International Journal of Cyber Behavior, Psychology and Learning
Volume 14 • Issue 1 • January-December 2024

Application of Situational Crime Prevention Framework for Cybercrime Mitigation

Oluwatoyin Esther Akinbowale
https://orcid.org/0000-0001-5886-3018
Tshwane University of Technology, South Africa

Mulatu Fekadu Zerihun
https://orcid.org/0000-0003-4797-928X
Tshwane University of Technology, South Africa

Polly Mashigo
Tshwane University of Technology, South Africa

ABSTRACT

The purpose of this study is to apply the Situational Crime Prevention (SCP) technique to cybercrime mitigation using the South Africa cybercrime incidences as a case study. The SCP was first explained from the theoretical perspective and its five major strategies namely "increase effort", "increase risks", "reduce reward", "reduce provocation" and remove excuses" were explained and linked to remote and online crimes. Prevalent cybercrimes perpetrated in South Africa were also highlighted with hacking used specifically as an example in this study. The SCP technique was tailored towards the mitigation of hacking and its prevalent forms. The SCP fraud prevention "hardening framework" was developed and validated using the hacking incidences in South Africa as a case study. Based on this policy recommendations were made to promote cyber resilience. The outcomes of this study are conceptual frameworks with guidelines for applying the SCP strategies to remote and online crime. The conceptual frameworks are suitable for cybercrime prevention and mitigation and for achieving cyber-resilience

KEYWORDS

Cybercrime, Cybercrime Prevention and Mitigation, Cyber Resilience, Hacking, SCP

INTRODUCTION

Cybercrime, one of the fastest growing crimes across the globe, involves the use of computers and digital platforms to conduct unlawful activities driven by motives like revenge or financial gain (Toona, 2022). It is a major challenge faced by financial institutions and intent service providers, including those in South Africa.

Accenture (2020) reported that the cost incurred due to cybercrime perpetration has increased to R2.2 bn per year. The National Cybersecurity Index (2018) indicated that South Africa ranked 102 out of 160 countries in terms of cybersecurity capacity, with an estimated score of 27.27%. The Global Cybersecurity Index ranked South Africa fourth and eighth in the list of African countries vulnerable to cybersecurity breaches in 2018 and 2020, respectively (Global Cybersecurity Index, 2018, 2020). According to Cyber Exposure Index (2020), South Africa maintained the sixth position among African countries with extreme exposure to cybersecurity vulnerabilities. This report aligns

DOI: 10.4018/IJCBPL.353436

with Surfshark (2022), which revealed that South Africa ranked sixth in cybercrime density, increasing from 11.8 victims per one million internet users in 2016 to 14.1 victims in 2019 and from 50.8 victims in 2020 to 56 victims in 2021.

Researchers like Mcanyana and Brindley (2020) and Akinbowale et al. (2024a, 2024b) reported that South Africa witnessed increasing rates of cyberattacks, impacting banks, service providers, and customers. According to Toona (2022), the main targets of cybercrime in South Africa are financial institutions, insurance companies, energy and utility companies, and the government. However, any business organization can be targeted. Toona (2022) also reported that since the COVID-19 pandemic, South Africa has witnessed high profile cyberattacks on financial institutions and critical national infrastructures like the Transnet (a state-owned freight logistics organization) and South Africa's Department of Justice and Constitutional Development.

Prominent cybercrime methods include phishing, spam e-mail, denial of service (DoS), ransomware, and malware attacks. Delport (2020) reported that from January to March 2020, cyberattack cases through malware increased by 33%, while spamming attacks increased by 26.3%. The cyber defense approach employed by banks, service providers, and customers proved quite effective, with the detection of fraud via impersonation increasing by 30.3%, malware detections increasing by 35.16%, and the blocking of fraudulent links increasing by 59.8% (Delport, 2020). A survey by Akinbowale et al. (2024b) on the effectiveness of anti-fraud technologies in South African banking industries also supported the notion that South African banks deploy up-to-date technologies to effectively mitigate cybercrime.

However, the rate of cybercrime perpetration in South Africa is still on the rise. In fact, anti-fraud technologies alone cannot ensure the sustainable or effective mitigation of cybercrime perpetration. Other issues must be considered, including internal controls, synergy among stakeholders saddled with the responsibility of ensuring cybersecurity, the enactment and implementation of anti-cybercrime laws, and the development and implementation of regulatory and control frameworks. Drawbacks delaying the fight against cybercrime in South Africa include a lack of strict anti-cybercrime laws and resources for law enforcement agencies (Rick Crouch & Associates, 2020).

The efforts of the government and other stakeholders in fighting cybercrime have yielded positive results. Still, the goal of cybercrime mitigation has not been achieved holistically. It is, however, worth mentioning that the challenge of cybercrime perpetration is not limited to South Africa. This costly global problem disrupts large and small businesses and puts data and networks at risk (Deloitte, 2016).

The outbreak of COVID-19 led to a rise in the number of digital banking channels and remote banks, fueling an increase in cybercrime attacks. Cybercriminals, in turn, began to exploit the vulnerabilities of digital and remote banking systems via malicious software like viruses, worms, spyware, and Trojans. They also leverage the anonymity of cyberspace to launch attack from different locations (Deloitte, 2016). Fearn (2017) attributed the increase in cybercrime perpetration, including data breaches, to a lack of experts in cybersecurity.

