) were applied. All ethical considerations were adhered to, as will be explained in further detail.

4.2 Research Paradigm

Bryman and Bell (2011) describe a paradigm as the entire collection of beliefs, values, and techniques that are shared in a given setting or a community. One approach to employing research methods for data collection and analysis is known as qualitative. According to Maree and Van Der Westhuizen (2013), in qualitative research it is assumed that the world is comprised of individuals who have their own beliefs, purpose, approach, principles, and way of understanding reality.

Because of its interpretive nature, the qualitative paradigm was chosen for this study. In order to analyse the data and write up the conclusions, the researcher used this paradigm to discover and exploit themes that emerged from the data. The implementation of this paradigm also enhanced the research quality by providing insight into the causes of cybercrime in the banking industry. The researcher considered cybercrime detectives key instruments in this study as they were vital participants in identifying and understanding the underlying causes of this crime.

The research utilised SAPS participants who were recruited from police stations and detective units in the eThekwini Metropolitan area in KwaZulu-Natal. The qualitative approach elicited in-depth understanding of the factors that contribute to cybercrime in South African banks as perceived through the lens of SAPS detectives. This study was context-specific and restricted to SAPS participants. It was conducted using primary sources (SAPS officials) of various ranks, ranging from lieutenant colonel to a captain and detectives. These participants possessed detailed and valuable information of cybercrime in financial institutions. Checking the primary data with those collected from secondary sources strengthened the legitimacy of the results and confirmed the interviewees' trustworthiness. The data collection tool was semi-structured interviews which were utilised as the primary form of data collection. Due to the code of ethics, the researcher will not disclose the names of the police stations and detective units that were

visited. The SAPS stressed that the researcher should conduct the research without any disruption to the duties of its members and this requirement was adhered to.

4.3 Research Methodology

Francis (2011:121) defines qualitative research as "an investigation to analyse, identify, track, and examine the attitudes, motivations, and behaviours of individuals". The researcher was interested in understanding the magnitude of cybercrime in financial institutions and not in the quantity of cases or in other numerical statistics. The researcher therefore engaged in face-to-face interviews with the research participants to optimise the value of the data that were obtained and to expand on the essence of people's understanding and perceptions of cybercrime. All COVID-19 protocols were adhered to when conducting the interviews.

This study aimed to explore the occurrence of cybercrime in the banking industry in Durban and to determine why these banks were vulnerable to cyberattacks from the perspective of SAPS officials who worked with incidences of this crime almost on a daily basis. It sought to establish the current nature of cybercrime that targets banks and to explore the reasons why the banking industry is continuously under attacked by cybercriminals. In brief, the study implemented a qualitative inquiry to investigate cybercrime using research participants employed by the SAPS. It is thus acknowledged that the study was limited to a law enforcement perspective as no bank employees were involved.

4.4 Research Design

Kumar (2005:95) defines research design as "the approaches that can be used to resolve research questions". A successful study design provides a clear description of the proposed procedures with such specificity that the same steps can easily be followed by another researcher. In selecting the research design, the researcher was cognisant of the fact that, while there had been extensive research on cybercrime, little was known about cybercrime in the banking industry from the perspective of SAPS officials who investigated this crime on a regular basis. It was thus deemed appropriate to adopt an exploratory research design as it is embedded within the qualitative approach. This design was used as it assisted in providing a thorough description of the investigation of cybercrime in the banking industry from the perspective of SAPS officials. Creswell (2014:158) suggests that an exploratory research

design is useful in exploring "…the occurrence of certain phenomena and predict future happenings". When this design is used, the researcher is able to understand and describe the relationship between dependent and independent variables that area associated with a research problem (Ahmed, 2019).

The reason for utilising the exploratory research design was that it could be applied to the research topic. For example, this design helped the researcher understand the causes and impact of the increased rate of cybercrime in the banking industry from a law enforcement perspective. The participants' ranks ranged from lieutenant colonel to a captain and detectives. The rationale for choosing these participants was that they were responsible for investigating cybercrime and would be able to provide valid, accurate, and current information. They investigated cybercrime on a regular basis, were able to identify the common mechanisms that cybercriminals use to perpetrate cybercrime, and they interacted with the banking industry when these crimes occurred. The research design was thus appropriate as it assisted in eliciting detailed data on cybercrime from SAPS officials' point of view.

4.5 Study Area

A field investigation into human ecology aims to collect and relate data on many aspects of a geographical region and its population, such as natural resources, history, language, institutions, or cultural economic traits (Dictionary.com, 2021). This is referred to as a study area. The current study was conducted in Durban which is located in the province of KwaZulu-Natal, South Africa. KwaZulu-Natal has the second largest population of the South African provinces with an estimate of 11,3 million people (Statistics South Africa, 2019). For practical reasons, the study was limited to the involvement of SAPS officials. The exact location or names of the police stations where the participants were recruited will not be disclosed for ethical reasons. Suffice it to state that the researcher visited four police stations/detective units in total. These are all located in the west, south, outer west, and inland areas of Durban and all fall under the eThekwini Metropolitan Municipality in KwaZulu-Natal.

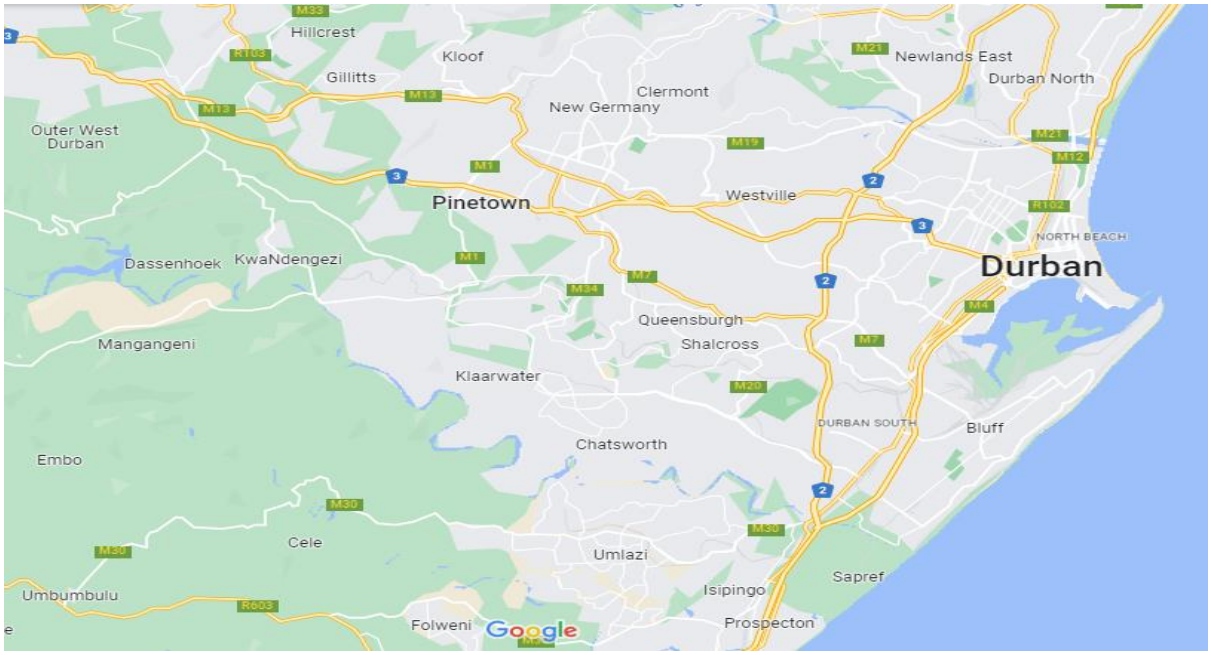

Figure 4.1: Map of Durban, KwaZulu-Natal

Source: Google Maps (2022)

4.6 Target Population

Blankenship (2010:82) defines a population as "a certain group of individuals, organisations, or artefacts that will be selected to participate in a research [study]". A target population comprises of an actual group or set to whom discoveries may be generalizable. In this study, the researcher's target population was SAPS officials in Durban, KwaZulu-Natal. Due to financial, time, and demographic constraints, the entire population could not be included in the study only thus 10 participants were selected. The researcher obtained data from these detectives and investigators as they were experienced in investigating cybercrime in the banking industry in the KZN area.

Before conducting the field research, the researcher was required to request permission from the National Office of the SAPS to conduct the study under its auspices and to involve its officers. The study proposal was perused by SAPS National Office according to the National Instruction 1 of 2006. This Instruction governs any application to undertake research involving the SAPS. The goal of this Instruction is to manage requests to conduct research involving the SAPS from people outside the Service or from individuals who want to conduct research for private reasons (such as post-graduate studies). The researcher adhered to the provisions in

sections 1-6 of this document and all other instructions while also signing the submission of indemnity and declaration documents (SAPS, 2006).

Final approval to conduct the study was obtained from the Office of the Provincial Commissioner of the SAPS in KwaZulu-Natal. The researcher conducted the study without any disruptions of the duties of the SAPS members involved. All participation was voluntary and the identities of the officers who provided the information were (and will be) treated as strictly confidential. It was also accepted that the nature of some information might be serious and that the participants would be within their right not to answer some questions or provide sensitive information. Both the Provincial Commissioner of the SAPS in KwaZulu-Natal and the National Office in Pretoria approved the study (see gatekeeper permission letter and South African Police Service approval letter).

The University of KwaZulu-Natal Humanities and Social Sciences Research Ethics Committee also granted approval to conduct the study (Protocol no. HSSREC/00002537/2021). Any changes or alterations made to the study had to be acknowledged and approved by this committee.

4.7 Sampling and Sampling Techniques

Sampling is the method of choosing a portion of the population that conforms to a designated set of specifications. According to Strydom (2009:195), "there is no rule for sample size in qualitative inquiry. The sample size depends on what needs to be known, the purpose of the inquiry, what is at stake, what is useful, what provides case credibility, and what can be done with the available time and research". For the purpose of this study and within the paradigm of non-probability sampling, the researcher utilised purposive sampling. According to Maxfield and Babbie (2008), purposive sampling is suitable for choosing a sample on the basis of one's understanding of the population, its elements, and the research aims, which are based on one's judgment and the purpose of the study. The reason for utilising purposive sampling was that there could be no random selection as the participants needed to be knowledgeable about the topic under investigation and the researcher needed to concentrate on issues that were of interest to the population (Steyn, 2013).

A sample of ten selected SAPS officials was therefore recruited. The gender distribution was one woman and nine men, but as gendered interpretations and views were not considered, this distinction had no impact on the data that were collected. Rather, participants who were well informed and would provide information-rich data due to their first-hand experiences of cybercrime were recruited as they would be well able to answer the interview questions (Alpaslan, 2010). The reason for utilising these participants was that they were able to provide rich, accurate, and contemporary data. As cybercrime occurs through online media, the banking industry is imminently at risk of cyberattacks, therefore the participants were SAPS officials who regularly investigated cybercrime.

4.8 Data Collection Method

The data collection method is a way of obtaining useful information to establish factual findings. A qualitative interview, according to Kvale and Brinkmann (2015), is a useful method that assists the researcher to understand the world from the perspective of the participants who have first-hand experiences as well as insightful knowledge based on the topic. The researcher utilised the semi-structured interview technique because it allowed the compilation of a large database of information about cybercrime in the banking industry. A semi-structured interview is a purposeful conversation that goes beyond the exchange of ideas in everyday conversation and becomes a careful questioning and listening method with the goal of gaining previously tested knowledge (Kvale & Brinkmann, 2015). It was envisaged that the utilisation of interviews would allowed the emergence of new themes that might not have been addressed in previous research. Interviews would also be valuable as they would allow the participants to freely discuss their insights and experiences. The semi-structured interview approach had a number of advantages, such as the fact that it provided an open-ended technique that allowed the participants to share their knowledge of cybercrime in the banking industry, and it elicited their personal thoughts and insight about their first-hand encounters with this crime.

An interview schedule containing open-ended questions guided the interviews. These questions aimed to fill the gap in cybercrime information due to the paucity of data on the impact of cybercrime on financial institutions in the study area. The questions thus focused on the SAPS officers' understanding of the causes of the escalation of cybercrime in the banking industry, and on their insight into policies and strategies (or the lack thereof) that should guide the implementation of effective measures to curb cybercrime in the banking industry.

The value of using semi-structured interviews in qualitative research is that each participating individual may be prompted to expand on their views, which could result in further inquiry and more in-depth data. Probing is crucial because it can reveal new themes that do not occur in the literature or that the researcher has not considered (Rubin & Rubin, 2012). Open-ended questions allow participants to share their views descriptively without the restriction of categories. They also prompt a vast array of answers that depict richness and self-expression. When compared to an indirect approach such as a telephone interview or survey that is confined to yes or no or limited responses, open-ended questions determine a person's genuine response and insight. They elicit thorough knowledge, which is why interviews are so beneficial in qualitative studies.

The interview schedule that was used kept the interview on track as the questions were pre-planned and guided the range of responses. These face-to-face interviews were conducted in the study area in locations that were safe and convenient. The duration of the interviews ranged from 20 to 30 minutes each, depending on how much information the participants were willing to share. The data collection was done over a period of five weeks between March and April 2022. The data that were gathered during the face-to-face interviews were recorded using both a voice recorder and handwritten notes, and the material was transcribed for data analysis. While conducting the interviews, the researcher ensured that all COVID-19 protocols were adhered to according to risk adjusted level 1, the requirements of the Human and Social Sciences Research Ethics Committee, and guidelines issued by the University of KwaZulu-Natal.

4.9 Thematic Data Analysis

Glass (2004) defines data analysis as a practice according to which raw data are ordered and organised so that useful information can be extracted. According to Creswell (2009), qualitative procedures require various steps for data analysis. The goal of qualitative data analysis is to interpret the data to reveal deep knowledge and understanding. In this process, the researcher must become a part of the environment and be aware of what is going on (Kvale & Brinkmann, 2015). It is critical that the researcher comprehends and revisits the data that were obtained on a regular basis. The researcher must be emotionally intelligent and be able to set aside his or her own opinions, emotions, impressions, or any notion for the information to be successful and valuable.

Because this process in qualitative research is circular rather than linear, there is no separation between the phases of data collection and data processing (Kvale & Brinkmann, 2015). The circular method of analysis allows the researcher to return to the divergent phases of the research. For example, if the first set of interviews has been completed and analysis is underway, the researcher may identify common themes, and can then return to the data collection phase to ensure that the common theme is supported by the participants' views. Data are constantly sorted and grouped during the analysis process to uncover common themes across all the responses. In qualitative research, the goal of data collection is to gain a detailed description of sensible and relevant information; hence it is critical to recognise relevant data.

Thematic analysis is used to identify, analyse, and report patterns (or themes) that emerge from the data and to group them to highlight emerging themes (Braun & Clarke, 2006). By applying the thematic analysis method, the researcher utilised the six phases of thematic analysis as proposed by Braun and Clarke (2006) to avoid prescriptive, linear, and inflexible rules.

Becoming familiar with the data

Firstly the transcribing of the data must take place and thereafter reading (and re-reading) the transcripts, as well as listening to the recordings. This allows the researcher to thoroughly and actively engage with the data, as proposed by Braun and Clarke (2006). The researcher ensured that she had a thorough comprehension of the data and was well-versed in all parts by reading the transcripts and listening to the audio-recorded interviews several times to become familiar with the content and ensure reliability in decoding the information garnered from the audio recordings and the handwritten notes.

Generating initial codes

After becoming familiar with the data, the researcher began the process of discovering preliminary codes, which were aspects of data that appeared to be interesting and relevant. These codes are generally more numerous and specific than themes, yet they help to identify the context of the various conversations that were conducted (Braun and Clarke, 2006). In this second stage of data analysis, the researcher was able to identify critical components and themes that were appropriate in resolving the problem, questions, and objectives of the study. The essential information that emerged from the participants' data were reviewed to determine both similarities and contradictions, and the significance of these findings in addressing the objectives of the study was determined.

Searching for themes

Interpretive analysis of collected codes begins in the process of searching for themes. Data extracts (combined or divided) can be sorted using broad themes. As discussed by (Braun and Clarke, 2006), the relationship that exist between codes, themes, as well as subthemes should be indicated in the researcher's cognitive process. The researcher thus went over the study questions again to see what the most important emerging themes were. Common denominators and differences inside and across the material were identified during the third stage, and these common denominators and disparities generated themes. The information was organised into themes, while non-applicable themes were deleted and relevant themes were matched with findings revealed in the literature review.

Reviewing themes

The next step was to consider whether to merge, improve, separate, or eliminate basic themes through a more thorough analysis. The data inside themes should make sense together, yet there should be obvious and distinct contrasts between them. This is normally done in two stages: first, the themes must be checked in connection to the coded extracts (phase 1), and then the entire data set must be checked (phase 2) (Braun and Clarke, 2006). This stage can lead to the creation of a thematic map. In many cases, the researcher has a set of themes that he or she forecasts, but after analysing the data, other themes emerge. The current researcher thus analysed the themes according to the steps as set out in stage four to ensure that they were coherent and that they matched the coded information.

Defining and naming themes

This entailed refining and identifying themes and potential subthemes that emerged from the data (Braun and Clarke, 2006. The researcher named the themes and provided precise working definitions that concisely and succinctly represented the core of each theme. The researcher established the most relevant themes in the fifth step.

Producing the report

By employing vivid and captivating extract examples that linked to the themes, research questions, and the literature, the researcher translated her analysis into an interpretable piece of writing, as proposed by Braun and Clarke (2006). The analysis results were relayed in such a way that the reader will be convinced of the value and validity of the findings. The researcher double-checked all interpretations to ensure that the data were presented as logical arguments

rather than as a mere list of discovered themes (Braun and Clarke, 2006). This was one of the most crucial stages of the data analysis process as the researcher had to ensure that the study objectives were addressed. The researcher provided a thorough and accurate description of the participants' viewpoints in line to the research questions, whereby the responses of the participants were quoted throughout the process of writing.

4.10 Methods to Ensure Trustworthiness

According to Barnes, Kroll, Burke, Lee, Jones and Stein (2000), in a qualitative study it is necessary that the researcher addresses the conformability and transferability of data. If this is achieved, it demonstrates that the researcher has broken through barriers and completely comprehends the various facets of the social context under investigation (Bashir, Afzal & Azeem, 2008). In qualitative research, the researcher must play an important role in ensuring that the study is trustworthy, authentic, and credible. In order to fulfil these requirements, the researcher was objective, attentive, and able to establish rapport not only with the participants, but also with other members of the study's social milieu (Kawulich, 2005). This approach ensures objectivity in the researcher's presentation of the data and findings, as proposed by Neuman (2014). To make sure that this approach would be trustworthy, Lincoln and Guba's (1999) model of trustworthiness was applied. The four constructs of dependability, transferability, credibility, and confirmability were addressed as proposed by this model as follows:

4.10.1 Dependability

According to Maxwell and Babbie (2015) and Adams, Khan, Raeside and White (2007), dependability addresses the requirement that the research's findings be stable and consistent enough to persuade the reader or evaluator that they were discovered in a sequential and ethical manner. De Wet and Erasmus (2005) argue that research is reliable when its methods are transparent, advanced, and peer-reviewed, while Trochim and Donnelley (in Kumar, 2011) state that dependability has to do with whether a researcher might obtain the same results from two separate examinations on a similar topic. In the current study, the researcher thus ensured that both literature data and data analysis findings are accurately and unambiguously stated to address the requirement for dependability. The responses of the research participants who were interviewed were accurately transcribed and the researcher took care to avoid changing the data

to support a particular argument. Moreover, the participants were not influenced in any way by the researcher during the interview process and their responses were transcribed and reported verbatim. The researcher also exercised extreme caution not to draw any conclusions or offer any advice that might have changed the participants' points of view. Because of these rigorous measures, the researcher is certain that identical results will be produced if a similar study is carried out by a different researcher.

