Exploring the Prevalence of Cybercrime in the Banking Industry in KwaZulu-Natal, South Africa

Perushka Pillay[1], Precious Nolwazi Ntuli[1], Stanley Osezua Ehiane[2,3]

[1]*Department of Criminology and Forensic Studies, University of KwaZulu-Natal, Durban, South Africa. Email: perushkapillay@gmail.com and Email: ntulip@ukzn.ac.za*

[2]*Department of Politics and Administrative Studies, University of Botswana. Gaborone, Botswana. Email: ehianes@ub.ac.bw*

[3]*School of Public Management and Governance, College of Business and Economics (CBE), University of Johannesburg, Johannesburg, South Africa. Email:* stanleyehiane@yahoo.com

ABSTRACTS: 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. As 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 paper analyses the causes of the increased rate of cybercrime in banks and determines the effectiveness of legislation in addressing the threat posed by cybercrime to the banking industry. This study utilised a qualitative research design using face-to-face interviews with ten participants who were purposively selected. 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 has been concluded that the 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, Police Service.

1. INTRODUCTION

Technological and social change has increased significantly in the twenty-first century and together with this, new criminal activities have emerged that were not previously prosecuted because they did not exist before [1]. Attacks on digital technologies are referred to as cybercrime or online crime; this is committed in the cyber-environment using technological systems that may involve computers, mobile phones, and credit card machines [2]. 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 [3]. 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 [4]. Across major economies such as the USA, China, Japan, and several 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 [5], and the South African landscape is no exception.

South Africa has presented some of the highest numbers of cases of cybercriminal activities globally [6], and according to the SAPS Directorate for Priority Crime Investigation (DPCI), cybercrime has risen steadily in banks in Durban, KwaZulu-Natal [7]. 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 Opland and Moodley, "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 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 [9]. 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 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 remains difficult to enact legislation to combat cybercrime and ensure data protection. Van der Westhuizen states that cybercrime caused severe losses to the South African business sector in 2015. The World Economic Forum [10] estimated the value of these losses to be around R5,8 billion. As indicated in a report by SABRIC, 75 per cent of fraud that occurred in South African banks was attributed to cybercrime schemes.

With the globe 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. In the 2014/2015 crime statistics report [12], no information on cybercrime could be traced. 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. In light of the aforementioned, this study examines the causes of the increased rate of cybercrime in the banking industry and the effectiveness of legislation and policies that serve as countermeasures to the menace of cybercrime in South African banks.

2. METHODOLOGY

The study adopted a qualitative research design. The objective of this qualitative research method is to understand human actions and behaviours from the subjective perspectives of the participants [13]. The narratives of the participants are detailed and insightful in how people experience any particular phenomenon. According to Crix, qualitative research involves an in-depth investigation of knowledge. This study is interested in understanding the magnitude of cybercrime in financial institutions and not the number of cases or other numerical statistics. The adoption of a qualitative approach in this study elicited an in-depth understanding of the prevalence of cybercrime in South African banks as perceived through the lens of South Africa Police Services (SAPS) detectives. The study relied on the participation of the SAPS detectives on the prevalence of cybercrime in South African banks, and the effectiveness of the legislation in addressing such crime.

The principal instrument for data collection was semi-structured in-depth interviews. The study engaged in face-to-face interviews with the research participants to expand on the essence of people's understanding and perceptions of cybercrime. The interviews were conducted among 10 SAPS participants who were purposively selected from various ranks, ranging from lieutenant colonel to captain and detectives in KwaZulu-Natal province. The study recruited these participants from two police stations and two detective units. The sample from the two police stations comprised three research participants, while seven research participants were recruited from the two detective units. 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 [16]. 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 five weeks. The adoption of the purposive sampling technique was based on the researcher's understanding of the population, its elements, and the research aims, which were based on the researcher's judgment and the purpose of the study [17]. 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 [18].

While conducting the interviews, the study 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. The University of KwaZulu-Natal's Ethics Committee permitted to conduct this research. The study's goal was clearly explained to participants before the interview sessions. The study's voluntary character was explained to participants, who were told they could leave the interview at any time without cause or consequence. A copy of the was completed by each participant. The field notes and recordings were analysed for themes using thematic content analysis, which is "an approach to the analysis of documents and texts (which may be printed or visual) that seeks to quantify content in terms of predetermined categories and a systematic and replicable manner" [19:181]. After using the computer application Nvivo to organise the interview transcripts, recurring themes and conceptual problems were found and developed into themes that served as the foundation for the analysis.