In Africa, cyberthreats increase in conjunction with the growth in the number of internet users. The growing population in Africa, particularly in South Africa, is expected to contribute to more cybercrime cases unless effective and sustainable means are deployed to mitigate it (Song, 2017).

According to Rose (2020), the cost incurred by South Africa due to cybercrime-related incidences exceed ZAR 2.2 billion per year.

In 2021, the South African Banking Risk Information Centre reported that the number of cybercrime cases attributed to digital banking in South Africa decreased by 18% as compared to 2020 and those attributed to mobile banking decreased by 45% (SABRIC, 2021). However, was a 13% increase in cybercrime incidences attributed to the use of other banking applications. Comparing the cybercrime density of 2021 to 2020, Surfshark (2022) indicated that South Africa witnessed a 2% increase in cybercrime density (the percentage of cybercrime victims among a specified internet user) in 2021 as compared to 2020. Writer (2023) found that South Africa's cybercrime density increased by 8% from 2021 to 2022, placing the country in the fifth position in the global ranking of cybercrime

density. Fifty-six out of one million internet users in South Africa fell victim to cybercrime in 2022, which implies the country recorded a total of 2,000 cybercrime victims (Writer, 2023). According to Kaspersky (2023), in the third quarter of 2023, Africa remained one of the regions most targeted by cybercrime, with South Africa accounting for 28% of Internet of things device attacks, totalling an alarming 106,000 cybercrime attempts detected (Kaspersky, 2023).

In 2013, the South African government enacted the Protection of Personal Information Act to ensure individual data security and privacy (South African Institute of Chartered Accountants, 2021). Furthermore, in 2012, the government passed the National Cybersecurity Policy Framework (NCPF), enforced by the Ministry of State Security (Sutherland, 2017). In it, the NCPF provides a blueprint to address national security in cyberspace and combat cybercrime or other cyber-related offenses. The implementation of the NCPF ensures the safe use of information communication technology-related devices and the combat of cybercrime. Additionally, the new cyberlaw (known as the Cybercrimes Act 19 of 2022) was passed by the South African government to proscribe cybercrime (Toona, 2022). The legislation, which is post-incident in nature, defines the various types of cybercrime and their investigative methods. The law identifies the offenses that constitute cybercrimes, aiming to regulate and prosecute the perpetrators. It also outlines cybercrime as acts of cyber extortion, cyberfraud, illegal access to computers or devices like a USB drive or an external hard drive, unlawful data interception, the illegal acquisition, possession, receipt, or use of a password, falsification, fraud, online extortion, malicious communications, and the illegal distribution of intimate contents (Allen, 2021). The legislation is binding on all individuals and organizations in South Africa who employ the internet for communication and data processing.

Reyns (2010) employed the situational crime prevention (SCP) technique to cyberstalking victimization, finding that it limits opportunities of different forms of crime in different situations. Ho et al. (2022) conducted a systematic literature review on the application of SCP to prevent and control cybercrimes, concluding that the technique can assist in the development of innovative solutions geared toward combating cybercrime beyond technical solutions or single dimensional responses.

Existing works have reported on the feasibility of combating digital crimes, as well as cyber and information security vulnerabilities with SCP (Back & LaPrade, 2020; Brewer et al., 2019; Hinduja & Kooi, 2013). For instance, Vidal and Choo (2018) found the SCP technique suitable for the mitigation of cloud computing threats.

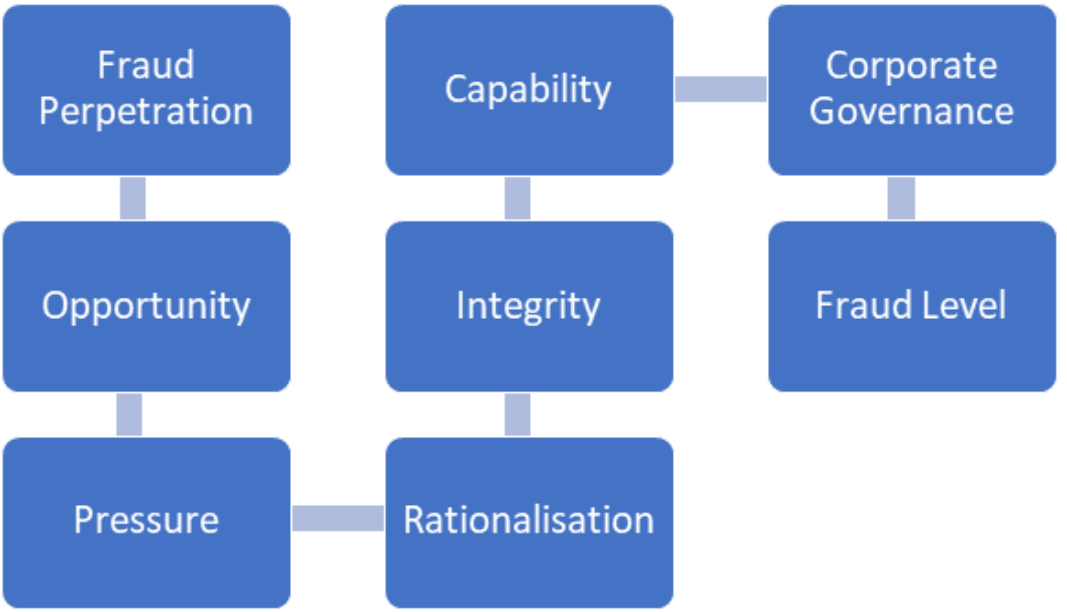
Armitage (2018) reported on the feasibility of achieving crime prevention through environmental design (CPTED). The CPTED is a multidimensional approach to crime reduction that draws theories from urban design, psychology, and criminology. However, CPTED did not make provision for digital crime.