4.10.2 Transferability

Transferability is the extent to which the findings of a qualitative study are transferable to different contexts or groups involving different participants (Korstjens & Moser, 2018). According to Schurink, Fouché and De Vos (in De Vos, Delport, Fouché & Strydom, 2011), it must be conceivable to apply the findings of a study to different contexts. Based on the choice of research methodology and the manner in which it was applied, the researcher can state unequivocally that the data, the insights gained from the research participants, and the findings will be transferable to similar groups of individuals, subjects, and contexts. This is because the researcher provides a thorough explanation of the assessment area, the participants, and the data collection techniques in this study report which will allow future researchers to assess whether or not the study's findings might be applied to other contexts with comparable study problems. In summation, it is anticipated that the same outcomes will be attained if a different researcher uses the same research design and methodology and subjects the findings of this study to comparable circumstances.

4.10.3 Credibility

De Vos et al. (2011:419) state that credibility is "the alternative to internal validity in which the goal is to demonstrate that the inquiry was conducted in such a manner as to ensure that the subject was accurately identified and described". The use of appropriate tools for data collection in the current study affirms that the research was authentic because interviewing and observation are often used as qualitative research methodologies. The researcher spent a significant amount of time with the study participants in their respective natural environments (i.e., SAPS police stations and detective units) in order to get to understand them, establish rapport with them, gain their trust, and minimise any information distortions that might have resulted from the researcher's presence in the field. This approach increased the credibility of

the study. Field notes were taken and interview data were recorded and transcribed verbatim using a voice recorder, which are processes that validate the analysis of data outside the field in the absence of the participants.

4.10.4 Confirmability

Trochim and Donnelley (in Kumar, 2011:185) state that confirmability is "the degree to which the results could be confirmed or corroborated by others". This means that, for results of different studies to be compared, the researchers should have adhered to exactly the same processes (Kumar, 2011:185). To attain confirmability, the researcher thus ensured that the responses by the research participants were supported by accurate and thorough comparisons with the literature that had been reviewed. Confirmability was also achieved by thorough explanations of the data collection and analysis procedures. This means that other researchers will be able to examine the research design and, after close perusal of the gathered data, reach similar findings. This is also achievable as the researcher focused on maintaining objectivity throughout the investigation, which means that the results will be the same if the study were to be carried out by another researcher in a manner comparable to the current one.

4.11 Limitations of the Study

The study initially focused on interviewing officials from a specific bank. The researcher was initially informed that she would be allowed to conduct research on cybercrime in this particular bank, but this permission was later retracted as all banking information is private and confidential. The researcher then contacted SABRIC as it publishes annual reports regarding cybercrime. A meeting was scheduled with an individual of the cybercrime division of SABRIC. She was advised that interviews would not be allowed, but that they would support any desktop research. However, after internal discussion this support was also retracted. The researcher then shifted her focus to SAPS officials dealing with cybercrime in the banking industry. Much time had been lost but relevant gatekeepers' letters were finally obtained from the SAPS, as was explained earlier.

Some financial constraints were experienced as no funding for the study had been obtained. The researcher acknowledges that this study was limited to Durban, KwaZulu-Natal in terms of its geographical delimitation. This impacted the generalisation of the study's findings.

Due to the busy schedules and the nature of the day-to-day activities of SAPS officials, the availability of detectives was often a challenge. Because the participants were interviewed at their workplace, their availability was difficult to manage.

It was also a challenge to identify detectives/investigators that were responsible for investigating cybercrime in KwaZulu-Natal as such people seemed to be very scarce. However, none of these challenges hindered the researcher from completing the study and meeting its objectives.

4.12 Ethical Considerations

Babbie and Mouton (2001) indicate that ethics is the practice of compliance with the standards of conduct of a given profession. Wahidin and Moore (2011) refer to ethical practice as the empirical science of humans' behavioural morality. This is realistic as it guides how humans act and behave. Ethics is a science because it is a set of coherent and systematic ideas that describe human morality and rationalise it. Bezuidenhout (2011) postulates that ethical behaviour is adherence to moral principles and behavioural norms. In scientific studies, researchers adhere to such ethics when communicating with others in order to avoid harm. In this research study, the following ethical considerations were adhered to:

4.12.1 Informed consent

As proposed by Barlow and Durand (2009:116), the researcher presented all relevant information about the study to assist the study participants in their decision to participate or not. The participants' informed consent was obtained only once the researcher had given full disclosure of all the relevant aspects of the study to them (Wassenaar, 2006). The information given to the participants was clear and in an understandable language. The study's purpose and methodology were clearly stipulated (Henning, van Rensburg, & Smit, 2004).

Before beginning the research study, the researcher had to formulate a consent letter which was attached to the application to the Ethics Committee. Before each interview, the participant signed this consent form and the declaration. The consent form stated that the participant's identity would be kept private, that the participant could withdraw from the study at any time,

and that there would be no remuneration for participating or not participating as the research would be used solely for academic purposes. The researcher ensured the participants that they would be granted confidentiality and they were told that the study fulfilled all the ethical criteria as compiled by the researcher and stipulated by the University of KwaZulu-Natal.

4.12.2 Voluntary participation

Babbie (2008) states that no participant should be forced at any point to take part in a research study. All the participants were therefore made aware of their individual right to choose whether or not they would like to participate, as was also stipulated as a condition by the SAPS. Sensitive information or the seriousness of cases could have result in some respondents' refusal to answer certain questions, and the researcher respected this right.

4.12.3 Confidentiality, anonymity and privacy

Confidentiality is fundamental in ensuring the accuracy of a criminological study. Jones (2012) states that criminal justice research frequently requires individuals to divulge information that is applicable to criminality and subversive action, and the source must remain unidentified. For this reason, researchers are morally compelled to safeguard their information so that it may not be exploited in contradiction to participants' rights in legal procedures (Jonas, 2012). According to Mugenda (2011), anonymity means not mentioning the ethnic and cultural setting of participants and refraining from addressing them by their names or disclosing any other sensitive information concerning them. The researcher thus assured that the identity of the person providing the information would be safeguarded at all times. The names of the research participants and the different police stations are thus not divulged.

Akaranga and Makau (2016) state that if any information has to be exposed, then permission must be sought from the relevant participant. According to Akaranga and Makau (2016), this increases honesty and the research subject is safeguarded from bodily or psychological harm. The researcher thus did not ask questions that would put blame on anyone or upset the participants in any way. This study had no intention of accusing any role-players of cybercrime, but merely sought to investigate the phenomenon by exploring its nature and the legal protective measures the banking industry employs, as mentioned in the literature and by legal experts.

4.12.4 COVID-19 protocols

Conducting research in the midst of the COVID-19 pandemic involved adaption while maintaining the quality of the research. The researcher adhered to South Africa's COVID-19 risk adjusted level 1, the Human and Social Sciences Research Ethics Committee, and guidelines of the University of KwaZulu-Natal. Social distancing (a 1.5-meter distance between the researcher and study participant), mask wearing, and hand sanitisation before and after the interview were maintained at all times.

4.13 Conclusion

This chapter outlined the methodology that the researcher employed to successfully complete the investigation and write the dissertation. As qualitative research is circular in nature, the researcher constantly re-evaluated sections of the research in order to obtain the best results. The research paradigm, the research methodology, and the research design were explained in detail. This chapter also included a description of the research area in which the study was conducted, while the sampling procedure was discussed in detail. The data collection and analysis methods were also explained with reference to scientific guidelines for qualitative study. The study's limitations were listed and the ethical considerations that had to be adhered to were presented. The interpretation and analysis of data will be discussed in the next chapter.

CHAPTER FIVE
DATA PRESENTATION AND INTERPRETATION OF FINDINGS

5.1 Introduction

In this chapter the data that were gathered from the participants by means of interviews are presented and interpreted with reference to findings in the literature. The conclusions generated from the data are also presented. The data are discussed in two sections. In the first section, the data that were obtained during the data collection phase are examined and the results are interpreted. In the second section, the data are interpreted as themes to address the study's goal and objectives.

5.2 Section one

In the first section the data are presented and analysed. The participants' words are reported in italics. To adhere to ethical guidelines, the participants are identified by code. The questions that were posed by the researcher during the interviews for this particular component of data presentation and interpretation are presented in italics. The responses of the participants were recorded using a voice recorder as well as handwritten notes and are coded as follows: R = researcher, P = participant, and P1 – P10 = individual participants.

5.2.1 Sequence of the Presentation of the Qualitative Data

The data were analysed using the emerging themes and sub-themes as a guide. A number of themes emerged that were connected to the causes of cybercrime, cybercrime legislation, and policies on how South African banks might reduce cybercrime. The analysis connected each of the following concepts to the research objectives as follows:

- Theme A: The causes of the increased rate of cybercrime in banks - Objective 1. (*What are the causes of the increased rate of cybercrime in banks?*)
- Theme B: Cybercrime legislation that guides the financial industry in South Africa - Objective 2. (*What cybercrime legislations have the government implemented to support financial industries in South Africa?*)

- Theme C: Policies that guide the implementation of cybercrime countermeasures in the banking industry - Objective 3. (*Are policies that guide countermeasures against cybercrime effective in the banking industry?*)

5.2.2 Objective 1: Establish the causes of the increased rate of cybercrime in banks

*5.2.2.1 Question 1: What is the general understanding of cybercrime as a phenomenon in the banking industry***?**

It was evident that the SAPS officials had a fairly similar understanding of cybercrime as a phenomenon in the banking industry. However, where P1 and P2 held a similar view the rest of the participants had a different view. Moreover, P7, P8, P9, and P10 shared the understanding that banks are aware of the threat of cybercrime:

> *"Yes, the banking industry is very much aware of cybercrime that takes place" (P7).*
> *"Yes, the banking industry is aware of cybercrime" (P8).*
> *"Yes, the banking institution is more up-to-date than we think" (P9).*
> *"I am sure the banks are aware of cybercrime. I am very sure that they are aware of what is going on" (P10).*

The responses presented above confirmed that banking institutions are aware that cybercriminals target banks. P6 stated:

> *"Yes, there is definitely an understanding of cybercrime from the banking industry. Fortunately, with me I have a direct link which has been created with all the financial institutions. Like, if I have a problem with a bank account, and we do something called a Section 205, it is a subpoena to the bank, informing them that this account is a fraudulent account, there has been activity, and please give all the information related to the bank account. Other than me going down to the bank branch and serving them with a subpoena, I have a direct linkage, I can email it directly to FNB, ABSA, Standard Bank, whoever, they will receive it and within a few days, they will forward us the information"*

Participant 6 shared the views of those cited above, but expanded by mentioning "a Section 205". This section appears in the Criminal Procedure Act that guides access to personal information. As indicated by Giles (2009), a police official can issue a subpoena requiring the

Internet service provider (ISP) to provide the requested information under Section 205 of this Act, in which case the ISP must cooperate and provide the information. Section 205 is used when an SAPS official requires personal and privileged information of individuals. Participant 6 had a direct link to the banking industry which other SAPS officials probably did not have.

Conversely, two participants questioned banks' awareness of cybercrime:

> *"There are just so many misunderstandings from the banks' perspective which actually occur on a regular basis. Banks are not adjusting accordingly. It is hard to say how aware the banks are of cybercrime as there are just so many loopholes within financial institutions" (P1).*

> *"It is difficult to say because information from banks is compromised when data sheets from the banks have been leaked. [So] the banks are leaking out information; their information is not safe or secure. Therefore, it is difficult to say how aware they are of cybercrime" (P2).*

In contrast to the earlier comments, Participant 1 and Participant 2 felt that banks were not keeping abreast of the cybercrime threat due to so many other issues. These latter responses raised an intriguing point that was not mentioned by other participants, which is that banks tend to release sensitive information and then deny complicity. For instance, ABSA stated that only a small percentage of its South African clients had been affected when a data breach had occurred in November 2020 (Buthelezi, 2021). The bank reported that its impacted clients' identifying information, contact information, and transactional account numbers had been hacked as one of its employees had improperly made some customer data available to a third party. The bank said at the time that the leak had only affected a small percentage of its South African customers, but in April 2021 it admitted that the leak had harmed more people than previously indicated. The wide range of this impact confirms that cybercrime does not occur in a single geographical region but that it can be perpetrated across borders in an interconnected and multi-faceted way that involves a variety of role-players.

*5.2.2.2 Question 2: What types of cyber-related crimes are committed, who commit/s them, how do they happen, and when do these crimes occur***?**

In response to what types of cybercrime are committed by cybercriminals, most SAPS officials shared the following view as expressed by Participant 6:

> *"There are various cybercrimes such as credit card fraud and money being taken out of bank accounts (P6).*

The foregoing statement confirmed the view of Business Tech (2021) that account takeover (ACTO) fraud is an emerging trend that is continuing to afflict bank institutions around the world. ACTO fraud occurs when criminals get unauthorised access to account information in order to withdraw funds from a person's bank account or make fraudulent credit card charges. Other comments in this regard were:

> *"Cybercrime occurs frequently within the banking industry; there is a lot such as your banking apps and digital bank fraud" (P1).*
>
> *"There are so many crimes that take place, like SIM swops, email attacks or phishing, vishing, and more" (P2).*
>
> *"There are many types of cybercrimes, like phishing, vishing, hacking, and more" (P3).*

These responses confirm that digital fraud, such as hacking banking apps and online banking facilities, is prevalent. SABRIC argues that phishing, vishing (voice phishing), smishing (SMS phishing), and e-mail or corporate e-mail hacking are the most prevalent fraudulent crimes that affect the digital banking arena (Malinga, 2019). SABRIC also mentions that the banking industry has documented a few rare occurrences when malware was utilised to compromise a client's digital banking credentials.

Another participant stated:

> *"It is digital fraud, online fraud, and mobile banking fraud. All of the above, but cybercrime is more of an opportunistic crime" (P10).*

Participant 10's insight that cybercrime is an opportunistic crime suggests that it occurs as a result of banks' poor internal controls, processes, and systems that entice cybercrime activities.

Participant 8 stated:

> *"There are various crimes that take place−such as common online fraud which is the interception of emails−and they are becoming more common. Another is intercepting*

cell phone networks and [the criminals go] onto your banking app and transfer funds out of your account" (P8).

Based on the abovementioned responses, maintaining the security of online portals and protecting clients' data should be a top priority for the banking industry so that cybercrime exposure may be reduced.

Participant 9 stated the following:

"…all fraud-related crimes like digital bank fraud, and more. There is not a specific time when cybercrime takes place as it occurs at all times throughout the year. I believe that these crimes are performed by criminals who are foreign nationals" (P9).

"Cybercrime is not seasonal. This crime occurs all through the year from January to December…For example, I will make a comparison to house breaking which occurs most frequently in the month of December due to people going on vacation, and homes being vacated" (P7).

The rates of cybercrime are consistent from January to December, which is a trend that was noted across all the major banks in the study area. Collectively, the participants agreed that cybercriminals search for loopholes in online banking systems and take advantage of them.

5.2.2.3 Question 3: What are the most prevalent methods used by cybercriminals to perpetrate cybercrime?

The researcher posed the above question in an attempt to determine the mechanisms that cybercriminals employ to sustain cybercrime. The responses obtained from the participants were diverse. For instance:

"Now you get phone calls from people that tell you they are calling you from the bank, and the number that they will call you from you will think it is from the bank. You get cases when people will tell you the last three transactions, so once that person tells you that, the call becomes legitimised. They will send the OPT number, you will receive the OPT number, and before you know, monies have been taken out of your account. That is very common now. However, you get different trends that start emerging" (P6).

The above response refers to cybercriminals' ability to use a mechanism known as vishing. They pretend to be employees of a financial institution and try to persuade you to reveal your

personal and banking information over the phone. This finding highlights the danger that cybercrime activities are encouraged due to the lack of account holders' awareness that a reputable financial service company will never ask you to disclose any information over the phone or through other channels such as emails.

Participant 7 stated:

> *"Cybercriminals utilise fraudulent documents. The banking institution does not verify the documents, therefore there is unverified documentation" (P7).*

The above response suggests that a lack of security controls is a significant management flaw in terms of cybercrime attacks on banks and their clients. This means that these financial institutions' approach to preventing cybercrime is reactive rather than preventive, which is a key concern. Other comments highlighted computer-related fraud and the cloning of cards:

> *"Cybercrime is your computers, online fraud, cell phones and computers" (P8).*
>
> *"That would be computer fraud" (P9).*
>
> *"…scanning devices and cloning of cards. Also infiltrating people's bank accounts by hacking …" (P10).*
>
> *"There are a few common ones such as card cloning of your debit or credit cards, and unauthorised debit cards" (P1).*
>
> *"Cybercriminals skim your data, and will send you a website or a link which appears legitimate, and this is done by email, which is known as phishing. They will even call you and appear to be a bank official, and they will send you an OTP number as well" (P2).*

The threat of cybercrime ranges wide, which suggests that risk mitigation measures must be implemented as a matter of urgency. Banks' approach to this issue seems to be reactive and detective rather than preventative, which may be due to the dynamic nature of cybercrime and its rapid pace of innovation. Clearly, the banking industry requires key staff to be upskilled on a regular basis to keep abreast of ever-changing technology and innovation.

5.2.2.4 Question 4: What are banks' perspectives on the root cause of cybercriminal activities based on current trends in cybercrime?

When this question was posed, it was accepted that the participants could only surmise based on their experiences and observations as they were not bank employees or managers. What emerged, however, was the confirmation that the prevalence of cybercrime in the banking sector is widespread. Banks have been a target of cybercrime for a long time, and this trend is escalating because faceless, untraceable cybercriminals benefit hugely from their nefarious activities. This trend is explained by the routine activity theory which posits that routines, in this case the systemic procedures used in banks that are quite predictable, are closely monitored and breached at the right moment. Clients' naivety often opens the door. Better strategies to combat cybercrime must therefore be developed.

The SAPS officials were also asked what they thought banks' perspectives on the core causes of cybercrime were. The following are the key responses:

> *"The banking industry does not disclose this information to the SAPS or their banking clients, I believe this is why the banking industry is attacked. Banking institutions do not constantly keep up-to-date [with threats]. The banking industry [also] does not verify the information before releasing monies. The SAPS is not told about the account information of a suspicious account holder" (P1).*
>
> *"The banking industry is not willing to share this information with the SAPS. For example, if there is a suspicious activity, we are not informed about this. It is also shocking because at times there are large amounts of money that are withdrawn at tellers in a bank. Also, there are instances when money was deposited, and the bank has a 7-day clearance period in which the money will be cleared. However, when we do our investigations we are able to see that the money was cleared immediately" (P2).*

The SAPS officials highlighted the fact that the banking industry does not disclose sensitive information to the SAPS. However, the Cybercrimes Bill, the ECT Act, and the POPI Act affirm that all electronic communication service providers and financial institutions are expected to report cybercrime activities to the SAPS (see sections 24-30, 35, 45(3), 52, and 54 of the Cybercrimes Bill) (Republic of South Africa, 2017). This necessitates strong strategic partnerships and cooperation, as resources must be combined to devise mutually beneficial solutions to this problem. It is important that financial institutions evaluate their current strategies and devise new ones, as cybercrime is escalating. Moreover, to address these issues, collaborative initiatives are required to overcome the lack of communication regarding cybercrime policing in KwaZulu-Natal.

When asked how cybercriminals gain access to information, Participant 6 stated:

> *"Crime in the banking arena can vary. It is hard for the banks, no matter what expertise they have at their disposal, to keep track of it, because there are so many millions of people that hold bank accounts. It's thus difficult for the banks. They cannot keep track of each account holder" (P6).*

Despite the fact that banks' IT architecture and systems are strong enough to prevent cybercriminals from simply gaining access, these criminals use methods that do not require network access, such as illegally obtaining users' information by deception to gain access to their online profiles. This invalidates the IT networks of banks and their efficacy. Other participants stated:

> *"Cybercrime occurs because of banks' negligence. The initial steps from the bank are not verified as they only verify when payments have been made, and I believe that at this stage it is already too late. Also, the POPI Act is a contributing factor, as it does not allow the bank to look into the personal information of that particular individual and this restricts banks from investigating further" (P7).*
>
> *"The root cause of cybercrime is the lack of passwords and thus personal information is divulged. Also, with regards to internal fraud, staff members divulge confidential information to the suspects (cybercriminals)" (P8).*

The banking industry's strategy to address cybercrime seems to include regular evaluations of cybercrime alerts issued by their fraud detection systems, but because banks rely on the capacity of their fraud detection systems to issue these alerts, this method can be considered tactical rather than strategic. There is a need to change this strategy in light of escalating internal and external cybercrime activities. A review of banks' internal control mechanisms such passwords and the implementation of other measure to safeguard banking clients' personal information are thus priorities. Measures to reduce any identified risks must be put in place based on an analysis and the patterns that are established. In addition, legislation needs to be examined to provide financial institutions access to Home Affairs to check the personal information of account holders before proceeding with the opening of an account.