3. STUDY LOCATION

The 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 estimated 11,3 million people [20]. 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 are not disclosed for ethical reasons. Four police stations/detective units in total were visited. These are located in the west, south, outer west, and inland areas of Durban and all fall under the eThekwini Metropolitan Municipality in KwaZulu-Natal.

4. 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 [21]. 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 several ways, including mathematically, through encryption, or by conversion to a holographic picture or music [22]. Okonigene & Adekanle 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 data breach, which makes dealing with cybercrime and data security breaches difficult [22].

It is essential to highlight two primary elements of cybercrime, namely computer-assisted and computer-focused crimes. Obeng-Adjei states that computer-assisted crimes can be referred to as unlawful acts that are performed in cyberspace; an example of this is money laundering. Software systems, as well as the internet, can be seen as enablers of cybercriminal activities. Ahmed states that computer-focused crimes are attacks that target IT systems, Hacking and virtual attacks are examples of these types 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 [24]. Rosewarne indicates that the multiplication of cybercrime ‘is ascribed to the two components or motivations of financial and psychological gain. Rosewarne [4] proposes that the common utilisation of the internet and low enforcement of punishment on cybercriminals, once detected, are the key drivers of the multiplication of cybercrime in South Africa.

5. INFORMATION COMMUNICATION TECHNOLOGY AND CYBERCRIME IN THE BANKING INDUSTRY

Information communication technology (ICT) has revolutionised and streamlined our lives. As Raghavan & Parthiban state, ICT has been implemented in various industries and has been used to streamline business

processes using coding, customising, categorising, and summarising facilities and applications. However, it has also launched unintended repercussions in the form of cybercrime. Cybercrime has plagued numerous sectors; one of these is the banking industry, which has experienced multiple types of cybercrime such as phishing, vishing, spam, identity theft, hacking, and malware. As history demonstrates, innovation is accompanied by disruption, and this 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 SABRIC, 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 [26]. By utilising these technologies, customers can access their bank finances through ATMs and smartphones, while online banking is available 24/7, all year round.

As mentioned by an Organisation for Economic Co-operation and Development report [27], 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 [28, 29]. The rise in fraud, as criminals access banking apps, can be attributed to increased use by bank clients of these facilities. SABRIC 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 & Parthiban 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. Cybercriminals use various means to steal information from customers' banks, and eventually their money [30]. 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 [11].

6. 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 [31]. The South African Banking Risk Information Centre's annual crime statistics for 2020 [11] mention 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% [31].

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 to gain their personal information and scam them on digital and online platforms [31]. According to Majola, 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 crimes. Furthermore, Cohen & Crabtree mention that consumers must ensure that their personal information and data are secure to avoid identity theft and deceptive actions on various online platforms as a result of the shift in public behaviour. Cohen & Crabtree highlight 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 data are at risk unless adequately safeguarded to prevent cybercriminals from obtaining access to defraud one of one's money [32].

A TransUnion study 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 [31]. 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 [31].

7. CYBERCRIME LEGISLATION IN SOUTH AFRICA

South Africa has common law offences that are described in a body of laws that cover 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 which additionally deals with illegal access to information and data damage [33]. 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 bounce their signal from country to country, making policing cybercrime in KwaZulu-Natal and South Africa very challenging. Shinder 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 [35]. Even if the attacker might be identified, digital evidence may be hard to prove. Consequently, the successful prosecution of a cybercriminal is challenging.

Likewise, as noted by Von Solmes, 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 [36]. However, the Bill has clear drawbacks as some experts that it leaves some important questions unanswered, such as whether South Africa has cyber experts who will be able to effectively enforce the Bill [37]. Von Solmes argues that, although cyber-capacity skills are global, South Africa is not familiar with these scarce skills yet. For South Africa to effectively and expertly enforce the Bill, Von Solmes states that 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.

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 [38]. This means that in certain cases, regulations governing violent crimes cannot be applied to crimes committed by electronic means [38], as cybercrime does not require a physical component for its commission. Online offences have no bounds and cannot be confined within a country's national boundaries [38]. According to Njotini, 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 statutes, Van der Merwe 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, concerning 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. Before 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 [41]. When it comes to cybercrimes, however, the common law's applicability has certain limits and is narrowed considerably [41]. 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 [41]. The SALC determined that courts would be reluctant to extend current common law offences and concluded that legislation was necessary [40]. Several 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 [43]. They questioned whether the legislation would be required to effectively address the issue. Before 2002, it was clear that legislation was woefully inadequate to cope with the rapid advancement of information technology [43].