Few studies have reported on the application of SCP strategies for mitigating remote and online crime. Therefore, the current study explores the SCP technique as a primary prevention measure for cybercrime mitigation in South Africa. The outcome of this study will assist financial institutions, network providers, and others in targeting cybercrime perpetration and reducing cybercrime opportunities rather than dispersing their resources on the characteristics of the perpetrators. The proposed framework will also help decision makers tackle cybercrime by reducing opportunities and rewards for cybercrime perpetration and increasing the risks and barriers in accessing an individual's or organization's digital infrastructure.

Many works have reported on the mitigation of cybercrime in South African financial institutions. However, the application of the SCP technique should be highlighted.

SCP is typically designed for physical crime perpetration; however, the modified framework presented in this study is geared toward the mitigation of remote and online crime. This study explores the SCP technique, providing a conceptual way by which the framework can be applied for cybercrime mitigation using the South African scenario as a case study.

Figure 1. Relationship among major factors influencing fraud perpetration



Note. Source: Authors.

The study contributes both theoretically and conceptually to cybercrime mitigation through an articulated framework, a standard methodology for tackling cybercrime, and a set of techniques aimed at reducing cybercrime opportunities.

METHODOLOGY

This section explains the theoretical framework of this study, introduces the proposed SCP technique, analyzes cybercrime within the South African context, and describes how SCP can be applied to combat cybercrime (with South Africa as a case study).

Theoretical Frameworks

The theoretical frameworks in this study include the following:

1. Fraud triangle theory (FTT), as developed by Cressey (1973)
2. Fraud scale theory, the redefined form of the FTT, as developed by Albrecht et al. (1984)
3. Fraud diamond theory, the extension of the FTT, introduced by Wolfe and Hermanson (2004)
4. Fraud box key model, as developed by Onodi et al. (2017) to address the perceived limitations of the FTT and fraud diamond theory.

These four theories categorize the factors responsible for the growing risk of fraud into six categories: (1) opportunity; (2) pressure/incentive; (3) rationalization; (4) integrity; (5) capability; and (6) corporate governance. The relationship among these six factors is depicted Figure 1.

Opportunity

Opportunity includes any loopholes or weaknesses that the threat actors can exploit to perpetrate fraud. These may be in the form of weak internal controls, poor corporate governance, ineffective or

outdated anti-fraud technologies and cybersecurity firewalls, inadequate sensitization of employers and customers, and weak transaction authentication (Akinbowale et al., 2024a, 2024b; Kelly & Hartley, 2010; Rae & Subramanian, 2008). Hooper and Pornelli (2010) noted that fraud perpetration cannot take place without an opportunity exploited by the perpetrators.

Pressure/Incentive

Pressure/incentive includes perceived urgent circumstances that propel the threat actors to commit fraud (Rasha & Andrew, 2012). Pressure can manifest in three forms: (1) corporate; (2) personal; and (3) external (Lister, 2007). It may arise as an urgent financial need, immediate access to an organization's assets, and fraud addiction (Rasha & Andrew, 2012; Vona 2008).

Rationalization

Rationalization is a justification formulated by perpetrators for committing fraud (Hooper & Pornelli, 2010). Reasons may include revenge, unemployment, and indebtedness.

Integrity

Integrity addresses the moral reasoning of the perpetrator. Rae and Subramanian (2008) indicated that fraud perpetration is a lack of integrity on the part of the perpetrator. Albrecht et al. (1984) posited that the pressure and opportunity to commit fraud are high when the integrity of the threat actor is low (and vice versa).

Capability

According to Wolfe and Hermanson (2004), even if there are opportunities to commit fraud or the threat actors can justify their actions due to a lack of integrity, fraud will not take place without capability. Capability refers to resources and attributes of the perpetrators, including their knowledge, skills, expertise, or resources invested in committing fraud. Capability can also include the perpetrator's position and influence, self-confidence and ability to cover up, coercion of associates into committing fraud, and their ability to handle stress and the risk related to fraud perpetration.

Corporate Governance

Corporate governance is the set of processes by which an organization is controlled and directed (Akinbowale et al., 2021). Onodi et al. (2017) indicated that a high level of corporate governance can promote fraud mitigation, reducing the rate of fraud perpetration. It could be in the form of public disclosures, internal control, oversight, managerial activities, ethical culture, risk management, regulatory compliance, internal or external audits, advisory, and monitoring (Onodi et al., 2017).