When asked why cybercriminals persist in their activities, some responses were the following:

"It is greed! I believe that these criminals are driven by greed whilst these offenses are committed" (P9).

"You can look at it as an opportunistic crime. They look for soft targets, just like all criminals out there look for soft targets. Not everybody gets affected by cybercrime but the people that do get affected by it, and you will see they were actually soft targets as they easily gave in to the criminals' questions to reveal their ID numbers and their banking information" (P10).

Cybercriminals perceive positive financial gain when they hack the banking industry in comparison with only a possible success rate if they target other businesses, and they conclude that cybercrime in this industry is decidedly safer and more profitable. This notion is directly related to the rational choice theory. The cost and benefit of cybercrime are weighed by cybercriminals whose obvious choice is the banking industry. Bank clients' lack of education and awareness might also be considered a significant root cause of cybercriminal activity, as people continue to click on anonymous links. Individuals in South Africa are vulnerable to internet fraud such as phishing and credit card cloning as they are often unaware of the risks connected with using these services. According to a recent survey, a large proportion of customers responded to fake emails, thus allowing their personal information to be fraudulently obtained.

5.2.3 Objective 2: To identify and examine cybercrime legislations that have been implemented for financial institutions in South Africa

5.2.3.1 Question 5: What is the conviction rate for cybercriminals?

This question was posed to explore the effectiveness of SAPS investigations of cybercriminal activity in the banking industry. The SAPS participants all agreed that the conviction rate of cybercriminals was low. With such a limited rate of conviction, the tendency to perpetrate cybercrime has escalated because few perpetrators of these crimes face penalties or legal retribution. The responses were as follows:

"It is very low. The other issue we have is that the banks allow people to use P.O. Box addresses or a letter from a local council which states that this person lives in this particular location. The bank will then open an account as the bank has a copy of an

ID and proof of address, and only when the police is trying to track the person down, then the banks will realise that this address is suspicious; and then we can travel the country and go right to wherever, only to realise that this place does not exist and the address is false" (P6).

As suggested by the above response, the banking industry must prioritise valid access and security at the outset in order to reduce the risk of cybercrime attacks. They must also ensure that their security procedures are robust enough to dissuade infiltration both internally and externally.

Other comments were:

"The conviction rates are very low, as criminals are untraceable. Also, SAPS resources are limited which makes it extremely difficult. The criminals are so advanced and have a 95% probability of getting away with the crime compared to the SAPS which only has 5% of resources" (P7).

"That is less than 40%, the problem being that you cannot identify the suspect. The suspect is behind the wall−behind the screens" (P8).

"The conviction rates are very low; however, statistics could say otherwise" (P9).

The above responses back up Kaushik's (2019) finding that cybercriminals are untraceable. According to Kaushik (2019), an increasing number of cybercriminals are shopping for software that allows them to stay anonymous while committing crimes on the dark web, which is an encrypted area of the internet that cannot be tracked. The dark web is a subset of the deep web, which is the non-indexed portion of the internet that is inaccessible to normal search engines like Google (Dutta, 2020). Furthermore, because the SAPS lacks information, experience, and personnel, policing cybercrime is difficult. However, dedicated SAPS officials have championed the subject and are working to gain greater resources and achieve higher success rates. It should be underlined that regulating cybercrime is the responsibility of everyone with internet access, and that the SAPS is doing their best with the limited resources at their disposal.

The following responses also highlighted the problems experienced in tracing cybercriminals:

"[Success] is minimal, when it comes to cybercrime, to locate the syndicate that is operating cybercrime. It is very difficult because if you are committing card fraud, you

have to find that swap card machine; that swap card machine is portable, you can move it from place to place. Then if you get cybercrime or fraud committed via the internet, you have to get the header address, you have to find out where it is, but these criminals bound their signal from country to country to country, and it is almost impossible to track cybercriminals. Their footprint is untraceable. Currently I have a case where an attorney received at email at 10 pm and the client had informed her that her banking details had changed and she EFTed money from her trust account into this new account, only to realise the next day that it was not a client from the bank. What the cybercriminals did was print the letter head and everything was like the client had done it, and the lady had lost R2,5 million. Truthfully, we in South Africa are way behind when it comes to cybercrime. Even our experts, our so-called computer experts and analysts, are way behind" (P10).

These findings suggest that end-users should be taught how to protect themselves from cyberattacks because cybercrime is continuously changing and cyber criminals are extremely proficient. As with any illegal activity, the most vulnerable are usually the first to be targeted. As a result, collaborating with cybersecurity and ICT security experts to identify needs and weaknesses will aid in cybercrime prevention. Banking clients are unable to protect themselves if they are unaware of security features, and necessitating user education on cybercrime could be a critical step. It is important to note that raising awareness is a common obligation for all of us as cybercrime affects everyone. We live in a society where we all rely on the internet to some extent. The SAPS, SABRIC, financial institutions, and government departments must collaborate to raise awareness of cybercrime so that people are aware of it or understand what it is.

Some reasons for the lack of cybercrime prosecutions were mentioned:

"There are very few convictions as there is a lack of cybercrime prosecutors in South Africa. Also, there is not adequate training for SAPS officials to thoroughly investigate cybercrime. We do not fully understand cybercrime and we do lack the knowledge– therefore it is very difficult. Cybercrime is very complex" (P1).

"The conviction rate is not high due to people's lack of knowledge and understanding of cybercrime" (P2).

Police officers lack the necessary skills to expose cybercriminals and access information as there is only a small number of police officers that have the requisite skills to investigate

cybercrime. Local police officers are inexperienced in dealing with this crime. The SAPS has only a few trained units, and officers in the lower ranks lack experience. More SAPS officials need to be trained in cybercrime prevention, investigation, prosecution/adjudication, and sentencing so that they can stay one step ahead of cyber criminals. In order to avoid being a victim of cybercrime, there is also a need to raise public knowledge about the dynamic character of this crime.

5.2.3.2 Question 6: Have there been any convictions for these crimes, and when were the perpetrators discovered?

The researcher posed a question about cybercrime convictions and when the perpetrators were discovered, in order to better address this issue in the future. According to the participants, although some arrests had been made, there had not been many convictions owing to the limited number of arrests and the lack of evidence to convict these criminals. Ryan Mer, the managing director of Eftsure Africa, which provides web-based payments and verification services, elaborated on this by saying that cybercrime is lucrative and can be perpetrated from anywhere in the world, with targets located anywhere (Maliba, 2021). Mer explained that, because of the "behind the screen" nature of this crime, apprehending and prosecuting these offenders is tough, which makes it appealing (Maliba, 2021). The following is what Participant 6 had to say:

> *"There are convictions, but generally to get to the source it is very challenging. People's bank accounts that are hacked are South African-based and they mostly live below the poverty line, and they rely on a few hundred rand from these syndicates. Like, in all of the dockets we have identified the account holders but these account holders are all over the country. They can be from any part of the country and when you find them and eventually when you do track them down, they will say 'Someone asked me if they could use my account', or 'Someone asked me if I could open a bank account and I went and opened the account and they gave me R500 to put in the account, they then took my bank card away'. This happens quite often and there we do not get prosecution because these individuals cannot lead us to the actual cybercriminal who asked them to do this. The prosecution you might get is a suspended sentence for allowing someone to use your bank account" (P6).*

The above participant highlighted two crucial point, which are that the bank accounts that are targeted are South African-based, and that the victims are often people who live below the

poverty line. Many rely on the few hundred rand that they receive from cybercriminals. It is evident that perpetrators who are recruited are external individuals and not only internal bank employees who divulge clients' information. This recruitment of ordinary folks who will commit a fraudulent act for a few hundred rand could be a result of South Africa's rising unemployment rates. Evidently, our legal system was designed to deal with physical crimes, and the expertise to successfully detect and prosecute internet-related crimes is unknown territory, which cybercriminals are aware of and use to their advantage.

Other methods that cybercriminals use were reportedly the following:

> *"The criminals change the picture of the ID, which makes it untraceable and difficult for detectives to investigate. Out of ten cases, there is only one successful conviction and this is usually a suspended sentence. It is very rare that such criminals are convicted and this is beyond the control of the SAPS. Also, criminal's use this to their advantage as they are aware of the low conviction rate and that is the reason cybercrime continues to increase" (P7).*

The Meta Compliance Marketing Team (2019) shares the same view as the one above, indicating that cybercriminals are aware of the low conviction rate and they exploit this to their advantage. Cybercrime is associated with fewer risks compared to other criminal activities, and cybercriminals have realised that, by leveraging technology for their own gain, they may generate more money with less risk of being detected and get smaller punishments if they are caught (Meta Compliance Marketing Team, 2019). We are witnessing organised criminal networks commit these crimes on an unprecedented scale in today's digitally linked society. These criminal gangs seem to operate without fear of retaliation because they can hide behind software that masks their identity. They exploit the anonymity of the internet to carry out their crimes. Participant 8 stated:

> *"The identification will usually take place within 2 to 3 months. Once the detectives have finished their investigation, we obtain all the necessary bank statements and question the recipient as how and why they have received these monies and possibly they can lead us to the main suspect" (P8).*

The SAPS seems to make every effort to identify the perpetrators of cybercrime through their investigations, but these criminals do not leave the same tangible evidence as traditional ones

and their crime can be conducted from afar, which adds to the difficulty of policing it. Some respondents stated:

> *"Yes, there have been a few convictions for these crimes. Only once the case comes back from court, then we are aware of the outcome" (P9).*
>
> *"There are minimal convictions for cybercrime and it happens randomly" (P10).*
>
> *"Very hard to say with regards to cybercrime convictions, as they are very low" (P1).*
>
> *"It is very rare, and from the investigation side, we are waiting for months to get information from the bank as they are not openly disclosing the information to the SAPS" (P2).*

The SAPS does not arrest all parties involved, which results in scattered evidence that is insufficient to support a successful conviction. This is due to a variety of factors, including banking clients who unknowingly disclose their personal information and banking details, cybercriminals acquiring innocent individuals to assist them in opening bank accounts, and cybercriminals having the resources and skills to bounce their signals from country to country. To address these issues, a collaborative connection between the commercial and public sectors is required to address the lack of expertise (fraud experts, cybercrime specialists, cyber risk specialists, and so on) and the resources associated with cybercrime policing in KwaZulu-Natal. Addressing the issue of user education could be seen as beneficial and this could lead to increased convictions for cybercrime in the banking industry.

5.2.3.3 Question 7: Do financial institutions have a profile of cybercriminals?

The researcher asked the above question in an attempt to determine whether banks had a profile of cyber criminals. The fact that the SAPS participants had a wide range of opinions on this matter was intriguing. Despite the fact that South African financial institutions have implemented stringent security measures, cybercrime in the local financial industry is expected to rise. The SAPS officers and bank fraud investigators agreed that detecting and identifying cybercriminals was difficult. Financial institutions are considered 'easy' or 'soft' targets, according to (Smal, 2022), as they typically pay that was demanded in order to keep the attack hidden. This is done to avoid unfavourable publicity and to safeguard their brand image. Participant 6 stated:

> *"The banks have their own forensic investigators, so they assist the South African Police in identifying potential fraudulent accounts. We ask the banks to freeze the*

accounts; freeze the funds in the account. There are people who are losing millions and millions of rand due to their vulnerability. There is just crazy stuff, crazy stuff that takes place" (P6).

The banking industry employs its own fraud investigators, but even experienced specialists and professionals have to ensure that they keep abreast of the latest digital advancements to curb growing cyber threats. Participant 7 stated:

"*The criminals use details of innocent people and steal their identities, making is very difficult for the SAPS to identify the cybercriminal. At times the criminals work with people who are employed in the banking industry to carry out these crimes" (P7).*

Net Guardians (2021:1) states that "it is no exaggeration to say that the greatest fraud risk that banks face walks through their doors every morning and sits down to work". This is a shocking reality in South Africa. Bank personnel are uniquely placed to discover and exploit weaknesses in their organisation's internal control systems and it is a travesty that some collaborate with cybercriminals to defraud the bank that pays their salaries. According to Net Guardians (2021), the banking industry should ensure that all systems are designed to prevent internal fraud and they should engage in employee monitoring, whether through controls that require employees to have certain actions validated by co-workers or through technology that monitors and records each individual's activities on the bank's IT systems and flags any suspicious or unusual behaviour. In this regard, the participants stated:

"…we are able to pick up IP addresses and then we can link via IP addresses as to whose terminal was used and where about it was used" (P8).

"It does not happen regularly; however, there have been linkages that have been made over the past with regards to criminals committing similar crimes and that is how they were identified" (P9).

In light of the foregoing responses, it is noteworthy that, due to the dynamic nature of cybercrime in the financial industry, digital evidence at crime scenes poses a considerable challenge. Cameron (2022) argues that digital evidence is no longer isolated to a single host but is now dispersed over various physical and virtual sites such as online social networks, cloud resources, and personal networks, which further complicates the task of successfully policing cybercrime. Therefore, as the above responses reveal that IP addresses have been

successfully detected, we must commend the SAPS for their efforts to combat cybercrime in the banking industry, especially given their limited resources.

However, cybercriminals are well versed in banks' control and detection measures and always seem to be a step or two ahead. Participant 10 stated:

> *"90% of the time, it is fake information, and this is generated via these criminal syndicates who have stolen lost ID books" (P10).*

Business Tech (2020) supports the preceding response, stating that cybercriminals are savvy and are continually seeking new ways to take advantage. Moreover, they do not employ tactics that may be easily exposed.

A general conclusion is that, in order to lessen the risk of cyberattacks on banks and their clients, banking institutions can use a technology known as 'threat emulation' or 'sandboxing' to provide an extra layer of defence against malware. This software looks for virus-like behaviour in email attachments and isolates any questionable files before they reach bank employees in boxes and risk infecting networks through an accidental click. Moreover, another crucial step is to educate employees about email and web-based infections which can protect banks and their customers' information.

5.2.4 Objective 3: To examine the policies that guide the implementation of cybercrime in the banking industry

5.2.4.1 Question 8: Do any monitoring and reporting of cybercrime activities occur in the banking industry?

For successful cybercrime monitoring and reporting, a link between banking institutions, SABRIC, and SAPS officials is required, particularly in terms of communication and cooperation. When asked if there is any monitoring and reporting of cybercrime activities, the participants indicated that there was some level of monitoring in the banking industry, and they agreed that banks had their own fraud departments. However, because there is no cooperation between the financial sector and local SAPS units to combat cybercrime, this crime continues unabated. The SAPS participants highlighted the fact that the South African Banking Risk

Information Centre keeps track of any cybercrime in financial institutions in South Africa. However, it is important to note that no single entity can effectively combat cybercrime by itself as it necessitates the participation of every account holder. The banking industry will indeed be fighting a lost battle without their cooperation. The following are some of the responses in this regard:

> *"Yes there is. Banks have their own fraud departments, but remember that cybercrime is very complex" (P6).*
>
> *"There is a fraud department in the banking industry; however, it is not helping to curb rising cybercrime activities. I believe that the bank does not trace those criminals and they do not liaise with the police" (P7).*
>
> *"Yes, all cybercrime is monitored by SABRIC" (P8).*
>
> *"There is definitely monitoring and reporting within the banking industry" (P9).*

On the question of monitoring and reporting, one participant stated the following:

> *"The banking industry has a fraud division, and they have meetings with the South African Banking Risk Information Centre in which they have monthly meetings where they red flag what is happening. For example, Mr A has opened up an account with five different banks, and this is the modus operandi, so they have their meetings and they do discuss this internally, but very little is done about it. For the banking industry, their business is based on new accounts, so they do not really look deep and hard into this criminal activity to curb it. It is like cybercrime is taking place and they accept it" (P10).*

According to the foregoing responses, it is clear that cybercrime reporting and monitoring occur, but that these reports are aggregated into monthly or quarterly reports that are addressed with SABRIC. CliffCentral.com (2022) states that SABRIC is a non-profit organisation established by South African banks to aid the banking industry in the fight against crime. SABRIC's clientele includes South African banks and large CIT firms, and its primary task is to detect, prevent, and minimise organised crime in the banking industry through successful public-private partnerships.

The general conclusion that can be drawn from the foregoing findings is that the banking industry's monitoring and reporting system to address cybercrime is ineffective. Banking customers expect a secure user experience and new services with seamless interaction with

their digital accounts on all of their mobile devices from anywhere in the world, and they also want assurance that their money and personal information are protected. All of this and more are what financial institutions seeks to provide, but cybercriminals make it their profession to hack into systems and breach security measures to steal money and information. Financial organisations do not have to choose between innovation and security, but the best approach to avoid internet banking and payment fraud is to prevent it from happening in the first place. The banking industry is required to assess its present control mechanisms and tactics and to devise cybercrime strategies and controls to protect online platforms with a focus on preventative rather than detective controls.

5.2.4.2 Question 9: Are there any oversight committees in place to monitor and evaluate the effectiveness of cybercrime interventions in the banking industry?

The researcher posed the above question to determine the existence of a committee that monitors and assesses the effectiveness of cybercrime in the banking industry. It does appear that cybercrime is widespread in the financial sector and that it has financial ramifications for banks and their customers. As a result, it is necessary to devise measures to combat this crime more effectively. The following are comments that the SAPS authorities offered:

> *"There is an oversight committee that monitors [this crime]" (P6).*
>
> *"I believe that the oversight committee is not effective, as they do not liaise with any investigators and they do not inform the SAPS who the account holder is" (P7).*

Participants 3, 4, 5 and 8 stated:

> *"Yes, there is SABRIC" (P3, 4, 5, & 8).*

Internally, banks seem to maintain a cybercrime oversight committee that monitors the challenges posed by cybercriminals' activities. In their meetings with SABRIC, they discuss cybercrime prevention strategies and whether they need to be revised in light of recent internal and external cybercrime events. The respondents below endorsed this notion:

> *"All cybercrimes that occur within the bank, the information is monitored by SABRIC. SABRIC is the oversight committee" (P9).*
>
> *"Yes, they have SABRIC in place for this. They meet on a monthly basis to discuss cybercrime and the means to stop criminal activity within the banking fraternity" (P10).*

A general conclusion is that an oversight body is in place to assess the effectiveness of cybercrime prevention and detection measures, and this body is SABRIC. It coordinates inter-bank efforts targeted at combating organised bank-related financial crimes, violent crimes, as well as cybercrimes, and serves as a nodal point for concerns linked to these crimes between the banking industry and others. It is evident from the literature that SABRIC is in partnership with numerous financial institutions in South Africa such as: ABSA, African Bank, alBaraka, Bidvest Bank, Capitec, Citibank, Discovery, FNB, Nedbank, Postbank, Standard Bank, and Tyme Bank (SABRIC, 2018). One of SABRIC's priority areas is raising public awareness of various bank-related crimes and educating the public on how to protect themselves. This raises the interesting point about the lack of user education among banking customers. In support of this argument, SABRIC itself has argued that most banking clients are still compromised as a result of phishing, vishing, or the installation of malware on victims' home computers. They then click on a link, which allows the criminal to gain enough personal information to access their online banking profiles, and this results in the cybercriminal defrauding a bank and its clients.

SABRIC has emphasised the need for cybersecurity education and has stated that they are raising awareness through a variety of media, including community radio and newspapers (Kubayi, 2017). According to Kubayi (2017), the general focus of such initiatives is the need for extensive and effective education on cybersecurity threats and how citizens can safeguard themselves. This has been recognised as a priority by both SABRIC and the Department of Telecommunications and Postal Services (DTPS) (Kubayi, 2017). It is clear that SABRIC is making some progress in combating cybercrime, but there is still much work to be done. Cooperation among various stakeholders is critical if the goal of mitigating cybercrime is to be achieved. It should be mentioned that, to address growing concerns regarding cybercrime, it will require joint responsibility and cooperation among all banks, banking clients, SABRIC, and the SAPS.