8. CYBERCRIME IN THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS (ECT) ACT

After years of legal ambiguity, Parliament passed the Electronic Communications and Transactions (ECT) Act in 2002 [44]. Chapter XIII is devoted to cybercrime and brings legal clarity to what constitutes and does not constitute cybercrime [42]. 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 to 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, realises that he or she is not supposed to access that data but proceeds to do so anyway [45]. 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 [46].

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 Picciano. between 70 and 80 per cent 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) [44]. 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 about 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 [8].

According to Anderson [47], 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. Before this, any information minimum requirements were only used as a general guideline rather than being made mandatory [48]. Cybercriminals and social engineers may need access to personal information to carry out 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 [44], which guarantees citizens' right to privacy. This right to privacy includes the right to confidentiality, which means that personal information must be protected from unauthorised collection, possession, dissemination, and use [44].

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 [8]. 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 evident. Van Rensburg 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.

9. RESULT AND DISCUSSION

Cybercriminals' activities evolve quickly. Analysis of the experiences of the participants unveils various causes for the prevalence of cybercrime in the banking industry and the effectiveness of the legislation in addressing the menace. The banking industry is frequently left behind, as 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 concerning 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 are lulled in a safe harbour while the implementation of legislation to curb their activities is ineffective. A bank is often hesitant to report cybercriminal activity for fear of harming its reputation and thus deterring investors and reducing public confidence, and this stumbling block should be addressed as a matter of urgency.

9.1 *Internal fraud within the banking industry*

The greatest fraud risk that banks face walks through their doors every morning and sits down to work" [24: 2]. Unfortunately, internal fraud is a sad reality in the South African banking industry. Below are the participants' comments in this regard:

"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; this, therefore, represents an unavoidable source of difficulties. According to a Hawks spokesperson 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 [50]. Bhengu 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. The responses suggest that some untrustworthy bank employees, lured by the smell of money, may leak information to a third-party platform.

9.2 Banks' poor internal controls, processes, and systems

Cybercriminals 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 other sector, is a common target for cybercriminals. Them people have witnessed an increase in cyber-attacks and data breaches over the last several years as cybercriminals 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. Bhengu mentions that the pressure on financial institutions to act is increasing, as attacks become more common, and regulators pay more attention. [51] 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. 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 occur regularly. The bank is 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).

Another participant 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).

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 [50]. This puts the back office as well as business controls, which would normally keep fraudulent behaviour away, at risk.

9.3 Banking Clients' Lack of Knowledge and Awareness

As mentioned by Gordon, 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 Gordon, 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 Investigation ranks South Africa eighth in the world in terms of cybercrime vulnerability [53]. 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 [54]. According to Picciano, cybercriminals take advantage of the fact that not all digital banking customers are computer literate, and they exploit this weakness; 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 [54]. 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 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" (P6).

Participant 6 further stated*: "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 how they defraud you"* (P6).

"Currently I have a case, where an attorney received an 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 letterhead and everything was like the client had done it, and the lady had lost R2,5 million" (P10).

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 Holt, *et al,* this is a way of deceitfully collecting personal information such as passwords, identity numbers, 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.

10. DETERMINE THE EFFECTIVENESS OF LEGISLATION AS A COUNTERMEASURE.

Participants in the study emphasized the importance of addressing the challenges of cybercrime. They further identified challenges in the effectiveness of legislation as a means to combat it.

10.1 Low Conviction Rates

South African financial institutions are members of the South African Banking Risk Information Centre which 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 have 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. As 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, criminals use this to their advantage as they are aware of the low conviction rate and that is the reason cybercrime continues to increase"* (P7).

However, because cybercriminals use customers' online profiles as their own, tracing these crimes to an individual is extremely difficult. Cybercriminals bounce their signals from country to country, which makes 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 [56]. Mer explained that because of the "behind-the-screen nature of the crime", catching and prosecuting these offenders was tough, which made such crimes appealing [56: 23]. This notion is supported by Loxton, 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 [56].