SCP Technique

The SCP technique argues that crime perpetration is influenced by the system's vulnerability, the perceived costs and benefits, and the degree of rationalization by the perpetrator (Clarke, 1995). Efforts must be geared toward reinforcing the security of the targeted asset. To further reduce the likelihood of crime perpetration, it is crucial to enhance the risk of being caught and reduce the benefits and rewards associated with the crime (Clarke, 1995).

Beebe and Rao (2005) explained that the relationship between the benefit and likelihood of fraud occurrence is moderated by the ability to neutralize or rationalize criminal behaviors. Hence, according to SCP, a criminal's pseudo-rational behavior is largely dependent on the perceived benefits.

The SCP technique is premised on the fraud theories discussed in the previous subsection, as well as other theories like the rational choice theory (Clarke & Cornish, 1985), routine activity theory (Cohen & Felson, 1979), and routine activities theory (Brantingham & Brantingham, 1999). The intersection among these theories is that fraud perpetration is a function of an opportunity exploited

by a capable perpetrator. For instance, the rational choice theory argues that if preventive measures do not increase the risks or costs of perpetration and do not reduce the anticipated benefits for the threat actors, the likelihood of the crime occurring remains high (Clarke & Cornish, 1985).

The SCP theory admits that the probability of crime is higher in areas known as "trouble or hot spots." Fraud is also more prevalent on emerging or trending products known as "hot products." In the context of cybercrime perpetration, these assumptions are presumed to be true because the reliance of institutions on information technology (IT) and big data for product and value creation or service delivery makes the financial institutions and their infrastructure targets for cybercriminals. Hence, the financial institutions, their service providers, and other business organizations who employ IT for their operations or infrastructure are "hot spots" for cybercrime perpetration.

Cybercrime is a global problem targeted at organizations and individuals through IT and internet-enabled devices or infrastructures (Akinbowale et al., 2020a, 2020b). Furthermore, the outbreak of COVID-19 promoted the use of remote and online transactions, making digital banking services a "hot product." In turn, the threat actors began targeting victims across various online banking platforms (Chigada & Madzinga, 2021; Lallie et al., 2021; Li & Liu, 2021). The COVID-19 and post-pandemic periods witnessed a surge in the use of technology for communication and remote work, resulting in an increase in cyber-related attacks.

Therefore, the SCP technique developed by Clarke (1995) classified 25 situational fraud prevention techniques, which are arranged into five categories: (1) increased efforts; (2) increased risks; (3) reduced rewards; (4) reduced provocations; and (5) removal of excuses. The proposed strategies aim to reduce the opportunities or vulnerabilities exploited by the threat actors.

1. **Increased Efforts:** This category is designed to raise the number of the threat actors' attempts. Thus, if the capabilities required to match or exceed these efforts are not put in place, fraud perpetration is less likely to take place.
2. **Increased Risk:** The second category aims to increase the risk of fraud perpetration, premised on the fact that the higher the risk of being caught, the lower the rate of fraud perpetration and vice versa.
3. **Reduced Rewards:** This category is designed to reduce the threat actors' anticipated benefits. With a reduction in the reward and an increase in the risk of perpetration, the motivation for committing fraud should decrease.
4. **Reduced Provocations:** The fourth category targets the reduction of the threat actors' opportunities and other factors that may encourage them to commit fraud.
5. **Removal of Excuses:** The final category aims to eliminate the threat actors' justification or rationalization for committing fraud (Beebe & Rao, 2005).

The SCP framework emphasizes understanding how crimes are committed and designing crime prevention techniques for people, places, and situations with high criminal activity, without focusing on the motivations of the criminals. The SCP framework considers situations that provide opportunities or advantages for threat actors and uses an action-based framework to minimize these opportunities and reduce fraud.

However, SCP is limited to combating fraud involving physical assets and locations. It does not consider digital crimes committed via the internet. To bridge this gap, Beebe and Rao (2005) modified the SCP theory to accommodate digital information systems security, addressing security challenges in the blockchain technology. Blasco and Fett (2019) also explained how digital systems can be secured using the modified SCP technique using blockchain security, SCP theory, and distributed cyber systems. The authors explain that criminal strategies on blockchain networks in the digital realm are comparable to criminal strategies in the physical realm. The outcome of the study, therefore, indicates the deployment of SCP to safeguard distributed cyber systems to achieve effective security protocols.

This study expanded the scope of SCP by applying it to remote and online crimes, using South Africa as a case study. It extends the SCP technique from the physical realm to the digital realm, proposing measures that can be used in cybercrime mitigation with the five categories found within the SCP techique.

Nature of Cybercrime in the South African Context

Kaspersky (2023) indicated that Africa was targeted by cybercriminals in 2023 because of the increasing number of online users and an inability to mitigate the loopholes exploited by the perpetrators. South Africa has the highest rate of cybercrime among African countries. It has the fifth highest rate of cybercrime across the globe, with 56 victims per one million online users. Cybercrime density is a measure of the percentage of people who have become victims of cybercrime among specific internet users (Surfshark's Report, 2022).

Kaspersky (2023) reported that South Africa experienced a 24% increase in online-based threats by corporate users in the second and third quarters of 2022. In addition, the country experienced 28% of the cyberattacks on Internet of things devices within the third quarter of 2023. They also had a 22% increase in malware attacks within the first quarter of 2019 as compared to the first quarter of 2018, which amounts to approximately 577 attempted attacks per hour. Card-not-present fraud on South African-issued credit cards increased by 79.5% in 2019 as compared to 2018, making it a major contributor to gross fraud losses in the country (Accenture, 2020).