5.2.4.3 Question 10: What steps are currently being taken by banks to combat cybercrime?

SAPS officials expressed similar views in response to the above question. Clearly, no matter how sophisticated the malware or mechanisms of action are, the starting point for all of these attacks in the banking industry is a simple, targeted phishing email, generally containing a file attachment with the malware payload (*How can branks protect themselves from cybercrime?*,

2015). As a result, the sophistication of cyber-attacks is one of the reasons why bank executives are extremely concerned. According to *how can banks protect themselves from cybercrime?* (2015), cybercriminal transactions appear to be legitimate from the bank's perspective, making cyber-heists a true inside operation that is planned by persons who have a thorough understanding of both business and consumer banking systems. While the financial services sector may be ahead of many industries in terms of financial crime prevention and detection, there is much more that can and should be done to curb cybercrime (Budnik, n.d.). An SAPS participant's response in this regard was as follows:

> *"The banks create awareness such as when you login into your mobile apps, they do have alerts that are informing banking clients of cybercrime and even they provide tips on how to protect yourself. The bank can only create certain alert mechanisms" (P6).*

The aforementioned response suggests that the banking industry raises awareness among banking clients by means of notifications concerning cybercrime when banking clients connect into their banking apps. As a result, the best defence against future attacks is to ensure that banking customers' PCs or devices that are used for online banking have up-to-date protection. Banking customers should be reminded on a frequent basis to protect themselves by installing up-to-date anti-virus software and a firewall on their home computers.

Participant 7 offered the following comment:

> *"The banks have introduced the bio metric functionality; however, I believe that it will not be successful has it is not linked to the Department of Home Affairs, therefore how will the bank be able to verify such information?" (P7).*

The banking industry is attempting to implement new measures and tactics to prevent cybercrime, as is evidenced by the above response. In the case of biometric functionality, this can be considered a significant tool, particularly when opening bank accounts. However, policies and legislation should be revised so that biometrics can be linked to the Department of Home Affairs for authentication purposes. Bielski (2000) adds that biometric technologies have the potential to become a one-of-a-kind technique for personal verification and secure identification in banking institutions.

In terms of the complete digitalisation of banks, Participant 8 stated:

"The banks are going digital where all correspondence will be sent via digital means. That will also be monitored by SABRIC, so more secure networks, more secure domains. It is not just going to be your normal public domains where members of the public will have access to. It is only going to be NPA, SAPS and the banking industry" (P8).

The point that was raised that the banking industry is moving towards full digitalisation in terms of correspondence is corroborated by PwC South Africa (2018), which states that the South African banking industry is increasingly shifting towards a marketplace without limits, driven by the fast-approaching entry of new digital companies that challenge the status quo and spur unprecedented levels of innovation to ensure more secure networks and domains. As a result, four universal banks (ABSA, FirstRand, Nedbank, and Standard Bank) have continued to invest in large-scale transformation programs aiming at improving customer experience, digital transformation, new methods of working, and cost reduction across the board. Participant 9 stated:

"There is relevant training that has been given to investigators within the banking industry. Also, specific laws have been put into place for cybercrime. It is promulgated. I believe the banking industry is up-to-date with patterns and trends; however, there are new methods that criminals use to defraud financial institutions" (P9).

It is evident that stopping these cyberattacks will necessitate a combination of employee and customer awareness as well as updated, comprehensive security defences on both bank networks and their customers' computers. Changes in legislation also need to be constantly reviewed due to the dynamic nature of cybercrime. Participant 10 stated:

"There is this measure where the banks discuss their shortcomings in respect of cybercrime and look for means to curb it in the future. They try to close the loopholes that criminals are using" (P10).

In response to the above comment about banks trying to close loopholes in the banking industry, some of the key proposals mentioned by (*How can banks protect themselves from cybercrime?*, 2015) are the continuous training of bank employees and scanning emails for vital socially engineered clues like misspelled words, unexpected email attachments, or links. Such vigilant scans can make a huge difference in reducing the success of any hacking attempts.

Criminals always seem to be abreast of digital development and innovations, as was mentioned by Participants 1 and 2:

> *"Criminals are constantly changing how cybercrime is perpetrated. I am not sure what measures are in place currently in banks" (P1).*
>
> *"Cybercriminals are changing their strategies–their modus operandi, and banks do not have effective systems in place" (P2).*

Due to the rapid speed at which cybercrime strategies develop, the banking industry must be ready to respond as rapidly, if not faster, to any new or emerging attack on any financial platform or client portal, as cybercriminals are continuously changing their modus operandi. According to the Global Provider of Secure Financial Messaging Services (2019), an experienced and motivated cybercriminal can negotiate most defences, enter a network in minutes, and elude detection for months by using several entry points. The financial services industry, more than any other, is therefore a common target for cybercriminals. We have seen an increase in cyberattacks and data breaches in recent years, and cybercriminals have successfully infiltrated banking institutions using everything from malware, ransomware, to social engineering tactics.

5.2.4.4 Question 11: Is there anything that you would like to elaborate on, or is there any final comment that you would like to make before we conclude?

Each participant was given the opportunity to respond outside the interview schedule. This open-ended question was included to ensure that the data would be enriched because these responses might reveal themes or give a new direction to the investigation that the researcher had not foreseen. The SAPS participants' responses were as follows:

> *"I think the banks are useless and they do not care about their banking clients. I am very disappointed with the interaction from the bank that we as SAPS detectives receive" (P1).*
>
> *"The banking industry is not openly divulging information. When the commission of an offense takes place, we have to serve the bank with a Section 205 in order to come to a positive conclusion about what has taken place, and it takes a long while until we receive any information from the bank. In cases when the banks have picked up something and we ask them what the money is for, the banks are not willing to disclose*

that information to us. Bank do not have effective systems in place [to address cybercrime]" (P2).

In light of the above responses, it is evident that cybercrime cannot be combated by acting alone. Instead, the public, the commercial sector, and the SAPS must work together to discover mutually beneficial solutions to this problem. South Africans have been targeted by cross-border syndicates, and their actions have had a severe impact on the financial industry and particularly on banking clients. Combating this crime thus necessitates intensive formal and informal coordination among key role-players. The banking industry must be more responsive to this challenge by for instance sharing information with SAPS officials and involving them in meetings with SABRIC. Only when there is a free flow of information between these role-players will the SAPS be able to successfully police and solve cases of cybercrime.

In terms of Section 205 of the Criminal Procedure Act 51 of 1977, (Republic of South Africa, 1977), SAPS officials who investigate cybercrime should be given a direct link to all financial institutions. In this way the officials will be able to email any queries directly to FNB, ABSA, Standard Bank, and other banks, and they will be able to receive information within a few days. If this process is streamlined, SAPS officials will not have to put their investigations on hold because they will not have to wait for correspondence from the banking industry.

Many people fall for fraudulent messages that lure unsuspecting victims into the spider web due to greed. Participant 6 offered the following example:

"You will get an email from the International Monetary Fund (IMF) telling you that you are a beneficiary of a couple of million rand, and then you get another email from Standard Bank stating that the International Monetary Fund has deposited money into your account, but before the money may be cleared, you need to pay certain taxes for clearing amounts. You then go ahead and pay this amount, but the irony of this is, why will the IMF be paying you money? One needs to consider whether the IMF will be paying you money in the first place. How can you be a beneficiary of the IMF? That is something that is happening now; cybercriminals are constantly changing the ways in which they defraud you" (P6).

The aforementioned statement is noteworthy as it highlights that the goal of all cybercriminal attacks is to acquire access to a customer's banking profile in order to commit fraud and obtain

money illegally. However, because criminals find it much easier to attack individuals than IT systems, the process begins by obtaining the customer's personal information, which is often easy as people are greedy and unrealistic and everyone likes to have more money. When the SAPS examines volumes and spikes, it can be seen when and where cybercrime is on the rise, particularly in cases where a customer's personal information was compromised and was unaware of it. This is evidence of users' lack of knowledge and understanding of cybercrime. It is worth noting that technical and support employees in the banking, IT, and other finance-related sectors, as well as those who are technologically aware, will have a better grasp and knowledge of the security risks involved in online transactions. The general public, on the other hand, does not have the same level of knowledge and awareness of cybercrime. How can this be addressed? Participant 10 provided quite and extensive response:

> *"I think, for the banking industry and the police, the only way we are going to rectify cybercrime is if we get people to become experts in this field. We get computer analysts, we get people to analyse the bank accounts to verify the accounts before they actually open it, or all the account information, because these cybercriminals are getting away with it and it is too late once the money is already into the account. Only then do we say that we should have done this or we should have done that. For example, if someone is taking 5c from your account and my account, we do not look at that, but the banks should implement some structure or some measure to say, 'Right, if 600 of our clients lost 5c due to an illegal withdrawal, then there is something wrong! Why is someone withdrawing 5c from so many accounts?' And this is what cybercriminals have been doing over the years and they have been getting away with it. If someone is taking money out of your account, and you do not pick it up and the bank is not even picking up on it, I think cybercrime is going to be a huge problem in the future. Currently, right now, white collar crime is taking the world by storm. You do not need to run into a bank branch to rob them anymore, you can rob a bank electronically" (P10).*

Three noteworthy points emerged from the foregoing response. (i) Training officials need to become experts or specialists in the field of cybercrime; (ii) the banking industry is reviewing their existing strategies but should do so on an ongoing basis, and (iii) criminals no longer need to physically rob a bank branch because they can do so electronically with impunity. The fact that their activities have not been curbed means that these criminals devise ever-changing strategies to commit cybercrime. To counteract cybercrime, experts and specialists are required who will find the means of staying abreast of the measures cybercriminals can and will design

to defraud unsuspecting citizens and banks. Perhaps a flippant, yet interesting thought is that these experts should be paid exceptionally high salaries as they might be so proficient that they revert to cybercrime themselves as a more lucrative means of obtaining money.

5.2.5 Summary of Findings Section One

The narratives and responses of the SAPS participants confirmed the argument in the literature that cybercrime is constantly evolving and that, in the context of financial institutions, it is primarily caused by a lack of preventative controls and IT systems that are not robust enough to proactively detect and prevent cybercriminal activity. It is clear that digital fraud, hacking, and online fraud are common in the banking industry, which is a statement that is supported by SABRIC. Furthermore, the rate of cybercrime remains consistent from January to December across all South Africa's major banking institutions. Moreover, banks are a desirable target for cybercriminals as they are the custodians of huge sums of money that are accessible on cyberspace on a global scale. The fact that banks devise safeguards but do not update them often enough (currently they need to be updated almost on a daily basis) means that cybercriminals are constantly watching their patterns to find loopholes. This phenomenon is explained by the routine activity theory. Moreover, cybercriminals are well aware of the low conviction rate for cybercrime in South Africa, which is why cybercrime is escalating in this country. Another important driver of cybercrime attacks in the South African banking system is a lack of user education (i.e., knowledge and awareness), and thus users engage in online activities while not being fully aware of security implications. According to SAPS officials who were interviewed, the banking industry should consider installing additional security measures to safeguard customer information and upgrade their internal systems and processes more often to reduce their exposure to cybercriminals. Experts and specialists in this field should be appointed and retained to deal with the challenges associated with cybercrime. It is important to note that policing cybercrime is the duty of everyone with internet access. Although the SAPS is understaffed, these people are doing their best with the limited resources available.

5.3 Section two

In this second section the research findings are applied to the literature that was examined in foregoing chapters. This section tells the story of the case and links the emerging themes to the

study's goals and objectives. An interview schedule was used to elicit responses that would address the research objectives and questions.

5.3.1 The causes of cybercrime

The main causes of cybercrime in South African banks in the study area were:

- Compromised client information due to the deliberate leaking of data (internal fraud);
- Banks' poor internal controls, processes and systems;
- User's lack of education (knowledge and awareness of cybercriminal activity in the banking industry);
- The low apprehension and conviction rates of cybercriminals in South Africa and the resultant lack of penalties or legal retribution;
- SAPS officials' lack of the necessary skills and information;
- A limited number of trained police officers that have the requisite skills to investigate cybercrime and apprehend cybercriminals.
- A lack of collaboration among and flow of information between key-role players to combat cybercrime.

SABRIC has been making progress in its fight against cybercrime but there is still much work to be done. Cooperation among various stakeholders is critical to achieve this goal, and there is a need for an industry-wide framework for effective e-fraud governance, regulation, and policies, with a focus on combating fraud through electronic channels.

The discussion that follows connects the above-mentioned themes to the literature and the theoretical framework of the study.

5.3.2 Internal fraud within the banking industry

Net Guardians (2021:1) states that "…the greatest fraud risk that banks face walks through their doors every morning and sits down to work". Unfortunately, internal fraud is a sad reality in the South African banking industry. Comments in this regard were"

> *"At times the criminals work with people who are employed in the banking industry to carry out these crimes" (P7).*

"…staff members divulging confidential information to the suspects [cyber criminals]" (P8).

The abuse of administrator credentials is one of the most serious internal fraud threats facing South African financial institutions, because some highly trusted IT personnel and other associated staff will always require super-user profiles to complete their daily responsibilities or undertake important maintenance on core banking systems, therefore this represents an unavoidable source of difficulties. The aforementioned responses suggest that some untrustworthy bank employees, lured by the smell of money, tend to leak information to a third-party platform. According to Bestpractice.biz (2020), a South African bank admitted that an employee had sold sensitive data of more than 200 000 clients to a variety of other parties, which highlights the importance of an information security management system within banks. (Buthelezi, 2021). The employee involved was a member of ABSA's credit analysis team and had access to critical information regarding the company's systems, including the risk-modelling system which was linked to the company's database (Buthelezi, 2021). The data breach was detected on 27 October 2020, but the bank delayed for a month before disclosing the extent of the incident to the public. This decision, according to ABSA, was made to ensure that court processes were not jeopardised. ABSA's Chief Security Officer, Sandro Bucchianeri, told South African news station *ENCA* that the data breach had affected only 2% of the bank's customer base, but it still means 200 000 people might have had their personal information compromised (Bestpractice.biz, 2020).

According to a Hawks spokesperson, Captain Mulamu (cited in Comins, 2021), Zandile Sibiya, Newtown's First National Bank (FNB) operations manager, fraudulently processed Forex payments with International Banking Centre System transactions and transferred approximately R4 million into her bank account. Bhengu (2022) stated that Xolela Masebani, an ABSA specialist engineer who worked in Sandton, was suspected of stealing R103 million from the bank and reportedly transferred the money into six other bank accounts between September and December 2021.

With the foregoing in mind, there are some measures that the banking industry should consider, such as employee monitoring, particularly for those employees who have access to a bank's most sensitive information. This is backed up by Net Guardians (2021), which claims that all internal fraud prevention systems rely on employee monitoring, whether through controls that

require employees to have certain actions validated by co-workers or through technology that watches and records each individual's activities on the bank's IT system that flags any suspicious or unusual behaviour. Monitoring is an important aspect of current anti-fraud systems as previous data on individual behaviour can be collected, and profiles can be created to evaluate and predict future behaviour and to detect irregular activities. Furthermore, informing employees that their usage of the company's IT system will be monitored is likely to dissuade internal fraud in banks.

IT administrators in South African banks should be required to sign in using their own credentials because they typically access networks using generic logins, which makes it impossible to follow their actions (SQN Banking Systems, n.d.). Banks have to create an audit trail by requiring their employees or contractors to use their own credentials. Checking user access profiles on a regular basis and looking for red flags (like personnel with higher-level access than they should have) should be a normal procedure to mitigate the risk of internal fraud.

Banking institutions should ensure that bank staff are regularly educated on the indicators of internal fraud, as a bank's staff is the most valuable asset in the banking industry when it comes to detecting internal fraud. According to SQN Banking Systems (n.d.), educating employees about red flags as indicators of internal fraud and letting them know what actions may indicate internal fraud are critical measures. Also, conducting awareness campaigns about the consequences and legality of committing internal fraud is vital if banks want to stem the tide of cybercrime.

5.3.3 Banks' poor internal controls, processes, and systems

Cyber criminals and the tools they employ to get access to sensitive data are becoming more sophisticated as technology advances. The financial services industry more than any sector is a common target for cyber criminals. We have witnessed an increase in cyber-attacks and data breaches over the last several years as cyber criminals successfully infiltrate banking industries using everything from malware, phishing emails, and ransomware to social engineering tactics. Due to the enormous value of information held by financial services firms, they are the prime target for cybercriminals. Budnik (n.d.) mentions that the pressure on financial institutions to act is increasing, as attacks become more common and regulators pay more attention. PwC

South Africa (2018) points out that Francois Groepe, the Deputy Governor of the South African Reserve Bank, has warned financial institutions to be mindful of cyber threats as they embrace technological improvements.

Moreover, numerous attempted cyberattacks aimed at manipulating bank payment systems have been made with many of them following a similar pattern. These attacks are followed by months-long breaches of bank systems allowing attackers to acquaint themselves with bank security defences and the best cash-out methods. In this way, by gaining authentic operator credentials and introducing fraudulent transactions straight into back-office systems, cybercriminals attempt to contaminate the local environment and payment processes of financial institutions (Budnik, n.d.). This puts the back office as well as business controls, that would normally keep fraudulent behaviour away, at risk. The following are some comments regarding the issues banks face:

> *"Cyber criminals are changing their strategies and their modus operandi, and banks do not have effective systems in place" (P2).*
>
> *"There are just so many misunderstandings from the banks' perspective which actually occur on a regular basis. The bank is not adjusting accordingly" (P1).*
>
> *"Cybercrime occurs because of the negligence of banks" (P7).*

Criminals have taken advantage of new technology-enabled opportunities and have been able to quickly adapt to previously segregated risk management procedures. Financial institutions could consider meeting colleagues in other financial crime pillars and starting dialogues around the idea of convergence by identifying short-term benefits, soliciting comments, and keeping the conversation going (PwC South Africa, 2018).

Furthermore, the banking industry must ensure that it has adequate mechanisms in place. The access to confidential information should be restricted depending on the roles and responsibilities of employees. The financial institution should constantly ensure that devices are secure and ensure that all employees who access company systems are protected from common threats and risks. Bank employees should be forced to keep their working devices patched and updated at all times when it comes to device updates. The banking industry is also required to provide regular awareness campaigns and education programmes to employees, particularly on topics such as how to recognise suspicious activity on working devices and how to report their concerns. However, the banking industry should ensure that it monitors the

effectiveness of this by continuously running tests. Banks can use experts to detect fraudulent emails and identify those employees who click on suspicious activities and provide them with additional training.

It is important to note that bank staff can easily grow complacent or become blinded to system problems, especially if they are not security experts (Standard Bank, 2021). As a result, it is recommended that professional contractors be recruited to conduct frequent security audits and discover vulnerabilities that the banking institution may have overlooked. These experts can also perform penetration tests using real-world hacking tools and tactics to try to get into the financial sector's network to test and verify banking defences. According to Whitney (2021), the banking industry should take advantage of existing ties with e-crime providers, dark web experts, and internal and external cybersecurity professionals to identify credential testing and verify consumer scam reports. It is important to realise that no security system is flawless, therefore the joint responsibility of government departments, experts in the field, SABRIC, and the SAPS is required.

5.3.4 Banking clients' lack of knowledge and awareness

As mentioned by Gordon (2002), cybercrime has no physical borders and is not subject to import/customs or currency restrictions, which makes it a desirable option for anyone from anywhere in the world who wishes to acquire money illegally. According to the Norton Cybercrime Report (2011), over one million people are victims of cybercrime every day, and 14 adults are victims of cybercrime every second. The Internet Complaints Centre of the Federal Bureau of Investigations ranks South Africa eighth in the world in terms of cybercrime vulnerability (Da Silva, 2011).

According to Pillay, the former CEO of SABRIC, criminals are continuously seeking new methods to exploit digital platforms to defraud victims; however, because banks' mitigation techniques are so strong, it is easier to target humans who are the weakest link (SABRIC, 2018). According to Pillay, cybercriminals take advantage of the fact that not all digital banking customers are computer literate and they exploit this weakness, and banking clients are thus most often infiltrated as a result of phishing, vishing or the installation of malware onto a victim's device via a link that allows the cybercriminal to gain enough personal information to access their victim's online banking profile (SABRIC, 2018).