10.2 SAPS Officials' Lack of Skills to Effectively Police Cybercrime

The SAPS faces major challenges as a result of the growing menace of cybercrime. 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 [55]. They have also been insufficiently trained, and officers who possess the appropriate skills to combat cybercrime often leave the service 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. 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 [48]. This necessitates the efforts of specialised cybercrime forensic experts and computer forensic investigations to maintain a proper chain of custody. 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).

Moreover, 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. This has implications for SAPS as the specialised investigation units face 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. In addition, the SAPS is either unprepared to respond to cyberattacks or lacks the necessary technology to collect evidence. Criminals will continue to benefit from a shortage of skilled specialists to investigate cybercrime. In addition, substantial resources are frequently needed to execute cyber-related investigations. Simultaneously, the crime could be high-tech and investigating such crimes generally necessitates a significant amount of traditional investigative work and highly technical expertise, both of which are in short supply in South Africa.

CONCLUSION AND RECOMMENDATIONS

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.

Recommendations

More Effective Internal Processes in The Banking Industry

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 [45]. 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 indicates that to ensure that the infrastructure is secure and compliant with the industry's best practices and standards, it should be reviewed regularly both internally and by third-party security assurance providers [45]. 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 ensure 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.

Utilising Blockchain to Enhance Security in The Banking Industry.

Blockchain is a collection of blocks that stores financial data in hash functions with a timestamp and a connection to the previous block [50]. 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. The implementation of blockchain in the banking industry will lower the cost of online transactions while also boosting their validity and security [50]. 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. The benefits of blockchain technology will not 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.

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, 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) [41]. To be successful in the battle against cybercriminals, SAPS needs expertise in sectors such as cybercrime, cyber risk, fraud, and data analysis.

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 several financial institutions in South Africa, including ABSA, African Bank, alBaraka, Bidvest Bank, Capitec, Citibank, Discovery, FNB, Nedbank, Postbank, Standard Bank, and Tyme Bank [54]. 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 [57]. 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 regularly, especially given the dynamic nature of cybercrime.

Acknowledgement

We acknowledge the support of the National Institute for the Humanities and Social Sciences (NIHSS), Johannesburg, South Africa

REFERENCES

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

[2] G. D. De Angelis and A. Sarat. Cybercrimes. In S. Sissing (Ed.), 2013. A criminological exploration of cyberstalking in South Africa. Pretoria: University of South Africa. 2022

[3] L. Bhengu. ABSA engineer and wife accused of stealing over R100m from bank. granted bail. 2022. https://www.news24.com/news24/southafrica/news/just-in-absa-engineer-and-wife-accused-of-stealing-over-r100m-from-bank-granted-bail-20220202.

[4] C. Rosewarne. The 2012/3 SA cyber threat barometer. 2012. https://www.bic-trust.eu/files/2012/10/SA-2012-Cyber-Threat-Barometer_Medium_res.pdf.

[5] A. Obeng-Adjei. 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. 2017

[6] B. Von Solmes. What is SA doing to tackle cybercrime? The conversation. Fin24.com. The University of Johannesburg. 2015. https://www.fin24.com/Tech/Opinion/What-is-SA- doing/.

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

[8] R. Opland and T. Moodley. What happens if we violate PoPI? 2013. https://www.ey.com/Publication/VWLUAssets/What-happens-if-we-violate-PoPI/$FILE/130522%20Privacy%20Thought%20Leadership%202.pdf

[9] H. Van der Westhuizen. New Bill offers a robust game plan against cybercrime in South Africa. 2019. Https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/.

[10] A. Ikedal. Challenges to financial inclusion in South Africa. World Economic Forum. 2017. https://www.weforum.org/agenda/2017/04/financial-inclusion-south-africa/.

[11] South African Banking Risk Information Centre (SABRIC). Annual crime statistics. 2018. https://www.sabric.co.za/annual-crime-stats-2018.pdf.

[12] South African Police Service. Crime Statistics 2015. https://www.saps.gov.za/resource_centre/publications/statistics/crimstats/2015/crime_stats.pp

[13] R. Ormston, L. Spencer, M. Barnard, and D. Snape. The foundations of qualitative research. Qual. Res. Pract.: Guide Soc. Sci. Stud. Res. 2, 52–55. 2014.

[14] J. Crix. The Foundations of Research. Palgrave MacMillan, New York. 2004

[15] D. Cohen, and B. Crabtree. Qualitative Research Guidelines Project. 2006. http://www.qualres.org/HomeSemi-3629.html.