Cybercriminals may perceive South African organizations as having lower combative or defensive strategies as compared to developed economies. They may also think the organizations will not track or prosecute criminals based on their low investment in cybersecurity-enabling technologies and the lack of cybercrime legislation in the country.

South Africa was chosen as a case study in the current research due to its scale of cybercrime. However, the application of the developed SCP is not limited to the South African context. Other countries can adopt or modify the technique for cybercrime mitigation based on their needs.

According to Akinbowale et al. (2022) and Toona (2022), cybercrime in South Africa targets financial and insurance institutions, service providers, and critical national infrastructures. Cyberattack incidences between 2010 and 2020 impacted various fields, including construction, education, finance, healthcare, IT, leisure and hospitality, manufacturing, media, public, retail, communication, and transportation (Pieterse, 2021). Perpetrators are motivated by personal, accidental, criminal, economic, and political reasons (Pieterse, 2021).

According to the International Criminal Police Organization's African Cyberthreat Assessment Report (2021), 230 million cyberthreats were detected in South Africa, with 219 million traced to e-mail-based attacks, which accounted for 95.21% of the country's cyberthreats 2021. Thus, existing studies and reports indicated that the most cybercrime in South Africa involves hacking, data breach, digital compromise, system intrusion, cyberfraud, DoS attack, phishing, spam e-mail, ransomware, and malware attacks amongst others (Akinbowale et al., 2024a; Pieterse, 2021).

Table 2 presents a summary of selected cyberattack incidences in South Africa.

According to the table, it can be inferred that hacking is a common phenomenon in South African cyberspace. It has also led to other forms of cybercrime, such as data breach, online theft, and ransomware. The next section presents the application of the SCP to cybercrime in South Africa, emphasizing ways to confront prevalent forms of cybercrime.

Application of SCP to Cybercrime Mitigation (South Africa as a Case Study)

Prevalent forms of cybercrime presented in Table 2 include hacking, data breach, compromised Websites, system intrusion, cyberfraud, DoS attacks, phishing, spam e-mail, ransomware, and malware attacks. Among these, hacking was used to validate the SCP technique in the current study.

Hacking is an unauthorized intrusion into an organization's Website, system, or database to access, hijack, control, or steal customer or organizational information (Kumudha & Rajan, 2018;

Table 1. SCP fraud prevention framework proposed by Clarke (1995)

Increased Efforts	Increased Risks	Reduced Rewards	Reduced Provocations	Removal of Excuses
Harden target	Extend monitoring	Conceal targets	Reduce stress and frustrations	Set rules
Access control to infrastructure	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce emotional arousal	Alert conscience
Deflect offenders	Utilize place managers	Disrupt markets	Neutralize pressure	Assist compliance
Control tools	Strengthen formal surveillance	Deny benefits	Discourage imitations	Control drugs and alcohol

Mugari et al., 2016). As shown in Figure 2, hacking can take the form of a virus, malware attack, DoS attack, password attack, or key logging. Virus or malware attacks involve the secret installation of malicious or illegal programs into an organization's computer system to enable the threat actors to gain unlawful access to the organization's Website, system, or database (United Nations Office on Drug Crime, 2013; Uppal et al., 2014). The virus or malicious software can alter the organization's network, systems, or system settings without prior notification or permission from an authorized user.

Another form of hacking is the DoS attack, which involves the flooding of an organization's network with high levels of traffic until it collapses under the pressure to grant the threat actors with unlawful access. A password attack is a hack in which the threat actors use guessed, stolen, or cracked passwords to intrude into an organization's system, database, or Website. Key logging is another form of hacking that involves the use of a secretly installed software (called keystroke logger) that records each keystroke the authorized user types. Then, the secret software periodically uploads the keystroke information to the installer via the internet. This act allows the installer an opportunity to access the organization's system, database, or Website using confidential information like log-in details. Hackers can design keylogging software to use keyboard application program interface, memory injection, or malicious script injection.

Table 3 presents the SCP fraud prevention framework geared toward tackling cybercrime, specifically hacking. It includes various identified forms, including virus/malware attack, DoS, password attack, and key logging.

Increased Efforts

To mitigate cyberattacks targeted against financial institutions, service providers, and national critical infrastructures (as in the case of South Africa), the "increased efforts" strategy includes five action-driven activities: (1) harden targets; (2) access control; (3) screen exit; (4) deflect offenders; and (5) control tools. The strategy focuses on approaches that prevent the threat actors from accessing individual and organizational cyber infrastructures. In turn, the threat actors will expend more unsuccessful efforts at committing their cybercrime (Ho et al., 2022).

An organization's IT infrastructures are the target of the threat actors. Thus, it can be protected (or "hardened") through efforts like application configuration, system and software protection, and firewalls to block intrusion and other unwanted features.

"Access control" and "screen exit" prevent access to private networks through strategies like input/output device controls, passwords, firewalls, and the implementation of robust remote authentication methods and intrusion detection systems (IDS; Coles-Kemp et al., 2015).