SABRIC mentions that they have seen an uptrend in vishing incidents, wherein criminals contact bank customers and mislead them into thinking they are speaking with the bank or a legitimate service provider. They then use social engineering tactics to trick them into disclosing their confidential bank card information as well as other personal information. Phishing is another method that cyber criminals utilise and according to the Banking Association South Africa (n.d.) states is a way of deceitfully collecting personal information such as passwords, identity numbers, and credit card information and in certain cases, money. Criminals may phone you or send you e-mails that appear to be from reputable organisations such as banks, financial institutions or legitimate businesses.

As mentioned by the Banking Association South Africa (n.d.), phishing emails typically ask recipients to verify or update their contact information or other sensitive financial information by clicking on a link in the email that takes them to a fake website which is designed by criminals to fool users into thinking that it is a legitimate site. In this way, spoof websites resemble the real websites of well-known financial institutions or businesses. There are thousands of phishing emails, which are a type of spam, that are sent to banking clients' email accounts. The attackers post forms on these fake websites to deceive victims into divulging personal information. Evidently, according to a recent survey, a significant number of customers responded to fake emails allowing their personal information to be obtained fraudulently. The participants commented as follows:

> *"Not everybody gets affected by cybercrime but the people that do get affected by it, you will see they were actually were soft targets, and they would easily have given in to the criminals' questions in terms of their ID numbers and their banking information" (P10).*
>
> *"They are people that are losing millions and millions of rand just because of their vulnerability. There is just crazy stuff, crazy stuff that takes place" (P6).*
>
> *"One needs to consider why the IMF will be paying you money in the first place? How can you be a beneficiary of the IMF? That is something that is happening now; cybercriminals are constantly changing the ways in which they defraud you" (P6).*
>
> *"Currently I have a case, where an attorney received at email at 10 pm and the client informed her that her banking details had changed and she EFTed money from her trust account into this new account, only to realise the next day that it was not a client from the bank. What the cybercriminals did was print the letter head and everything was like the client had done it, and the lady had lost R2,5 million" (P10).*

The first and most important step is to provide customers with information on how to protect themselves against cybercrime. Banks should urge their clients to check their accounts frequently between statements to ensure there are no irregularities. The banking industry is required to provide awareness campaigns to inform the public that Wi-Fi networks are frequently insecure and that cybercriminals can simply eavesdrop on their activities if they do not utilise a VPN (Sanders, 2020).

There are many consumers that continue to use the same password for multiple accounts, which increases their risk exponentially. By helping customers understand the importance of using a unique password for each account and directing them to tools to securely manage their passwords, both banking clients and the banking industry could enjoy more security. The banking industry is required to ensure that customers are aware of technology that is available to secure their accounts, such as using on/off card features, documenting trip plans with banks and card issuers, as well as setting up purchase notification features for debit and credit cards (Sanders, 2020).

Banking consumers may need more than one effort to fully absorb the cybercrime prevention message, therefore it is vital that banks employ all communication channels available such as statement inserts, website messages, social media posts, texts, emails, and in-person contacts to educate their clients about cybercrime. Furthermore, banks should provide their banking clients with educational workshops or online videos on fraud and cybersecurity to help them better understand the true scale of cybercrime. The banking industry should also educate and capacitate citizens against cybercrime and cyber fraud through schools, universities, and FET institutions by through awareness programmes. The banking industry should ensure that the internet is safe and secure for everyone by paying special attention to vulnerable populations such as women, persons with disabilities, and the elderly (Grobler, Jansen, van Vuuren, & Zaaiman, 2013).

5.3.5 Low conviction rates

South African financial institutions are members of the South African Banking Risk Information Centre that collects information on cybercrime from all banks in the country. The major goal of SABRIC is to combat bank-related crimes. According to the literature and the responses of the participants, cybercrime activities are monitored by SABRIC and the SAPS,

but a limited number of cybercrime-related cases resulted in successful convictions. Although some arrests have been made, there have been few convictions due to the small number of arrests and the absence of evidence to convict cybercriminals.

Furthermore, because cybercriminals use customers' online profiles as their own, tracing these crimes to an individual is extremely difficult. Cybercriminals bound their signals from country to country which making policing cybercrime extremely challenging anywhere in the world. Mer, the Managing Director of Eftsure Africa, which provides web-based payments and verification services, stated that cybercrime was lucrative and could be perpetrated from anywhere in the world with targets located anywhere (Maliba, 2021). Mer explained that, because of the "behind the screen nature of the crime", catching and prosecuting these offenders was tough, which made it appealing (Maliba, 2021). This notion is supported by Loxton (cited in Business Tech, 2013:1), head of the Business Crime and Forensics unit at Werksmans, who stated: "South Africa has been proven to be a particularly fertile ground for cybercrime due to it being a lawless society, with cybercrime syndicates knowing that law enforcement is paper thin, with low chances of being arrested and successfully convicted". The participants stated:

> *"There are minimal convictions for cybercrime and it happens randomly" (P10).*
>
> *"Very hard to say with regards to cybercrime conviction, they are very low convictions" (P1).*
>
> *"Out of ten cases, there is only one successful conviction and this is usually a suspended sentence. It is very rare to convict criminals and this is beyond the control of the SAPS. Also, criminal's use this to their advantage as they are aware of the low conviction rate and that is the reason cybercrime continues to increase" (P7).*

With the foregoing in mind, it is critical that strategic steps be implemented to combat cybercrime in the banking industry. It is vital that the government trains police and prosecutors in how to effectively investigate and arrest cyber-offenders, as well as how to explain cybercrime prosecution to a judge. The banking industry must ensure that it has the appropriate expertise in-house to deal with potential threats and to put procedures in place to minimise its vulnerability. Van Der Merwe (2014) argues that, while the introduction of the ECT Act is to be applauded, there is still opportunity for improvement. For instance, the criminal sanctions under Section 89 of the ECT Act have been criticised for being far too lenient. Cassim (2011) elaborates on this point by mentioning that most offences that are prohibited by Section 86 are punishable by a maximum of one year in prison, but crimes prohibited by Sections 86(4) and

(5) (such as denial of service attacks) and crimes prohibited by Section 87 (extortion, fraud, and forgery) are punishable by a maximum of five years in prison. Therefore, to dissuade sophisticated cybercriminals in South Africa from attacking banks, harsher penalties and sanctions are required.

5.3.6 SAPS officials' lack of skills to effectively police cybercrime

The SAPS faces major challenges as a result of the growing menace of cybercrime. According to Holt, Burruss, and Bossler (2019), Bossler and Holt (2012), and Lee, Holt, Burruss, and Bossler (2019), law enforcement officials are having a difficult time dealing with cybercrime due to their inability to acquire the necessary technology to conduct adequate police investigations. They have also been insufficiently trained, and officers who possess the appropriate skills to combat cybercrime often leave the Force for greener pastures. More SAPS officials need to be trained in cybercrime prevention, detection, and prosecution/application of the law and punishment so that they can stay one step ahead of cybercriminals. According to Aphane and Mofokeng (2021), the SAPS must be better equipped to gather evidence of the commission of cybercrime as they must be able to prepare and address some of the myriad issues related to examining physical and digital evidence. This necessitates the efforts of specialised cybercrime forensic experts and computer forensic investigations to maintain a proper chain of custody.

As was stated earlier, when police officers become experts or specialists in cybercrime, they often leave the SAPS to work in the private sector where they have more job security. Furthermore, unlike in the SAPS where resources are scarce, the private sector permits cybercrime specialists to improve their abilities and knowledge because resources are easily available. The implications for the SAPS are that the specialised investigation units are facing significant capacity challenges due to a lack of personnel and technical tools to meet the demand for cybercrime-related investigative support. The SAPS is also restricted by a lack of cooperation or collaboration with other role-players, and this limits officials' ability to implement strategies such as task force models to help overcome cybercrime challenges.

Moreover, the SAPS is either unprepared to respond to cyberattacks or lack the necessary technology to collect evidence. Criminals will continue to benefit from a shortage of skilled specialists to investigate cybercrime. In addition, the resources necessary to execute cyber-

related investigations are frequently significant, simultaneously the crime could be high-tech and investigating such a crime generally necessitates a significant amount of traditional investigative work and highly technical expertise, both of which are in short supply in South Africa. The participants stated:

> *"Also, there is not adequate training provided to SAPS officials to thoroughly investigate cybercrime. We do not fully understand cybercrime and we do lack the knowledge, therefore it is very difficult" (P1).*
>
> *"The only way we are going to rectify cybercrime is if we get people to become experts in this field" (P10).*

Law enforcement agencies and cyber professionals must receive training on current trends and strategies to stay up-to-date with evolving and sophisticated cybercrime threats. This means that a strategic approach is needed to ensure that the SAPS vision and mission statements are emphasised throughout detective training. Also, mandatory refresher training on cybercrime and law-related modules should be implemented. Instead of developing training programs when flaws are discovered through training audits or criticisms from the general public, legislators or the media, a strategic approach is essential to anticipate the changing landscape within the wider Criminal Justice System and/or detective programme best practices.

Beyond internal courses, a capacity development and mentoring program should focus on the development of potential detectives as well as the support of inexperienced detectives' investigative competencies, particularly in terms of the battle against cybercrime. These capacity-building strategies should provide support, resources, information, and learning opportunities that will systematically target and improve desired performance and behaviour among SAPS officials. Leal (2008) proposes that one strategy to combat the threat of cybercrime is to employ law enforcement professionals who already have technical expertise. The effectiveness of new forms of training, such as those delivered electronically, would potentially be impacted by such a recruitment strategy. According to Mofokeng and De Vries (2016), the detective curriculum of the SAPS should be kept up-to-date with recent developments in the broader criminal justice environment, and the SAPS should conduct research on a regular basis and liaise with overseas counterparts for best practices and modify the curriculum accordingly.

5.3.7 Lack of collaboration between key role-players

The co-operation and collaboration between the SAPS and other stakeholders is critical for the banking industry. It is crucial to remember that cybercrime differs from other types of crime in that the offenders may be thousands of kilometres away from the targeted bank and its customers, with no crime scene. In terms of cybercrime, criminals' modus operandi are quite complicated. South Africa is one of the countries with the highest rates of cybercrime in the world, and the SAPS should play a critical and effective role in the fight against it (Dlamini & Mbambo, 2019). It is therefore crucial that the SAPS Directorate for Priority Crime Investigation (or Hawks), detective units, the cybercrime unit, and other units are all directly involved in combating cybercrime, financial crime, and corruption in South Africa.

While there are sound policy reasons for certain barriers to information sharing within the banking industry, such as the privacy of banking clients, SAPS officials believe that sharing information for effective collaborative between the banking industry and the SAPS is vital. The necessity for law enforcement and banks to cooperate has never been greater, but the problems in achieving this continue to be a major stumbling block. The participants commented as follows:

> *"The banking industry is not willing to share this information with the SAPS. For example, if there is a suspicious activity, we are not informed about this" (P2).*
>
> *"I believe that the bank does not trace those criminals and they do not liaise with the police" (P7).*
>
> *"I think the banks are useless and they do not care about their banking clients. I am very disappointed with the interaction from the banks that we as SAPS detectives receive" (P1).*

There are certain mechanisms such as laws, conventions, the banking industry's initiatives, and information-sharing platforms that already exist to ensure cooperation. However, these seem insufficient because cybercrime continues unabated. Clearly, cybercrime cannot be combated by unilateral action. Instead, the banking industry and SABRIC must join forces with the SAPS to identify mutually beneficial solutions to deal with this phenomenon. This means that the banking industry should be more open to releasing information to the SAPS and allow its officers to effectively police cybercrime without any hurdles that impede investigations. It must be mentioned that successful cooperation between banks and the SAPS will necessitate a

certain level of confidence, which may be reached by creating and maintaining an environment of fairness, transparency, and equity in all their interactions. The various stakeholders must commit to a long-term dialogue and cooperation based on a better knowledge of their unique requirements, goals, and values, as well as shared decision-making.

5.3.8 Summary of findings: Section two

The nature and characteristics of cyberspace should conform to the dynamic spatial environment with identity flexibility, anonymity, and deterrence measures for cybercrime. As there is a blurred border in terms of geography and time between cybercrime and traditional crime, cyber offenders commit their crimes with impunity as they can hardly be traced. If the banking industry wants to reduce internal fraud, banks should conduct extensive monitoring of employees by doing pre-employment screening checks, particularly when employees are exposed to sensitive information. The banking industry should continue to establish and implement robust and stringent internal processes and systems to manage cybercriminal activity. This is critical for the execution of operations that are targeted at countering cybercrime. It seems that banking clients' understanding of the dangers of cybercrime does not keep pace with the rate of advancement of technological and cyber-related activities, and therefore the banking industry needs to employ every available communication channel to educate clients about cybercrime, such as statement inserts, website messages, social media posts, texts, emails, and in-person contacts.

To reduce and eventually eradicate the number of clients who fall victim to cyberattacks, South African banks must identify, design, and implement preventative controls and also educate their clients to utilise these online services effectively and safely. The dilemma that the SAPS faces is not only a South African issue, but a global one. Research has shown that one of the primary hurdles to successful cybercrime legislation is a shortage of resources available to cybercrime investigation units. Therefore, as a first step towards eradicating the scourge of cybercrime in the banking industry, important security stakeholders such as the government, banks, private corporations, academia, the military, and the general public must work together to safeguard cyberspace and develop resilient solutions to combat cyberattacks.

5.4 Conclusion

With the advent of the fourth industrial revolution, cybercriminals have become increasingly aggressive in their attacks on financial institutions. Therefore, efforts to mitigate cybercrime should include changes in the financial industry to better safeguard personal data. This process will necessitate a large number of key role-players. In Section one the data obtained from ten SAPS participants were evaluated and the main findings were presented. The participants shared both similar and diverse views on the causes and impact of cybercrime in the banking industry. The interview schedule (see Appendix C) contained eleven questions that were posed to address the study's objectives. The responses highlighted that technical difficulties, a lack of information and awareness, and a lack of laws are among the challenges that the banking industry faces in its efforts to deal with cybercrime. Clearly, combating cybercrime has become an increasingly serious challenge that might stall growth in the South African economy.

The researcher first presented the main findings related to the objectives, and then the themes that emerged from the data analysis process were discussed. Six themes were addressed in Section two. A key finding is that technological advancements occur rapidly, but cybercriminals' activities evolve as quickly, if not faster. The banking industry is thus frequently left behind while the availability of new technologies with high operational speeds, capacity, and connectivity makes illicit operations more difficult to identify. There is a lack of public awareness about how to maintain a minimum level of security with regard to personal information or electronic property, and it is critical not only to educate those involved in the fight against cybercrime, but also to draft appropriate and effective legislation to advance and win this battle. Due to the intangible nature of cyberspace, most law enforcement agencies lack the technical expertise, sufficient regulatory powers, and automated equipment to investigate complicated evidence and apprehend and prosecute those who engage in fraudulent digital transactions. As a result, cybercriminals lull in a safe harbour while the implementation of legislation to curb their activities is ineffective. A bank is often hesitant to report cybercriminal activity in fear of harming its reputation and thus deterring investors and reducing public confidence, and this stumbling block should thus be addressed as a matter of urgency.

In conclusion, the banking industry, SABRIC, and SAPS are making slow progress in combating cybercrime, and much work needs to be done to harness cooperation, collaboration, transparency, and understanding among the various stakeholders in this industry. The following chapter will present the main conclusions and recommendations.

CHAPTER SIX
CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

Conclusions based on the discoveries that were elicited from the data and pertinent recommendations will be presented in this final chapter. The researcher will also affirm that the research objectives were met. This study focused on a criminological analysis of cybercrime activities in the South African banking industry. As stated in Chapter one, one of the aims of this study was to establish the causes of cybercrime in light of its devastating course in the banking industry. The study was limited to ten SAPS officials who discussed their experiences of cybercrime in the banking industry in Durban, KwaZulu-Natal, with the purpose of addressing the objectives and achieving the aims of the study. Another aim was to explore the legal framework that guides cybercrime investigations in South Africa. The intensive literature review that was conducted revealed that cybercrime is an escalating problem that has become a matter of global concern.

The routine activity theory, the rational choice theory, and the space transition theory guided the study. The routine activity theory was utilised to explain why cybercrime can so easily infiltrate the financial sector, while the rational choice theory, which elucidates that the presupposition of human criminal behaviour is based on rational decisions, was used to explain why the banking industry is so readily targeted by cybercriminals. For instance, a large number of banking clients and security systems that can be breached offer financial rewards that are considerably greater than those when a single customer is targeted. The space transition theory was used to underscore that cybercriminals believe that, due to their anonymity on online platforms, they feel free to commit their planned offence.

The researcher posed open-ended research questions during semi-structured face-to-face interviews with the ten participants to investigate the causes and impact of cybercrime in the banking industry. One female and nine males participated in the study. Thematic analysis was conducted to make sense of the data that had been collected from the participants (Braun & Clarke, 2006). The open-ended questions that had been devised prior to conducting the interviews aided the researcher in directing the discussions and focusing on the required data. By keeping the objectives in mind, the researcher was able to extract relevant data to answer

the research questions. Ultimately, the research aims were met as a thorough grasp of the causes of cybercrime in the banking industry was attained while the exploration of legislations and policies revealed their ineffectiveness to curb cybercrime.

Cybercrime remains a dire threat to the South African banking industry due to increased attacks on its networks and clients. A substantial share of these attacks includes fraudulent access to consumer information that is later used to withdraw funds from various accounts. As relatively little research could be traced on cybercrime in the South African banking industry, this study should fill many gaps in scholarly knowledge regarding this phenomenon. Despite the overwhelming presence of cybercrime in the banking industry in South Africa in recent years, cybercrime remains a subset of crime and there is thus a lack of laws and policy implementation to successfully combat it in South African banks.

6.2 Establishing the causes of the increased rate of cybercrime in banks

The following discussion focuses on the conclusions that were drawn from the study's findings. The three objectives as outlined in Chapter one are addressed with the purpose of achieving the aims of the study.

Activities by cybercriminals in the banking industry are driven by a variety of factors. The SAPS officials were asked to express their opinions on what types of cybercrime are committed by cybercriminals and on the prevalent mechanisms cybercriminals employ to sustain cybercrime. Furthermore, they were asked to comment on their views regarding banks' assessment of the core causes of cybercrime. This objective was achieved as the causes of cybercrime were identified. These are summarised in Table 6.1 below.

Table 6.1: The causes of cybercrime in the South African banking industry

Types of/portals for Cybercrime	Causes of Cybercrime
Cybercrime occurs through banking apps, digital bank fraud, and online fraud.	Phishing, vishing (voice phishing), smishing (SMS phishing), and e-mail hacking or corporate e-mail comprise were mentioned as the most prevalent fraud types affecting the digital banking arena.

Cybercrime is an opportunistic crime.	Banks' poor internal controls, processes, and systems result in cybercrime activities.
Non-verification of documents.	Security controls appear to be the most significant management flaw in terms of cybercrime attacks in banks. As a result, these financial institutions' approach to preventing cybercrime is viewed as detective and reactive rather than preventive.
Banks' negligence.	The banking industry's cybercrime strategy includes regular evaluations of cybercrime alerts issued by their respective fraud detection systems. Because it relies on the capacity of fraud detection systems to recognise cybercrime alerts, this method can be considered tactical rather than strategic.
Untrustworthy members of staff.	The abuse of administrator credentials is one of the most serious internal fraud threats facing South African financial institutions, because some highly trusted IT personnel and other associated staff will always require super-user profiles to complete their daily responsibilities or undertake important maintenance of core banking systems, therefore this represents an unavoidable source of difficulties.
The banking industry's unwillingness to share key information and their suspicions of cybercrime attacks with the SAPS.	SAPS officials claimed that the banking industry does not disclose information to the SAPS. However, as outlined in the Cybercrimes Bill, the ECT Act, and the POPI Act, all electronic communication service providers and financial institutions are expected to report cybercrime

	activities to the SAPS (Sections 24-30, 35, 45(3), 52, and 54 of the Cybercrimes Bill).
Banking clients' lack of knowledge and awareness.	SABRIC refers to an uptrend in vishing incidents. Vishing is when criminals contact bank customers and mislead them into thinking they are speaking with the bank or a legitimate service provider, then use social engineering tactics to trick them into disclosing their confidential bank card information as well as other personal information. There are thousands of phishing emails, which is a type of spam, are sent to banking clients' email accounts. The attackers employ forms on these fake websites to deceive victims into divulging their personal information. In a recent survey, a significant number of customers responded to fake emails, allowing their personal information to be obtained fraudulently.