[16] A. F. Alpaslan. 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. 2010

[17] A. Picciano. Educational research primer. London: Continuum. 2007. Comp. Educ. Res. Approaches Method. 19, 39–62. 2004. http://education.pwv.gov.za/index.asp?src¼dvieandsrc¼64.

[18] J. Steyn. Assignment Writing. Pretoria: Van Schaik Publishers. 2013

[19] K. Budnik. Building a united front on financial crimes in the financial services sector. Https://www.pwc.co.za/en/press-room/cyber-security.html.

[20] Statistics South Africa. Mid-year population estimates: Statistical release. Pretoria: Statistics South Africa. 2019. Https://www.statssa.gov.za/publications/P0302/P0322019.pdf.

[21] F. Ibikunle and O. Eweniyi. 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. 2013

[22] R. E. Okonigene and B. Adekanle. Cybercrime in Nigeria. Business Intelligence Journal, 3(1), pp. 15-17. 2009

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

[24] M. Yar. Cybercrime and society. London: Sage Publications. 2013.

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

[26] M. Vrancianu and L. A. Popa. Considerations Regarding the Security and Protection of E-Banking Services Consumer's Interests. The Amfiteatru Economic Journal, 1228: pp. 388-403. 2010.

[27] Organisation for Economic Co-operation and Development (OECD). 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. 2007

[28] H. Asghari. 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. 2010

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

[30] K. K. R. Choo. The cyber threat landscape: Challenges and future research directions. Computers and Security, 308, pp. 719-731. 2011.

[31] G. Majola. The banking sector sees a hike in criminal incidents amid Covid-19. https://www.iol.co.za/business-report/economy/banking-sector-sees-hike-in-criminal-incidents-amid-covid-19-5ac126c6-5575-4658-aa97-3a4be01ac4e8. 2021.

[32] Business Tech. 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/. 2013.

[33] A. Kilian. 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. 2017.

[34] D. Shinder. What makes cybercrime laws so difficult to enforce? Tech Republic, 26 January. [Online]. Available at: https://www.techrepublic.com/blog/it-security/what-makescybercrime-laws-so-difficult-to-enforce/. 2011.

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

[36] African Union. List of Countries that 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. 2018.

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

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

[39] M. Njotini. Information and Communication Technology Law, in D.P. 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. 2019.

[40] D. Van der Merwe. 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), pp. 297-327. 2016.

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

[42] S. Snail. Cybercrime in South Africa–Hacking, cracking, and other unlawful online activities. Journal of Information, Law and Technology, 1, pp. 2009-2019. 2009.

[43] M. Sulfab. Challenges of cybercrime in South Africa. Research paper for Master of Arts in National Security Studies. American Military University: United States. 2014.

[44] The Republic of South Africa. Department of Justice. Protection of Personal Information Act No. 4 of 2013. Government Gazette No. 37067. Cape Town: Government Printer. 2013.

[45] M. Gould. How can banks protect themselves from cyberattacks? [Online Blog]. Available at: https://blog.nettitude.com/how-can-banks-protect-themselves-from-cyber-attacks. 2021.

[46] The Republic of South Africa. Interception and Monitoring Prohibition Act No. 127 of 1992. Government Gazette No. 35821. Cape Town: Government Printer. 1992.

[47] G. Anderson. POPI: The race to data safety. [Online]. Available at: https://www.itweb.co.za/content/p6GxRKqYW1D7b3Wj. 2015.

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

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

[50] L. Comins. FNB bank manager nabbed for allegedly stealing R4 million. [Online]. Available at: https://www.thesouthafrican.com/news/breaking-fnb-manager-arrested-fraud-theft-hawks/. 2021.

[51] PwC South Africa. 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. 2018.

[52] B. Gordon. Hacking, denial of service and Electronic Communications and Transactions Act. Servamus, 34. 2002.

[53] Norton Cybercrime Report. Cybercrime Report, Opswat, September 22, 2011. [Blog]. Available at: https://www.opswat.com/blog/2011-norton-cybercrime-report. 2011.

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

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

[56] A. Maliba. 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. 2021.

[57] L. Mashiloane. *Piet Pieterse: SAPS intensifies cybercrime battle*. [Online]. Available at: https://www.itweb.co.za/content/x4r1ly7RQl1vpmda. 2014.

DOI: https://doi.org/10.15379/ijmst.v10i1.3283