The "deflection" of offenders monitors the traffic and activities on unused ports or system services within a network. Any activity detected on these unused areas is likely to be the handiwork

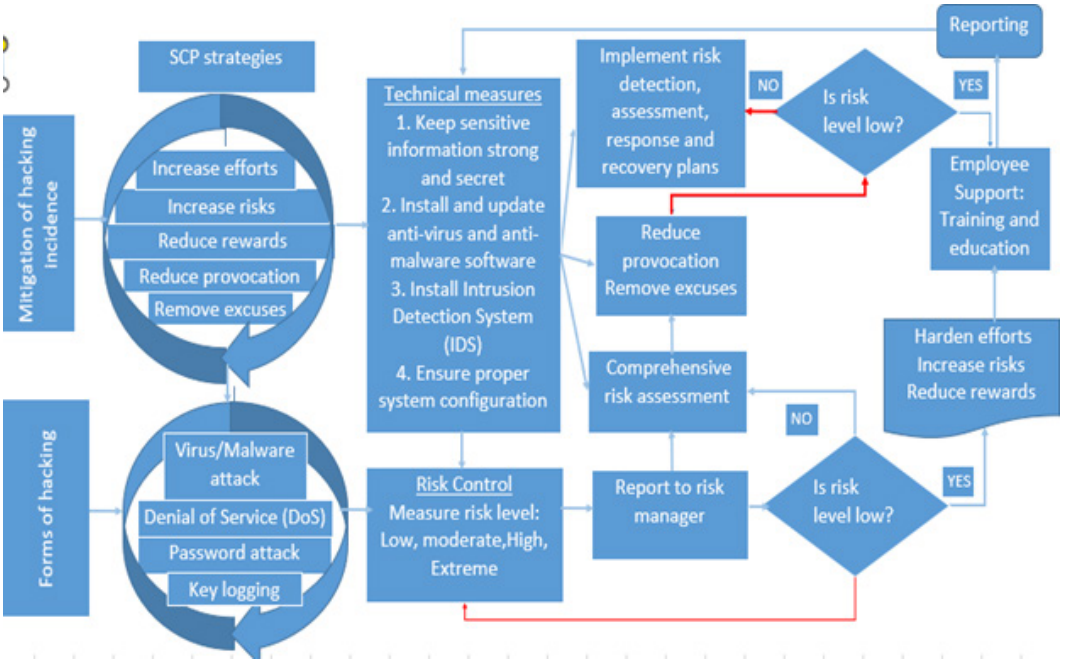
Table 2. Summary of selected cyberattack incidences in South Africa

S/N	Year	Target	Nature	Description	Reference
1.	2012	Post Bank	Hacking of computer system and fraudulent online transfer	R42 million unauthorized online transfers made	Rasool (2012)
2.	2013	MTN and online service providers like Afrihst and Axxess	Denial of service attack and data exposure	Network flooded with traffic until it collapsed to the pressure	IT News Africa (2013)
3.	2014	South African government Website and other Website	Ransomware, hacking, malicious software attack	Unpatched security vulnerability due to use of outdated version of digital contents and hidden links sent by cybercriminals were clicked by authorized users, leading to compromised security	Pieterse (2021)
4.	2016	Standard Bank	Hacking of computer system, running of computer program without authorization, and fraudulent online transfer	Standard Bank system and internal banking process led to the compromise of customer database and fraud and R300 million was fraudulently withdrawn by cybercriminals from automated teller machines in Japan	van Zyl (2016)
5.	2016	MTN	Hacking, data exposure	Computer system intrusion	Pieterse (2021)
6.	2017	Telkom (telecommunication provider), Office of the South Africa Chief Justice	Ransomware	Unpatched security vulnerability due to use of outdated version of online contents and hidden links sent by cybercriminals were clicked by authorized users, leading to compromised security	Pieterse (2021)
7.	2017	South African database	Hacking, data exposure	Website compromise and computer system's intrusion	Pieterse (2021)
8.	2018	South African presidency Website	Hacking	Data breach exposes data of 934,000 South African citizens	Mngadi (2018)
9.	2020	Post Bank	Intrusion, card fraud	Compromised 12 million bank cards	Pieterse (2021)
10.	2023	Nedbank	Data exposure	Exposed data from 41,000 clients, with stolen data of South African citizens used by cybercriminals to create fraudulent profiles on Nedbank's Money app	Timeslive (2023)

of cybercriminals. Once the threat actor connects to the unused port or service, the deflect function will redirect the threat to a decoy, which mimics legitimate applications, data, or servers that are of no value. In doing so, criminals are tricked into believing they have gained unlawful access into the organization's assets. This strategy allows the organization's security team time to study the attack, identify the criminals and their location, neutralize the threat, and block similar intrusions.

"Control tools" is comprised of the following strategies: withdrawal of access rights of former employees; control over digital access; multilevel transaction authentication; masking of the internet protocol address; and the periodic background check and forensic auditing.

Figure 2. Framework for validating the SCP technique applied to hacking



Note. Source: Authors.

Increased Risks

This strategy is made up of five approaches: (1) extend monitoring; (2) assist natural surveillance; (3) reduce anonymity; (4) utilize place managers; and (5) strengthen formal surveillance.