Source: Researcher's analysis (2022)

6.3 The Effectiveness of Legislations against Cybercrime in the Banking Industry

The second aim of the study was to identify and examine cybercrime legislations with the objective of determining if they are effectively implemented to protect the banking industry, and this objective was achieved. All the SAPS officials agreed that the conviction rate of cybercriminals is low, thus the tendency to perpetrate cybercrime is high because these criminals face no penalties or legal retribution. Although some arrests have been made, there have not been many convictions owing to a lack of evidence to convict cybercriminals. This is emphasised by Loxton (cited in Business Tech, 2013:1), who is head of the Business Crime and Forensics unit at Werksmans. Loxton stated: "South Africa has been proven to be a particularly fertile ground for cybercrime due to it being a lawless society, with cybercrime syndicates knowing that law enforcement is paper thin, with low chances of being arrested and successfully convicted". Cassim (2011) mentions that most offenses prohibited by Section 86

of the ECT Act (Republic of South Africa, 2002) are punishable by a maximum of one year in prison, but crimes prohibited by Sections 86(4) and (5) (such as denial of service attacks) and those prohibited by Section 87 (extortion, fraud, and forgery) are punishable by a maximum of five years in prison. Therefore, to dissuade sophisticated cybercriminals from attacking the South African financial system, legislation has to be revised, particularly as harsher penalties and sanctions are required to deter cybercriminals.

The study also intended to examine policies that guide the implementation of cybercrime in the banking industry, and this objective was achieved. The SAPS officials highlighted some monitoring measures in the banking industry and the functioning of fraud departments in all banks. However, because there is no (or extremely limited) cooperation between these banks and the local SAPS to combat cybercrime, it continues to be an issue. The responses echoed the fact that the South African Banking Risk Information Centre (SABRIC) keeps track of any cybercrime that occurs in financial institutions in South Africa. However, in general, the banking industry's monitoring and reporting of cybercrime seems to be ineffective. Internally, SABRIC is a cybercrime oversight committee that monitors and assesses the impact of cybercrime activities. The banking industry reportedly discusses cybercrime strategies in meetings with SABRIC and determines whether they need to be revised in light of recent internal and external cybercrime events. But it is clear that SABRIC makes very slow progress in combating cybercrime as the latter is escalating virtually unabated. There is therefore still much work to be done, and cooperation among various stakeholders is critical if the goal of mitigating cybercrime in the banking industry is to be achieved.

6.4 Recommendations: The Banking Industry, SABRIC, and the SAPS

The recommendations that are offered emerged from the data analysis and the literature review. The recommendations are presented under seven categories, which are: (i) the implementation of effective internal processes in the banking industry, (ii) enhancing consumer awareness and the education of banking clients, (iii) the introduction and expansion of artificial intelligence (AI) in the banking industry, (iv) utilising blockchain to enhance security in the banking industry, (v) the employment of more qualified SAPS IT experts, (vi) the need for SABRIC to steer the continuous improvement of security measures in the banking industry; and (vii) the effective enactment and implementation of government policies and regulations.

6.4.1 More effective internal processes in the banking industry

According to Gould (2021), the infrastructure of the banking industry should not only be capable of supporting current business requirements, but it should also be constructed with the future in mind to allow for seamless updates that will enhance capacity and, even more crucially, security. To protect the banking industry against new cyber threats, banks' infrastructure should allow network and security teams to respond quickly to security incidents and provide consistent system maintenance, configuration, and software patching. Gould (2021) indicates that, to ensure that the infrastructure is secure and compliant with the industry's best practices and standards, it should be reviewed on a regular basis both internally and by third-party security assurance providers. This will provide insight into areas where the banking environment's security can be improved, thereby helping to protect banks against cyber threats.

The banking industry should also ensure strong data encryption and protect decryption keys, which is an important aspect of data security to assure the protection of this sensitive asset. To lessen the risk of account compromises, banks should enforce the usage of multi-factor authentication (MFA) for all user accounts, and this should be combined with other exceptional account security policies such as a strong password policy and an account lockout policy.

6.4.2 Enhancing consumer awareness and knowledge

According to Red Hat, Inc. (2019), the banking industry must ensure that clients are educated on how to protect themselves, as this is the most critical aspect of a satisfactory and secure banking experience. According to the Organisation for Economic Co-operation and Development (2005), financial education programmes should be developed to enable financial consumers to locate information regarding cybercrime and be aware of the drawbacks and risks associated with various types of this crime form. Furthermore, keeping customers informed about what to look for to protect their information and what to do in the event of a breach can help to improve the bank-customer relationship. As information evolves in response to new technologies and risks, keeping customers informed will go a long way towards attracting and retaining them. The banking industry should also explore the use of all available media for the delivery of educational messages connected to cybercrime to attain larger coverage and exposure. The banking industry should also take into account the various backgrounds and

languages of banking clients in South Africa, and should provide education programmes, or information dissemination initiatives, that are designed for specific sub-groups such as young people, university students, disadvantaged groups, the elderly, the disabled, and so forth (Organisation for Economic Co-operation and Development, 2005).

6.4.3 Artificial intelligence (AI) in the banking industry

AI can help the banking industry to manage massive amounts of high-speed data and can provide important insights. Furthermore, features like digital payments, AI bots, and biometric fraud detection systems can lead to high-quality services for a larger consumer base. Dumasia (2021:1) states: "AI comprises a broad set of technologies including, but not limited to, machine learning, natural language processing, expert systems, vision, speech, planning, robotics, etc.". By utilising data from previous threats and learning patterns and signs that appear unrelated to forecast and prevent assaults, AI can dramatically increase the effectiveness of cybersecurity systems in the banking industry. Apart from mitigating external risks, AI may also detect internal dangers or breaches and recommend corrective steps, thus preventing data theft and/or abuse.

6.4.4 Utilising blockchain to enhance security in the banking industry

Blockchain, as mentioned by Gupta (2017), is a collection of blocks that stores financial data in hash functions with a timestamp and a connection to the previous block. These blocks are anonymously shared with other network participants. This eliminates the possibility of cyber criminals exploiting centralised areas of weakness. Furthermore, earlier blocks in a blockchain cannot be changed and all transactional data are confirmed by all necessary stakeholders, making data manipulation extremely difficult.

According to Gupta (2017), the implementation of blockchain in the banking industry will lower the cost of online transactions while also boosting their validity and security. As a result, payment processors, custodians, and reconciling organisations are no longer required. These advantages may be the primary reason for the adoption of this technology by the banking industry. However, the benefits of blockchain technology will not only be confined to the protection of digital transactions, but blockchain will also benefit the financial IT infrastructure

that processes digital transactions because it provides many cybersecurity benefits to banking applications.

6.4.5 Appointing experts in the SAPS

The SAPS requires cybercrime task teams that are operational 24 hours a day, seven days a week, to conduct preventative investigations. According to Piet Pieterse, head of the Electronic Crime Unit of the SAPS (Mashiloane, 2014), a uniform South African version of a digital practice field guide is needed to enable all law enforcement officials to search, seize, secure (acquisition), and protect the evidential integrity of digital evidence (i.e., data storage devices). To be successful in the battle against cybercriminals, the SAPS needs expertise in sectors such as cybercrime, cyber-risk, fraud, and data analysis.

6.4.6 SABRIC to initiate continuous improvement in the banking industry

SABRIC is a committee that oversees cybercrime activity and is responsible for the banking industry's cybersecurity risk management initiatives. SABRIC is in partnership with a number of financial institutions in South Africa, including ABSA, African Bank, alBaraka, Bidvest Bank, Capitec, Citibank, Discovery, FNB, Nedbank, Postbank, Standard Bank, and Tyme Bank (SABRIC, 2018). According to Cossin and Hongze Lu (2021), SABRIC's cyber preparation is crucial because when cyber incidents occur in the financial industry, SABRIC must ensure that the necessary team is deployed to respond according to set protocols to minimise any negative outcomes. It should be highlighted that there is no one-size-fits-all answer to the problem of cybercrime. Therefore, any cyber preparation structure that is developed should be aligned with overall risk management policies and a business strategy while being amended on a regular basis, especially given the dynamic nature of cybercrime.

SABRIC should conduct penetration tests on a regular basis in the banking industry. According to Cossin and Hongze Lu (2021), a penetration test is a simulated cyberattack on a computer system aimed to find weaknesses in the banking industry's networks and applications. It is essentially a simulated hacker attack in which professional testers employ the same techniques as a criminal hacker to probe for flaws in a safe manner. A penetration test is used to assess the system's security and uncover both its strengths and vulnerabilities. The financial industry can quickly remedy any potential security gaps through a complete risk assessment, which will

allow for the detection of breaches and the recovery of crucial data and systems. SABRIC, as an oversight committee, should be attentive and actively interact with the financial sector as well as the SAPS in preparedness, detection, reaction, and disclosure initiatives because a cyberattack can occur at any given time.

6.4.7 Effective enactment of government policies and regulations

The banking industry demands government assistance in the fight against cybercrime. The government must implement and execute stricter laws that will result in heavier penalties for cybercriminals who are convicted. Cybercrime must be a major priority on the Information, Communication, and Technology (ICT) agenda in order to accomplish this goal. According to Sutherland (2017), given the importance of cybersecurity to human rights and the growth of the digital economy, government should develop methods to address the issue's cross-governmental and technical nature by, for instance, establishing a forum or panel of expert advisers and a mechanism for coordination among parliamentary portfolio committees.

6.5 Recommendations for Future Research

This study explored the cybercrime phenomenon in the banking industry in the study area through the lens of KwaZulu-Natal SAPS officials responsible for investigating cybercrime. Because the sample size was small, a larger sample size and purposively sampled individuals are needed to undertake a similar study in the future. Furthermore, because the study was conducted in KwaZulu-Natal only, the extent of the study was limited and additional research in other locations is required to validate or refute the findings. The following specific recommendations are offered:

- Qualitative research can be conducted on cybercriminal activities across financial institutions in South African through the lens of banking employees such as bank managers, the cybercrime division, the fraud division, and the information technology division.
- It is suggested that in-depth research should explore how banking institutions might work with the government, public sector, and private sector to develop and enforce laws associated with the Information Communications and Technology industry.

- Further research should also be conducted to determine which policies and laws banking industries in other countries have adopted to combat cybercrime and to determine their effectiveness in comparison with the South African context.
- Furthermore, research should be conducted to determine how to enhance cybercrime risk management involving data transfer through the use of the Internet, with the focus on security against cyberattacks.

6.6 Conclusion

Owing to the rapidly evolving and global nature of cybercrime, it is clear that the only effective way to combat it is for all role-players to cooperate and respond quickly and decisively to this threat. Africa is a developing region that has embraced digital transformation, but countries on this continent, particularly South Africa as one of its leading economies, must invest heavily to ensure cyberspace safety and security. In addition to incurring unprecedented financial costs, a cyber-incident can harm the image, brand, and market value of any financial sector. The development of an effective cybersecurity system will generate coordinated public-private sector actions that will, in turn, reduce cybercrime in the banking industry and accelerate the improvement of virtual space security in South Africa.

The banking industry should continuously devise and implement robust and stringent internal processes and systems to manage cybercriminal activity. This is critical in governing and guiding the execution of operations targeted at counteracting cybercrime. As information evolves in response to new technologies and risks, keeping customers informed will go a long way towards attracting and retaining them. The banking industry should explore the use of all available media for the delivery of awareness messages connected to cybercrime with the aim of attaining comprehensive coverage and information exposure.

It is clear that establishing cooperation among banking institutions, SABRIC, law enforcement agencies, and government agencies will generate real and updated statistics of cybercrime in the banking industry. Such data will enhance the effectiveness of investigations, both in terms of interaction models and increasing the level of trust among the private sector, government officials, and law enforcement officers. It is also critical for banks to protect themselves by constantly improving their fraud detection, mitigation, and control mechanisms through timely identification, investigation, and information exchange. This is required not only for bank

safety, but also for the stability and resilience of the entire financial industry. Moreover, maintaining stakeholder confidence and strengthening financial institutions' integrity will also be achieved. In conclusion, it must be reiterated that a strong foundation must be established in the banking industry by utilising robust information technology systems, framing effective policies and procedures, establishing strict compliance processes and high integrity standards, developing efficient monitoring capabilities, and taking swift and severe punitive action against cybercriminals.

REFERENCES

Acheson, J. (2002). Rational choice, culture change, and fisheries management in the Gulf of Maine. *Research in Economic Anthropology*, 21, 133-159.

Adams, J., Khan, H.T.A., Raeside, R., & White, D. (2007). *Research methods for graduate business and social science students*. London: Sage Publications.

African Union. (2018). *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection*. [Online]. Available at: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf. [Accessed on: 10 August 2021].

Aghatise, J. (2014). *Cybercrime definition*. [Online]. Available at: https://www.researchgate.net/publication/265350281_Cybercrime_definition. [Accessed on: 09 April 2020].

Ahmed, N. (2019). *Cyberstalking: A content analysis of gender-based offenses committed online*. (Master of Social Science dissertation), School of Applied Human Sciences, University of KwaZulu-Natal.

Akaranga, S.I., & Makau, B.K. (2016). Ethical considerations and their applications to research: A case of the University of Nairobi. *Journal of Educational Policy and Entrepreneurial Research,* 3(12), 1-9.

alBaraka Bank., (2021). *Protect yourself against increasing levels of cybercrime, warns al Baraka bank*. [Online]. Available at: https://www.albaraka.co.za/blogs/press-releases/protect-yourself-against-increasing-levels-of-cyber-crime-warns-al-baraka-bank. [Accessed on: 15 May 2022].

Allen, K. (2021). South Africa lays down the law on cybercrime. *Institute for Security Studies.* [Online]. Available at: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime. [Accessed on: 19 May 2021].

Alpaslan, A.F. (2010). *Social work research: A step-by-step guide on how to conduct your fourth year research project and write the research report: Only study guide for SCK4108*. Pretoria: University of South Africa.

Amadeo, K., (2021). What is banking?. *The Balance*. [Online]. Available at: https://www.thebalancemoney.com/what-is-banking-3305812. [Accessed on: 27 March 2021].

Anderson, G. (2015). *POPI: The race to data safety*. [Online]. Available at:

https://www.itweb.co.za/content/p6GxRKqYW1D7b3Wj. [Accessed on: 20 September 2021].

Aphane, M., & Mofokeng, J. (2021). South African Police Service capacity to respond to cybercrime: Challenges and potentials. *Journal of Southwest Jiaotong University*, 56(4), 1-22.

Arbak, E. (2005). Social status and crime. *GATE Working Paper No*. W.P.05-10

Asghari, H. (2010). *Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity*. Delft: University of Technology.

Babbie, E. (2008). *The basics of social research* (4th ed.). Belmont, CA: Wadsworth/Thomas Learning.

Babbie, E., & Mouton, J. (2001). *The practice of social research*. Cape Town: Oxford University Press.

Babbie, L. (2010). *Qualitative and quantitative research methods*. Chicago: Chicago University Press.

Bachman, R., & Schutt, R.K. (2015). *Fundamentals of research in Criminology and Criminal Justice* (3rd ed.). London: Sage Publications.

Banking Association South Africa (The). (n.d.). *Phishing scams*. [Online]. Available at: https://www.banking.org.za/consumer-information/bank-crime/. [Accessed on: 17 April 2022].

Barlow, D.H., & Durand, V.M. (2009). *Abnormal psychology: An integrative approach* (5th ed.). Belmont: Wadsworth Thomson Learning.

Barnes, J., Kroll, L., Burke, O., Lee, J., Jones, A. and Stein, A., (2000). Qualitative interview study of communication between parents and children about maternal breast cancer. *Bmj*, 321(7259), pp.479-482.

Bashir, M., Afzal, M.T. and Azeem, M., (2008). Reliability and validity of qualitative and operational research paradigm. *Pakistan journal of statistics and operation research*, pp.35-45.

Bestpractice.biz. (2020). *Bank admits employee sold data of 200 000 clients.* [Online]. Available at: https://bestpractice.biz/bank-admits-employee-sold-data-of-200000-clients/. [Accessed on: 16 April 2022].

Bezuidenhout, C. (2011). *Elementary research methods in Criminology*: *A Southern African perspective on Fundamental Criminology*. Cape Town: Pearson Education South Africa.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. Textbooks Collection Book 3. Available at: https://digitalcommons.usf.edu/oa_textbooks/3/. [Accessed on: 29 May 2020].

Bhengu, L. (2022). *ABSA engineer and wife accused of stealing over R100m from bank granted bail*. [Online]. Available at: https://www.news24.com/news24/southafrica/news/just-in-absa-engineer-and-wife-accused-of-stealing-over-r100m-from-bank-granted-bail-20220202. [Accessed on: 23 April 2022].

Bielski, L. (2000). Time to start biometrics. *American Bankers' Association Banking Journal*, 92(10), 54-59.

Blankenship, D.C. (2010). *Research and evaluation methods in recreation*. Leeds, United Kingdom: Human Kinetics.

Bocij, P. (2004). *Cyber stalking: Harassment in the Internet age and how to protect your family*. Wesport: Praeger.

Bond, M. (2015). Criminology: Rational choice theory explained. *LinkedIn*. [Online]. Available at: https://www.linkedin.com/pulse/criminology-rational-choice-theory-explained-mark-bond. [Accessed on: 15 February 2023].

Booysen, K. (2011). Economically motivated crimes: An overview. In C. Bezuidenhout (Ed.), *A Southern African perspective on Fundamental Criminology* (pp. 143-170). Cape Town: Pearson Education.

Bossler, A.M., & Holt, T.J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies and Management*, 35(1), 165-181.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P.M. Camic, D.L. Long, A.T. Panter, D. Rindskopf, & K.J. Sher (Eds.), *APA handbook of research methods in psychology* (Vol. 2, pp. 57-71). Washington, DC: American Psychological Association.

Brindley, C. (2020). Hackers on the dark web love South Africa. *Business Insider South Africa*. [Online]. Available at: https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6. [Accessed on: 16 March 2021].

Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime policing. *International Journal of Police Strategies & Management*, 29(3), 408-433.

Bryman, B., & Bell, E. (2011). *Business research methods* (3rd ed.). Oxford: Oxford University Press.

Budnik, K. (n.d.). *Building a united front on financial crimes in the financial services sector*. [Online]. Available at: https://www.pwc.co.za/en/press-room/cyber-security.html. [Accessed on: 10 April 2022].

Burns, N. & Grove, S.K. (2001). Introduction to qualitative research. *The practice of nursing research*. Conduct, critique and utilization, pp.67-68.

Business Tech. (2013). *South Africa is a cybercrime hot spot: FBI*. [Online]. Available at: https://businesstech.co.za/news/trending/48142/south-africa-is-a-cyber-crime-hot-spot-fbi/. [Accessed on: 25 April 2022].

Business Tech. (2020). *Beware these banking scams and fraud tactics in South Africa*. [Online]. Available at: https://businesstech.co.za/news/banking/458206/beware-these-banking-scams-and-fraud-tactics-in-south-africa/. [Accessed on: 23 April 2022].

Business Tech. (2021). *This type of banking fraud is becoming more common in South Africa*. [Online]. Available at: https://businesstech.co.za/news/technology/524850/this-type-of-banking-fraud-is-becoming-more-common-in-south-africa/. [Accessed on: 08 April 2022].

Buthelezi, L. (2021). ABSA informs more customers of data leak, 15 months later. *Fin24*. [Online]. Available at: https://www.news24.com/fin24/companies/absa-informs-more-customers-of-data-leak-15-months-later-20220124. [Accessed on: 15 April 2022].

Brady, S. and Heinl, C., (2020). *Cybercrime: Current Threats and Responses*. [Online]. Available at: https://www.justice.ie/en/JELR/Cybercrime_-_Current_Threats_and_Responses.pdf/Files/Cybercrime_-_Current_Threats_and_Responses.pdf. [Accessed on: 31 May 2022].

Bransen, J. (2001). Rational choice organisational theory. *International Encyclopaedia of the Social & Behavioural Sciences*, 12(19), 12751-12755.

Brush, K. Rosencrance, L and Cobb, M. (2021). *Cybercrime*. [Online]. Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime. [Accessed on: 15 June 2022].

Cambridge Dictionary. (n.d.). *Cyberspace*. [Online]. Available at: https://dictionary.cambridge.org/dictionary/english/ [Accessed on: 06 April 2020].

Cameron, L. (2022). *Future of digital forensics faces six security challenges in fighting*

borderless cybercrime and dark web tools. [Online]. Available at: https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime. [Accessed on: 22 April 2022].

Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, 44(1), 123-138.

Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 308, 719-731.

CliffCentral.com. (2022). *SABRIC features: Laws of life*. [Online]. Available at: https://cliffcentral.com/sabric-features-laws-of-life/. [Accessed on: 22 April 2022].

Cohen, L.E., & Felson, M. (1976). Social change and crime rate trends. *American Sociological Review*, 44, 588-605.

Cole, B. (2013). Cybercrime is real and it's here. *IOL News.* [Online]. Available at: https://www.iol.co.za/news/cyber crime-is-real-and-its-here-1583736. [Accessed on: 01 March 2021].

Comins, L. (2021). *FNB bank manager nabbed for allegedly stealing R4 million*. [Online]. Available at: https://www.thesouthafrican.com/news/breaking-fnb-manager-arrested-fraud-theft-hawks/. [Accessed on: 19 April 2022].

Cornish, D.B., & Clarke, R.V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. New Jersey: Transaction Publishers.

Cossin, D., & Hongze Lu, A. (2021). *Board oversight of cyber risks and cybersecurity*. [Online]. Available at: https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/. [Accessed on: 28 April 2022].

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology*, 44, 431-464.

Craig, N. (2021). Cybercrimes on the up, with SA annually losing about R2.2 billion. *IOL News*. [Online]. Available at: https://www.iol.co.za/sunday-tribune/news/cybercrimes-on-the-up-with-sa-annually-losing-about-r22-billion-974c9f5c-40f4-46fa-9a36-2ac9678463bb. [Accessed on: 28 January 2022].

Creswell, J.W. (2009). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Lincoln: Sage Publications.

Creswell, J.W. (2014). *Research design, qualitative, quantitative, and mixed methods approaches*. Los Angeles: Sage Publications.

Creswell, J.W. and Miller, D.L., (2000). Determining validity in qualitative inquiry. *Theory*

into practice, 39(3), pp.124-130.

Criminology theories. (2022). *Routine activities theory*. [Online]. https://criminal-justice.iresearchnet.com/criminology/theories/routine-activities-theory/ [Accessed on: 10 May 2021].

Criminology Web. (2022). Rational choice theory in Sociology and Criminology explained. *Criminology Web*. [Online]. Available at: https://criminologyweb.com/rational-choice-theory-in-sociology-and-criminology-explained/. [Accessed on: 16 February 2023].

Crow, I., & Semmens, N. (2008). *Researching Criminology* (xiith ed.). New York: Open University Press.

Da Silva, I.S. (2011). *Cybercrime increases worries: Vulnerable groups targeted*. [Online]. Available at: https://www.bizcommunity.com/Article/196/19/64855.html. [Accessed on: 1 February 2022].

De Angelis, G.D., & Sarat, A. (2000). Cybercrimes. In S. Sissing (Ed.), 2013. *A criminological exploration of cyberstalking in South Africa*. Pretoria: University of South Africa.

De Vos., A.S., Delport, C.S.L., Fouché, C.B., & Strydom, H. (2011). *Research at grass roots: A primer for the caring professions*. Pretoria: J.L. van Schaik Academic.

De Wet., J., & Erasmus, Z. (2005). Towards rigour in qualitative analysis. *Qualitative Research Journal*, 5(1), 27-40.

Dictionary.com. (2021*). Area of study*. [Online]. Available at: https://www.dictionary.com/browse/area-study. [Accessed on: 31 March 2021].

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges, and effective responses. *Cogent Social Sciences*, 5(1), 1675404.

Du Toit, R., Hadebe, P.N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: A South African context. *Acta Criminologica: Southern African Journal of Criminology*, 31 (3), 111-131.

Dumasia, J. (2021). *5 applications of artificial intelligence in banking*. [Online]. Available at: https://ibsintelligence.com/ibsi-news/5-applications-of-artificial-intelligence-in-banking/. [Accessed on: 26 April 2022].

Dutta, P., (2020). Surface Web and Dark Web: Exploring Layers of Web. *Kratikal*, April 27, 2020. [Online Blog]. Available at: https://www.kratikal.com/blog/surface-web-and-dark-web-exploring-layers-of-web/. [Accessed on: 22 March 2022].

Furnell, S., (2002). *Cybercrime: Vandalizing the information society* (pp. 3-540). London:

Addison-Wesley.

Francis, P. (2011). Planning criminological research. In P. Davies, P. Francis, & V. Jupp (Eds.), *Doing criminological research* (2nd ed.). London: Sage Publications.

Gereda, S L., (2006), 'The Electronic Communications and Transactions Act' in Thornton, L (ed.) *Telecommunications Law in South Africa*, pp. 262-294.

Giles, J. (2009). *ISPs: When and when not to reveal information of your client.* [Online]. Available at: https://www.michalsons.com/blog/isps-when-and-when-not-to-reveal-information-on-your-client/1176. [Accessed on: 10 April 2022].

Glass, G. V. (2004). Analysis of data on the time-series quasi-experiment. *Law and Society Review*, 3(1), 55−75.

Global Economic Crime Survey. (2016). Adjusting the Lens on Economic Crime. *PwC*. [Online]. Available at: https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf. [Accessed on: 31 May 2021].

Global Provider of Secure Financial Messaging Services (The). (2019). *Modus operandi of a cyberattack*. [Online]. Available at: https://www.swift.com/news-events/news/modus-operandi-cyber-attack. [Accessed on: 18 April 2022].

Gordon, B. (2002). Hacking, denial of service and the Electronic Communications and Transactions Act. *Servamus,* 34.

Goredema, C. (2012). *Predatory cybercrime in South Africa: Current risks and realities*. Cape Town: Institute for Security Studies.

Gould, M. (2021). *How can banks protect themselves from cyberattacks?* [Online Blog]. Available at: https://blog.nettitude.com/how-can-banks-protect-themselves-from-cyber-attacks. [Accessed on: 26 April 2022].

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. *Crime and the Internet*. Routledge, Taylor & Francis Group: London, pp. 29-43.

Grobler, M., & Bryk, H. (2010). *Common challenges faced during the establishment of a CSIRT*. Pretoria: CSIR.

Grobler, M., Jansen van Vuuren, J., & Zaaiman, J. (2013). Preparing South Africa for cybercrime and cyber defence. *Systemics, Cybernetics and Informatics*,11 (7). 1690-4524.

Grobler, M., & Jansen van Vuuren, J. (2007). *Combating cyberspace fraud in South Africa*. [Slides]. Council for Scientific and Industrial Research.

Gupta, S. (2017). *How blockchain technology is changing the security landscape in the*

banking sector. [Online]. Available at: https://economictimes.indiatimes.com/small-biz/security-tech/technology/how-blockchain-technology-is-changing-the-security-landscape-in-the-banking-sector/articleshow/60981747.cms?from=mdr. [Accessed on: 26 April 2022].

Gwala, S. (2016). *Barriers to implementation of the (SA) national cybersecurity policy framework*. (Master's dissertation), University of Johannesburg. Wits Institutional Repository Environment on DSpace.

Harry, H. (2002). E-fraud: Current trends and international developments. *Journal of Financial Crime*, 9(4), 347-354.

Henning, E., van Rensburg, W., & Smit, B. (2004). *Finding your way in qualitative research*. Pretoria: Van Schaik.

Herselman, M., & Warren, M. (2010*). Issues in information and technology: Cybercrime influencing business in South Africa*. [Online]. Available at: https://www.semanticscholar.org/paper/Cyber-crime-influencing-businesses-in-South-Africa-Herselman-Warren/60f3bcc9f457d57297b25701c239704c979e0c5b [Accessed on: 21 February 2021].

Higgins, G.E. (2009). Quantitative versus qualitative methods: Understanding why quantitative methods are predominant in Criminology and Criminal Justice. *Journal of Theoretical & Philosophical Crimin*ology, 1(1), pp. 23-37.

Hinduja, S., & Patchin, J.W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behaviour*, 29, 129-156.

Hitchcock, J.A., & Page, L. (2006). *Net crimes and misdemeanours: Out-manoeuvring web spammers, stalkers, and con artists* (2nd ed.). New Jersey: Cyber Age Books.

Holt, T., & Bossler, A.M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Abingdon, Oxon: Routledge.

Holt, T.J., Bossler, A.M., & Seigfried-Spellar, K.C. (2015). *Cybercrime and digital forensics: An introduction*. London: Routledge.

Holt, T., Bossler, A.M., & Spellar, S.K. (2015). *Cybercrime and digital forensics*. Abingdon, Oxon: Routledge.

Holt, T.J., Burruss, G.W., & Bossler, A.M. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society*, 29(8), 906-921.

How can banks protect themselves from cybercrime?. (2015). *eNCA*. Available at:

https://www.enca.com/technology/what-should-banks-be-doing-protect-themselves-cybercrime. [Accessed on: 15 April 2022].

Ibikunle, F., & Eweniyi., O. (2013). Approach to cyber security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science, Engineering and Education*, (1)1, pp.1-11.

Ikdal, A., (2017). 6 challenges to financial inclusion in South Africa. *World Economic Forum*. [Online]. Available at: https://www.weforum.org/agenda/2017/04/financial-inclusion-south-africa/. [Accessed on: 27 March 2021].

Introduction to Rational Choice Theory in Social Work. (2022). *Online MSW Programs*. Available at: https://www.onlinemswprograms.com/social-work/theories/rational-choice-theory/#.[Accessed on: 14 February 2023].

Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River. NJ: Prentice Hall.

Jaishankar, K. (2018). Space transition theory simplified. *LinkedIn*. [Online]. Available at: https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar. [Accessed on: 16 February 2023].

Jones, J.A. (2012). Ethical considerations in criminal justice research: Informed consent and confidentiality. *Inquiries Journal/Student Pulse*, 4. [Online]. Available at: https://www.inquiriesjournal.com/a?id=674. [Accessed on: 10 April 2020].

Kader, S., and Minnaar, A. (2015). Cybercrime investigations: Cyber-process for detecting cybercriminal activities, cyber-intelligence and evidence gathering. *ACTA Criminologica*, 4(6), 123-134.

Kaushik, T. (2019). *Cyber criminals hide in the 'dark web' to remain anonymous*. [Online]. Available at: https://economictimes.indiatimes.com/tech/internet/cyber-criminals-hide-in-the-dark-web-to-remain-anonymous/articleshow/69139795.cms. [Accessed on: 15 April 2022].

Kawulich, B.B., (2005). Participant observation as a data collection method. In *Forum qualitative sozialforschung/forum: Qualitative social research*. Vol. (6), No. 2.

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of Bitcoin in Darknet markets: Examining facilitative factors on Bitcoin-related crimes. *American Journal of Criminal Justice*. doi:10.1007/s12103-017-9394-6.

Kgosana, R. (2018). *Cybercrime costs SA almost R2.2bn a year.* [Online]. Available at:

https://citizen.co.za/news/south-africa/crime/2047717/cybercrime-costs-sa-almost-r2-2bn-a-year/. [Accessed on: 18 March 2020].

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4), 470-486.

Kilian, A. (2017*).* Cybercrime becoming a major threat in South Africa. *Engineering News*, 19 September. [Online]. Available at: https://engineeringnews.co.za/article/cybercrime-becoming-amajor-threat-in-south-africa-2017-09-19. [Accessed on: 06 April 2020].

Kodellas, S., Fisher, B.S., & Wilcox, P. (2015). Situational and dispositional determinants of workplace victimization: The effects of routine activities, negative affectivity, and low self-control. *International Review of Victimology*, 21(3), 321-342.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, 24(1), 120-124.

Kubayi, M. (2017). *Cybersecurity. Department of Telecommunications and Postal Services & SABRIC briefing, with Deputy Minister present*. [Online]. Available at: https://pmg.org.za/committee-meeting/24042/. [Accessed on: 19 April 2022].

Kufa, M., (2008). Cybersurfing without boundaries. *De Rebus*, December, 20.

Kumar, R. (2005). *Research methodology: A step-by-step guide for beginners* (2nd ed.). London: Sage Publication.

Kumar, R. (2011). *Research methodology: A step-by-step guide for beginners.* London: Thousand Oaks; Calif: Sage Publications.

Kvale, S. & Brinkmann, S. (2015). *Interviews: Learning the craft of qualitative research Interviewing* (3rd ed.). California: Sage Publications.

Lambert, K. (2018). *Protecting financial institutions from DDoS attacks*. [Online]. Available at: https://www.imperva.com/blog/protecting-financial-institutions-from-ddos-attacks/. [Accessed on: 10 March 2021].

Leal, J., (2008). *E-learning and online education: implications for the future of law enforcement training*. Sacramento: California Commission on Peace Officer Standards and Training.

Lee, J.R., Holt, T.J, Burruss, G.W., & Bossler, A.M. (2019). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review*, 31 (1), pp. 1-20.

Leedy, P.D., (1997). *Practical research: Planning and design* (6th Edition). New Jersey:

Prentice-Hall.

Leukfeldt, E.R., & Yar, M. (2016*).* Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour*, 37(3), 263-280.

Lincoln, Y., & Guba, E. (1999). Establishing trustworthiness. In: A. Bryman & R.G. Burgess (Eds.), *Qualitative research.* London: Sage Publications.

Majola, G., (2021). *Banking sector sees hike in criminal incidents amid Covid-19.* [Online]. Available at: https://www.iol.co.za/business-report/economy/banking-sector-sees-hike-in-criminal-incidents-amid-covid-19-5ac126c6-5575-4658-aa97-3a4be01ac4e8. [Accessed on: 01 June 2022].

Maliba, A. (2021). *The scary nature of cybercrimes and the strain of bringing perpetrators to book.* [Online]. Available at: https://www.iol.co.za/sundayindependent/news/the-scary-nature-of-cybercrimes-and-the-strain-of-bringing-perpetrators-to-book-7faee4e6-a180-4649-8ab5-40ad0590bc91. [Accessed on: 3 April 2021].

Malinga, S. (2019). *Fraudsters also prefer digital banking*. [Online]. Available at: https://www.itweb.co.za/content/nWJad7b89rVqbjO1. [Accessed on: 12 April 2022].

Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures*. Unpublished DPhil thesis. Gower Publishing Company: England.

Mannan, M., & Van Oorschot, P.C. (2008). *Security and usability: The gap in real-world online banking*. In Proceedings of the 2007 Workshop on New Security Paradigms, pp. 1-14.

Maree, K., & van Der Westhuizen, C. (2013). Planning a research proposal. In K. Maree (Ed.), *First steps in research*. Pretoria: Van Schaik.

Mashiloane, L. (2014). *Piet Pieterse: SAPS intensifies cybercrime battle*. [Online]. Available at: https://www.itweb.co.za/content/x4r1ly7RQl1vpmda. [Accessed on: 26 April 2022].

Maxfield, M.G., & Babbie, G. (2008). *Basics of research methods for Criminal Justice and Criminology*. Boston, US: Cengage Learning.

Maxfield, M.G., & Babbie, E.R. (2015). *Research methods for criminal justice and criminology* (7th ed.). United States of America: Cengage Learning.

McConnell International. (2000). *Cyber Crime and Punishment? Archaic Laws Threaten Global Information*. [Online]. Available at: https://uh.edu/tech/cisre/resources/ia-resources/_files/7033/Week12/cybercrime.pdf. [Accessed on: 03 July 2021].

Meta Compliance Marketing Team. (2019). *How do hackers normally get caught?*

[Online]. Available at: https://www.metacompliance.com/blog/how-do-hackers-normally-get-caught/. [Accessed on: 23 April 2022].

Mofokeng, J.T., & De Vries, I. (2016). Anti-fraud training in the South African Police Service (SAPS): A strategic perspective. *International Journal of Social Sciences and Humanity Studies*, 8(1), 84-102.

Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S., (2014). Social engineering attack framework. *In 2014 Information Security for South Africa* (pp. 1-9). IEEE: United States.

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime: The emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences,* 7 (3), pp.1-9. Rome, Italy: MCSER Publishing.

Mugenda A.G. (2011). *Social science research methods: Theory and practice*. Nairobi: ARTS Press.

Mungadze, S. (2019). *SA needs effective laws to curb cybercrime, say experts*. [Online]. Available at: https://www.itweb.co.za/content/G98YdMLxjQRMX2PD. [Accessed on: 10 April 2020].

Mwaita, P., & Owor, M. (2013). *Workshop report on effective cybercrime legislation in Eastern Africa*. Dar Es Salaam, Tanzania: Council of Europe.

Naidoo, S. (2018). *Cybercrime is advancing fast*. [Online]. Available at: https://www.iol.co.za/weekend-argus/news/cyber-crime-is-advancing-fast-18516412. [Accessed on: 07 April 2020].

Net Guardians. (2021). *eBook: A-Z of Internal Banking Fraud*. [Online]. Available at: https://netguardians.ch/internal-banking-fraud/. [Accessed on: 19 April 2022].

Neuman, W. L. (2003). *Social research methods: Qualitative and quantitative approaches* (4th ed.). Boston: Allyn & Bacon.

Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime.* Cullompton: Willan Press.

Neuman, W.L. (2014). *Social research methods: Qualitative and quantitative approaches.* London: Pearson Education.

Njotini, M., (2019). Information and Communication Technology Law, in DP Van Der Merwe, D.P, Roos, A, Pistorius, T., Eiselen, G.T.S. & Nell, S.S. (Eds.). *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg, 2019*(2), pp.420-423.

Norton Cybercrime Report. (2011). Cybercrime report, *Opswat*, September 22, 2011. [Blog].

Available at: https://www.opswat.com/blog/2011-norton-cybercrime-report. [Accessed on: 24 April 2022].

Obeng-Adjei, A. (2017). *Analysis of cybercrime activity: Perceptions from a South African financial bank*. (Coursework Master's dissertation in Commerce on Information Systems), School of Economic and Business Sciences, University of Witwatersrand.

Okonigene, R. E., & Adekanle, B. (2009). Cybercrime in Nigeria. *Business Intelligence Journal*, 3(1), pp.15-17.

Oladipo, T. (2015). Cybercrime is the next big threat experts warn. *BBC*. Monitoring African Security Correspondent. Available at: https://bbc.com/news/ world-africa-34830724/. [Accessed on: 26 February 2021].

Opland, R., & Moodley, T. (2013). *What happens if we violate PoPI?* [Online]. Available at: https://www.ey.com/Publication/VWLUAssets/What-happens-if-we-violate-PoPI/$FILE/130522%20Privacy%20Thought%20Leadership%202.pdf. [Accessed on: 28 February 2021].

Organisation for Economic Co-Operation and Development (OECD). (2005). *Recommendation on principles and good practices for financial education and awareness*. Paris: Directorate for Financial and Enterprise Affairs.

Organisation for Economic Co-operation and Development (OECD). (2007). *Malicious software malware: A security threat to the Internet economy.* South Korea: Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy.

Pillay, L. (2016). *Get a head start on PoPI with these 5 tips*. [Online]. Available at: https://www.itnewsafrica.com/2016/01/get-a-head-start-on-popi-with-these-5-tips/. [Accessed on: 12 March 2021].

Polit, D. F., & Beck, C. T. (2004). *Nursing research: Principles and methods.* (7th ed.). Philadelphia, PA: Lippincott, Williams & Wilkins.