The main objective of this strategy is to increase monitoring and surveillance within and outside of the organization to detect intrusions or cyberattacks (Ho et al., 2022). Top management monitoring, anomaly detection through data mining and artificial intelligence (AI), regular forensic audits and review of communication logs, and the provision of hotlines for customers and employees are tactics that can be employed under this strategy.

Fraud investigators can use data mining and AI like machine learning to gain insights into detecting hidden patterns, trends, or anomalies within a dataset (Clayton, 2011; Decker et al., 2011; Kenyon & Tilton, 2011; Miller & Martson, 2011; Mittal, Kaur, & Gupta, 2021; Ngai et al., 2011). Specialized algorithms train datasets to recognize an anomaly.

The IDS is a network-based security technology developed for the detection of vulnerabilities against a target computer or application. IDS monitors the traffic for malicious transactions and reports any threats to the security administrators.

Reduced Rewards

The objective of this strategy is to protect the primary targets (cyber infrastructure) to ensure that the threat actors do not actualize their rewards for constituting cyberthreats (Coles-Kemp & Theoharidou, 2010; Ho et al, 2022). This strategy has five approaches: (1) conceal targets; (2) remove targets; (3) identify property; (4) disrupt markets; and (5) deny benefits.

In the first two approaches, information can be classified and secured in a repository to prevent intrusion. Another approach, watermarking, is a network security process of embedding a marker on important documents to hide them in a carrier signal. Digital watermarks can be employed to verify the integrity and authenticity of the carrier signal to know the identity of its owner.

Table 3. SCP fraud prevention framework in the digital context

Increased Efforts	Increased Risks	Reduced Rewards	Reduced Provocations	Removal of Excuses
1. Harden target● Harden cyber infrastructure and hardware● Harden operating systems and firewalls● System and software protection● Application configuration● Update operating system and apps● Secure network	6. Extend monitoring● Supervision and monitoring of critical infrastructure● Management supervision	11. Conceal targets● Classify information● Regulate disclosures● Watermark documents, digital signatures● Systems and database back-up● Hide customers' and organisations' confidential and sensitive information	16. Reduce stress and frustration● Effective response to breaches● Develop and implement risk management plans	21. Set rules● Ethical code of conduct● Reporting routes
2. Access control to infrastructure● Input/output device control● Implement strict account control management and policies via passwords● Implement strong remote authentication methods and intrusion detection systems (IDS)● Firewalls	7. Assist natural surveillance● Observe communications● Anomaly detection through data mining artificial intelligence● Regular forensic audit and review of communication logs	12. Remove targets● Move database to safe repositories	17. Avoid disputes● Forensic investigation	22. Post instructions● Warning messages
3. Screen exits● Asset monitoring and accountability● Firewalls● Implement authorized data exfiltration● Virus scanning and IDS	8. Reduce anonymity● Establish a baseline for network behavior and performance and detect any anomaly	13. Identify property● Know and classify assets and information● Label dataset and database● Identify digital signature● Data and asset encryption	18. Reduce emotional arousal● Effective disclosures and information management● Sensitization and awareness creation	23. Alert conscience● Sensitization and awareness creation
4. Deflect offenders● Decoys● Monitor suspicious behaviors● Respond to disruptive tendencies● Segregate information	9. Utilize place managers● Appoint managers at offices and locations of critical assets to improve monitoring and accountability	14. Disrupt markets● Disrupt network and chains of intruders● Develop and implement risk management plans● Data destruction approach● Artificial intelligence	19. Neutralize pressure● Cyber risk resilience● Adopt best practices● Regular assessment of security risk● Develop governance model and human capacity development● Awareness and implementation of ethical code of conduct	24. Assist compliance● Sensitization of customers● Human capacity development of employees● Threat awareness● Healthy work culture and sound practices● Cyber ethics education● Supervision and regulatory compliance

continued on following page

Table 3. Continued

Increased Efforts	Increased Risks	Reduced Rewards	Reduced Provocations	Removal of Excuses
5. Control tools● Withdrawal access rights of ex-employees● Web access control● Multilevel transaction authentication● Mask internet protocol (IP) address● Periodic background check● Regular forensic auditing	10. Strengthen formal surveillance● IDS● Hotlines for customers and employees	15. Deny benefits● Secure safe recovery processes● Effective incident handling● Insurance● Implementation of cyberlaws	20. Discourage limitations● Prosecution of culprits● Education, awareness, and implementation of ethical code of conduct	25. Control drugs and alcohol● Sensitization and awareness creation● Control substance and alcohol abuse

Note. Source: Authors developed from the concept of Clarke (1995).

Under the third approach, "identify property," critical assets like data must be classified, labelled, and encrypted. Through encryption, sensitive data is protected from intrusion (i.e., comprise, theft, or alteration) by locking it with a secret code that can only be opened by authorized users via a unique digital key.

In the fourth approach, "disrupt market," disruptive technologies like AI can be employed to recognize threats, complex data patterns, and anomalies. Then, it provides actionable recommendations before the culmination of a cybercrime. This approach can also be used for vulnerability management, malware analysis, and user authentication.

The fifth approach, "deny benefits," can be achieved by securing safe recovery processes, establishing effective incident handling tactics, and implementing insurance of business.