PwC South Africa. (2018). *Building a united front on financial crimes in the financial services sector*. [Online]. Available at: https://www.pwc.com/mt/en/publications/united-front-financial-crimes-2018-pwc.pdf. [Accessed on: 10 April 2022].

Raghavan, A.R., & Parthiban, L. (2014). The effect of cybercrime on a bank's finances. *International Journal of Current Research and Academic Review*, 2(2), 2347-3215.

Red Hat, Inc. (2019). *What is financial services security (and compliance)?* [Online].

Available at: https://www.redhat.com/en/topics/security/security-and-compliance-financial-services. [Accessed on: 26 April 2022].

Republic of South Africa. (1965). Civil Procedure and Evidence Act No. 25 of 1965. *Government Gazette No. 1066*. Cape Town: Government Printer.

Republic of South Africa. (1983). Computer Evidence Act No. 57 of 1983. *Government Gazette No. 13819*. Cape Town: Government Printer.

Republic of South Africa. (2015a). *Cybercrimes and Cybersecurity Bill Draft for Public Comment*. [Online]. Available at: https://www.justice.gov.za/legislation/invitations/Cyber CrimesBill2015.pdf. [Accessed on: 07 April 2020].

Republic of South Africa. (2015b). Cybercrime and Cybersecurity Bill Notice 878 of 2015. *Government Gazette No. 39161*. Cape Town: Government Printer.

Republic of South Africa. (2016). *Cybercrime and Cybersecurity Bill, B6-2017*. [Online]. Available at: https://www.gov.za/sites/default/files/b6-2017_cybercrimes_ 170221_a.pdf. [Accessed on: 09 April 2020].

Republic of South Africa. (2005). Electronic Communications and Transactions Act 25 of 2005. *Government Gazette No. 23708*. Cape Town: Government Printer.

Republic of South Africa. (2001). Financial Intelligence Centre Act No. 38 of 2001. *Government Gazette No. 22886*. Cape Town: Government Printer.

Republic of South Africa. (1992). Interception and Monitoring Prohibition Act No. 127 of 1992. *Government Gazette No. 35821*. Cape Town: Government Printer.

Republic of South Africa. (1998). Prevention of Organized Crime Act No. 121 of 1998. *Government Gazette No. 19553*. Cape Town: Government Printer.

Republic of South Africa. Department of Justice. (2013). Protection of Personal Information Act No. 4 of 2013. *Government Gazette No. 37067.* Cape Town: Government Printer.

Rosewarne, C. (2012). *The 2012/3 SA cyber threat barometer*. [Online] Available at: https://www.bic-trust.eu/files/2012/10/SA-2012-Cyber-Threat-Barometer_Medium_res.pdf. [Accessed on: 17 March 2020].

Rubin, H.J., & Rubin, S.I. (2012). *Qualitative interviewing* (3rd ed.). California: Sage Publications.

Sabinet Law. (2017). *Cybercrimes and cybersecurity*. [Online]. Available at: https://www.sabinetlaw.co.za/justice-and-constitution/legislation/cybercrimes-andcybersecurity. [Accessed on: 08 April 2020].

Sanders, S. (2020). *Cybersecurity protection for bank customers starts with awareness*.

[Online]. Available at: https://www.bai.org/banking-strategies/article-detail/cybersecurity-protection-for-bank-customers-starts-with-awareness/. [Accessed on: 15 April 2022].

Sarrab, M., Aldabbas, H., & Elbasir, M. (2013). Challenges of computer crime investigation in North African countries. *The International Arab Conference on Information Technology*. Aero Association of the California Institute of Technology: United States.

Schmalleger, F., & Pittaro, M. (2008). *Crimes of the Internet* (1st ed.). United States: Prentice Hall Press.

Schultz, C.B. (2017). *Cybercrime: An analysis of current legislation in South Africa*. (Master's Dissertation in LLM Mercantile Law), Faculty of Law, University of Pretoria.

Shinder, D. (2011). *What makes cybercrime laws so difficult to enforc*e? Tech Republic, 26 January. [Online]. Available at: https://www.techrepublic.com/blog/it-security/what-makescybercrime-laws-so-difficult-to-enforce/. [Accessed on: 10 April 2020].

Shneiderman, S.B., & Plaisant, C. (2005). *Designing the user interface* (4th ed.). Boston, MA: Pearson Addison Wesley.

Shuttleworth, M. (2008). *Definition of research*. [Online]. Available at: https://explorable.com/definition-of-research. [Accessed on: 29 September 2020].

Siegel, L.J. (2011). *Criminology: The core* (4th ed.). Belmont: Wadsworth: Cengage Learning.

Sissing, S. (2013). *A criminological exploration of cyberstalking in South Africa*. (Dissertation for Master of Arts), University of South Africa, Pretoria.

Smal, D. (2022). *Financial firms increasingly targeted by cybercriminals*. [Online]. Available at: https://www.moneyweb.co.za/news/tech/financial-firms-increasingly-targeted-by-cybercriminals. [Accessed on: 20 April 2022].

Snail, S., (2009). Cyber crime in South Africa–Hacking, cracking, and other unlawful online activities. *Journal of Information, Law and Technology*, 1, pp.2009-1.

Solak, D., & Topaloglu, M. (2015). The perception analysis of cybercrimes in view of computer science students. *Procedia: Social and Behavioural Sciences*, 182, 590-595. [Online]. Available at: https://core.ac.uk/download/pdf/82258715.pdf. [Accessed on: 07 April 2020].

South African Banking Risk Information Centre (SABRIC). (2014). *Card fraud*. [Online].

Available at: https://www.sabric.co.za/media/1141/final-card-booklet.pdf. [Accessed on: 23 March 2020].

South African Banking Risk Information Centre (SABRIC). (2018). *Annual crime stats*. [Online]. Available at: https://www.sabric.co.za/annual-crime-stats-2018.pdf. [Accessed on: 31 July 2020].

South African Banking Risk Information Centre (SABRIC). (2020). *Annual crime stats*. [Online]. Available at: https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2020/. [Accessed on: 31 July 2021].

South African Police Service. (2006). *National Instruction 1/2006: Research in the Service*. Strategic Management: Management Services. Issues by Consolidation Notice 2/2006. Pretoria: South African Police Services.

South African Police Service. (2015). *Crime statistics 2015*. [Online]. Available at: https://www.saps.gov.za/resource_centre/publications/statistics/crimstats/2015/crime_stats.pp. [Accessed on: 09 April 2020].

Spyridon, S. (2012). *Insider fraud and routine activity theory*. [Online]. Available at: https://eprints.lse.ac.uk/50344/1/Samonas_Insider_fraud_routine_2013.pdf. [Accessed on: 07 April 2020-04-10].

SQN Banking Systems. (n.d.). *9 strategies to protect your bank from internal fraud*. [Online]. Available at: https://sqnbankingsystems.com/blog/9-strategies-to-protect-your-bank-from-internal-fraud/. [Accessed on: 17 April 2022].

Standard Bank. (2021). *How to protect your business from cybercrime*. [Online]. Available at: https://www.standardbank.co.za/southafrica/business/bizconnect/help-me-manage-my-business/guides/how-to-protect-your-business-from-cybercrime. [Accessed on: 18 April 2022].

Statistics South Africa. (2019). *Mid-year population estimates*: *Statistical release*. Pretoria: Statistics South Africa. Available at: https://www.statssa.gov.za/publications/P0302/P0322019.pdf. [Accessed on: 30 July 2020].

Steyn, J. (2013). *Assignment Writing*. Pretoria: Van Schaik Publishers.

Strydom, H. (2009). *Ethical aspects of research in the caring professions.* In A.S. De Vos, H. Strydom, C.B. Fouché, M. Poggenpoel, & E.M. Schurink. *Research at grass roots a premier for the caring professions*. Pretoria: Van Schaik.

Suler, J. (2005). *The psychology of cyberspace*. [Online]. Available from:

https://users.rider.edu/~suler/psycyber/psychspace.html. [Accessed on: 07 April 2020].

Sulfab, M., (2014). Challenges of cybercrime in South Africa. *Research paper for Master of Arts in National Security Studies*. American Military University: United States.

Sutherland, E. (2017). Governance of cybersecurity: The case of South Africa. *The African Journal of Information and Communication*, 20, 83-112.

Terre Blanche, M., & Painter, D. (2006). *Research in practice* (2nd ed.). Cape Town: University of Cape Town Press.

Thomas, D., & Loader, B., (2001), Cybercrime: law enforcement, security and surveillance in the information age, *Semantic Scholar*, 30 (1), 149-188.

Tibbetts, S.G. and Hemmens, C., (2009*). Criminological theory: A text/reader*. Sage: California.

United Nations Economic Commission for Africa. (2014). *Tackling the challenges of cybersecurity in Africa*. Addis Ababa, Ethiopia: Commission for Africa.

United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive Study on Cybercrime.* [Online]. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed on: 4 March 2021].

Uys, H. H. H & Basson, A. A. (1991). *Research methodology in nursing*. Pretoria: Kagiso

Van der Merwe, D. (2014). A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 17(1), 297-327.

Van der Westhuizen, H. (2019). *New Bill offers robust game plan against cybercrime in South Africa*. [Online]. Available at: https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/. [Accessed on: 07 April 2020].

Van Rensburg, K.S.J., (2017). *The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa*. (Doctoral dissertation). University of South Africa.

Verdegem, P., Teerlinck, E., & Vermote, E. (2015). Measuring cost and impact of cybercrime in Belgium. *BCC D.3.1.1. Risk perception monitor report* (1st wave, 2015). Ghent.

Von Solms, B. (2015). What is SA doing to tackle cybercrime? The conversation. *Fin24.com.* University of Johannesburg. [Online]. Available at: https://www.fin24.com/Tech/Opinion/What-is-SA- doing/. [Accessed on: 05 March 2021].

Vrancianu, M., & Popa, L. A. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. *The Amfiteatru Economic Journal*, 1228: 388-403.

Wahidin, A., & Moore, L. (2011). Ethics and criminological research. In P. Davies, P. Francis, & V. Jupp (Eds.), *Doing criminological research* (2nd ed.). London: Sage Publications.

Wassenaar, D.R. (2006). Ethical issues in social science research. In M. Terre Blanche, K. Durkheim, & D. Painter (Eds.), *Research in practice: Applied methods for the social sciences*. Cape Town: University of Cape Town Press.

Watney, M.M., (2012). *Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position,* Presented at Cyber Crime Africa. Monte Casino.

Whitney, L. (2021). *How banks and banking customers can protect themselves against financial crimes*. [Online]. Available at: https://www.techrepublic.com/article/how-banks-and-banking-customers-can-protect-themselves-against-financial-crimes/ [Accessed on: 24 April 2022].

Wickert, C. (2020). *Routine activity theory (RAT).* [Online]. Available at: https://soztheo.de/theories-of-crime/rational-choice/routine-activity-theory-rat/?lang=en. [Accessed on: 14 February 2023]

Widsup, S., Spitter, M., Hylender, D., & Basset, G. (2018). *Verizon data breach: Investigations report*. [Online]. Available at: https/www.researchgate.net.publication/32445340_2018-verizon-data-breach-investigationreport [Accessed on: 04 March 2021].

Wright, P. (2009). *Rational choice theory.* Boston: Harvard Press.

Yar, M. (2006). *Cybercrime and society*. London: Sage Publications.

Yedaly, M., Amazouz, S., & Yankey, A. (2016). *Cybercrime and cyber security trends in Africa*. USA: Symantec Corporation.

APPENDICES

ANNEXURE A: Gatekeeper Permission Letter

University of Kwa-Zulu Natal
238 Mazisi Kunene Road
Glenwood
Durban
South Africa

South African Police Service
15 Bram Fischer Road
Durban Central
Durban
4001

02 August 2021

Dear Sir/ Madam

REQUEST FOR PERMISSION TO CONDUCT RESEARCH

My name is Perushka Pillay and I am a University of Kwa-Zulu Natal student at the Howard College Campus. The research I wish to conduct is for a master's dissertation. My study is entitled: "A criminological analysis of the commission of cybercrime in the South African Banking Industry: A case study of cybercrime in banks in Durban, KwaZulu-Natal". Due to the improvement and development in technology, societies have seen an increasing number of individuals with devices and smart phones that are simply connected online. Therefore, many South Africans using digital banking platforms are targets for savvy cyber criminals. At present, there is a paucity of data in terms of cybercrime that in available in South Africa and within financial institutions. When a cybercrime is committed, victims often find themselves confused as to what to do, as well as what is the potential legal action available to them. This research would shed light specifically on financial institutions regarding cybercrime.

I am hereby seeking your consent to conduct research for a master's dissertation. The participants whom I wish to interview and obtain data from should comprise of SAPS officials. The participants can be anyone that investigates cybercrime from detectives or investigators, or/and so forth. For the purpose, of this study, the researcher will focus specifically on KwaZulu Natal. In this study, all the participants will be made aware of their individual rights to choose whether they would like to participate. The choice will be entirely up to the

participant and they should not feel obligated to participate in the study in any way. Confidentiality will always be maintained and names of participants will not be disclosed.

This research is based solely for academic purposes and the researcher will present the research findings to the University of Kwa-Zulu Natal. This study sees no intent or benefit by accusing role players, but seeks merely to investigate the phenomenon, nature and legal protective measures as mentioned in literature and by legal experts. If you require any further information, kindly contact me on 081 472 2965/ 031 469 2358. My email address is 213562910@stu.ukzn.ac.za. I hope my request is successful.

My supervisor is Ms Precious Nolwazi Ntuli who is located at the School of Applied Human Sciences, College of Humanities, Pietermaritzburg Campus of the University of Kwa-Zulu Natal. Contact details: Email address: NtuliP@ukzn.ac.za. Phone number: 033 260 6572.

Thank you for your time and consideration in this matter.

Yours Sincerely
Perushka Pillay

ANNEXURE B: Informed Consent Letter

Applied Human Sciences,
College of Humanities,
University of KwaZulu-Natal,
Howard College Campus

Dear Participant

INFORMED CONSENT LETTER

My name is Mrs Perushka Pillay, I am a master's candidate studying at the University of KwaZulu-Natal, Howard College Campus, South Africa. My study is entitled: "A criminological analysis of the commission of cybercrime in the South African Banking Industry: A case study of cybercrime in banks in Durban, KwaZulu-Natal". South African Banking Risk Information Centre (SABRIC) said South Africa has the third-highest figure of cybercrime victims worldwide, losing around R2,2 billion a year to cyber-attacks. At present, there is a paucity of data in terms of cybercrime that is available in South Africa and within financial institutions. As indicated by the South African Banking Risk Information Centre (SABRIC) report (2014), 75% of fraud that occurred in South African banks was credited to cybercrime schemes. This study therefore, seeks to analyse the causes of cybercrime activities within banks, in specific the lack of qualified technicians and fraud experts within the industry. This research would shed light specifically on financial institutions regarding cybercrime.

Please note that:

- Your confidentiality is guaranteed as your inputs will not be attributed to you in person but reported only as a population member opinion.
- The interview may last for about 25-35 minutes and may be split depending on your preference.
- Any information given by you cannot be used against you, and the collected data will be used for purposes of this academic research only.
- Data will be stored in secure storage and destroyed after 5 years.
- You have a choice to participate, not participate or stop participating in the research. You will not be penalized or held responsible in any way for taking such an action.
- The research aims are to establish the causes of the increased rate of cybercrime as well as to identify and examine cybercrime legislations that has been implemented for financial industries in South Africa.

- Your involvement is purely for academic purposes only, and there are no financial benefits involved.
- This research is based solely for academic purposes and the researcher will present the research findings to the University of Kwa-Zulu Natal. This study sees no intent or benefit by accusing role players, but seeks merely to investigate the phenomenon, nature and legal protective measures as mentioned in literature and by legal experts.
- If you are willing to be interviewed, please indicate (by ticking as applicable) whether, or not you are willing to allow the interview to be recorded by the following equipment:

	Willing	Not willing
Audio equipment		

I can be contacted at:
Email address: 213562910@stu.ukzn.ac.za.
Phone number: 081 472 2965.

My supervisor is Ms Precious Nolwazi Ntuli who is located at the School of Applied Human Sciences, College of Humanities, Pietermaritzburg Campus of the University of KwaZuluNatal. Contact details:
Email address: NtuliP@ukzn.ac.za.
Phone number: 033 2606572.

You may also contact the Research Office through:
HSSREC Research Office,
Contact details:
E-mail address: Hssrec@ukzn.ac.za.
Phone number: 031 260 8350/ 4557/ 3587.

ANNEXURE C: Interview Schedule Guide

A CRIMINOLOGICAL ANALYSIS OF THE COMMISSION OF CYBERCRIME IN THE SOUTH AFRICAN BANKING INDUSTRY: A CASE STUDY OF CYBERCRIME IN BANKS IN DURBAN, KWAZULU-NATAL.

Objective 1: Establish the causes of the increased rate of cybercrime in banks

1. What is the general understanding of cybercrime as a phenomenon in the banking industry?

2. What types of cyber-related crimes are committed, who commit/s them, how do they happen, and when do these crimes occur?

3. What are the most prevalent methods used by cybercriminals to perpetrate cybercrime?

4. What are banks' perspectives on the root cause of cybercriminal activities based on current trends in cybercrime?

Objective 2: To identify and examine cybercrime legislations that have been implemented for financial institutions in South Africa

5. What is the conviction rate for cybercriminals?

6. Have there been any convictions for these crimes, and when were the perpetrators discovered?

7. Do financial institutions have a profile of cybercriminals?

Objective 3: To examine the policies that guide the implementation of cybercrime in the banking industry

8. Do any monitoring and reporting of cybercrime activities occur in the banking industry?

9. Are there any oversight committees in place to monitor and evaluate the effectiveness of cybercrime interventions in the banking industry?

10. What steps are currently being taken by banks to combat cybercrime?

11. Is there anything that you would like to elaborate on, or is there any final comment that you would like to make before we conclude?

ANNEXURE D: South African Police Service Approval Letter

South African Police Service — Suid-Afrikaanse Polisiediens

Privaatsak Private Bag X94	Pretoria 0001	Faks No. Fax No.	(012) 334 3518

Your reference/U verwysing:

My reference/My verwysing: **3/34/2**

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: **Lt Col Joubert**
AC Thenga
Tel: **(012) 393 3118**
Email: **JoubertG@saps.gov.za**

APPROVED

P Pillay
UNIVERSITY OF KWAZULU-NATAL

RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: A CRIMINOLOGICAL ANALYSIS OF CYBERCRIME ACTIVITIES IN SOUTH AFRICAN BANKING INDUSTRIES: A STUDY OF KWAZULU-NATAL: UNIVERSITY OF KWAZULU-NATAL: MASTERS DEGREE: RESEARCHER: P PILLAY

The above subject matter refers.

You are hereby granted approval for your research study on the above mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office:

The Provincial Commissioner: KwaZulu-Natal:

- **Contact Person:** Lt Col DN Govender
- **Contact Details:** (031) 325 5809/4934
- **Email Address:** GovenderDN@saps.gov.za

The Provincial Commissioner: KwaZulu-Natal has stressed that participation in interviews will be on a voluntary basis and respondents may refuse to answer questions implying sensitive information.

Kindly adhere to paragraph 6 of our attached letter signed on the **2021-10-21** with the same above reference number.

[redacted] **MAJOR GENERAL**
RESEARCH
DR PR VUMA

DATE: 2021-11-16

1

ANNEXURE E: University of KwaZulu-Natal Full Approval Letter

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

09 December 2021

Perushka Pillay (213562910)
School Of Applied Human Sc
Howard College

Dear P Pillay,

Protocol reference number: HSSREC/00002537/2021
Project title: A criminological analysis on cybercrime activities in South African Banking Industries: A study of Standard Bank at Kingsmead branch in Kwa-Zulu Natal.
Degree: Masters

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 25 February 2021 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid until 09 December 2022.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

HSSREC is registered with the South African National Research Ethics Council (REC-040414-040).

Yours sincerely,

[redacted]

Professor Dipane Hlalele (Chair)

/dd