Reduced Provocations

This combination of technical and nontechnical strategies aim to reduce negative tendencies that can spur the threat actors into committing cybercrime (Ho et al., 2022; Padayache, 2015). Five approaches are used to reach this goal: (1) reduce stress and frustrations; (2) avoid disputes; (3) reduce emotional arousal; (4) neutralize pressure; and (5) discourage imitations.

The standardized release of information and disclosures to the public must be handled professionally to prevent giving out information that can propel the threat actors. Also, disputes should be resolved thoughtfully as "revenge" has been identified as one of the causative factors for cybercrime perpetration (Akinbowale et al., 2024d). Cyberthreat pressures can be neutralized through cyber resilience tactics, including leveraging anti-fraud technologies, adopting cybersecurity best practices, regularly assessing cybersecurity risks, developing a governance model and human capacity plan, and discouraging imitation by prosecuting the threat actors. Other approaches include effective response to breaches, development and implementation of risk management plans, forensic investigation, and resolution of disputes or breaches.

Removal of Excuses

Rationalization is a major component of fraud theory. This includes the threat actors' justification or excuses for committing fraud. Thus, the objective of the last strategy is two-fold. The first is an attempt to neutralize justifications and excuses by the threat actors to discourage them from committing crimes. The second is an attempt to eliminate excuses that security personnel may present to justify the security failure that led to the crime.

Table 4. Cyber risk and mitigation strategies (proactive and reactive technical measures)

Cyber risk	Proactive	Reactive
Hacking1. Virus/ malware attack2. Denial of service (DoS) attack3. Password attack4. Key logging	1. Use firewall2. Install and update anti-virus and anti-spy software3. Update log-in details (user identification and password), operating software, apps, and browser4. Keep sensitive information like log-in details strong and secret5. Use network protection via virtualization6. Implement multilayer authentication7. Establish data encryption and endpoint security8. Block public network9. Educate employees and clients10. Classify and back up sensitive data11. Monitor systems and perform periodic vulnerability assessments12. Identify third party or vendor risk management13. Harden operating systems and firewalls14. Protect system and software15. Install intruder detection system (IDS)16. Use proper and regular application configuration and cloud and network security17. Develop risk management plans18. Develop disaster recovery and business continuity plan	1. Identify source of breach2. Disconnect systems or devices from network3. Implement incidence response plan4. Implement communication plans and contact stakeholders (service provider, security agencies, insurance provider, clients, etc.)5. Deploy experts to investigate and assess level of impact6. Secure and monitor data entry points7. Implement risk management plans8. Implement disaster recovery and business continuity plan9. Fix vulnerabilities and restore system10. Deploy disclosure11. Train employees and educate clients12. Appraise performance of risk management and incidence response plans

Note. Source: Authors.

Approaches that can be employed under this strategy include set rules, post instructions, alert conscience, assist compliance, and control drugs and alcohol. These approaches can be implemented through an information security policy, public sensitization and awareness, insider threat awareness, employee education and training, implementation of an ethical code of conduct, and security education of users (Dargahi et al., 2019; Ho et al., 2022; Luo & Lioa, 2007; Kirwan & Power, 2013; Wilson & Siponen, 2009).

VALIDATION OF THE SCP TECHNIQUE USING SOUTH AFRICA AS A CASE STUDY

As discussed, cybercrime in South Africa mainly targets financial and insurance institutions, service providers, and critical national infrastructures. Those highlighted in Table 2 include hacking, data breach, Website compromise, system intrusion, cyberfraud, DoS attack, phishing, spam e-mail, ransomware, and malware attacks. This section focuses on the application of the SCP to mitigate hacking and its identified forms (i.e., virus/malware attack, DoS, password attack, and key logging).

Table 4 presents a summary of the major cyber risk (hacking) and mitigation strategies classified into proactive and reactive technical measures. Table 5 presents the hacking incidence severity level, as well as a description of the severity, incidence response level, and proposed SCP technique.

Figure 2 presents the framework for validating the SCP technique applied to hacking. The SCP is typically designed for physcial crimeperpetration, but the modified framework in Figure 2 enables its deployment for remote and online crime prevention. Figure 2 links the five major strategies of the SCP to the prevalent forms of hacking. Thestrategies are also linked to the preventive technical measures highlighted in Table 4 as a form of hardening the target while the technical measure is linked to the risk control as a subset.

An important component of the risk control is to measure the level of the risk, classifying it as low, medium, high, or extreme (see Table 5). Furthermore, the risk level is communicated to the risk manager, who validates the level of the risk. When the risk is low, the system may be further hardened through the first three SCP strategies (increased effort, increased risk, and reduced rewards). This is followed by employee support in terms of training, education, and reporting.

Table 5. Hacking incidence severity level, description, incidence response level, and proposed SCP technique

S/N	Severity Level	Description	Level of Incidence Response	SCP Technique and Severity	Team Allocation
1.	0 (low)	General threat or fraud to individual or organization with minimal impact	Identification and protection	Harden targets, access control, screen exit, deflect offenders, control tools	Organization's information technology (IT) and security personnel, IT vendors, anti-fraud personnel
2.	1 (Medium)	Threat or fraud to individual's or organization's sensitive information with moderate impact	Detection and response	Harden targets, access control, screen exit, deflect offenders, control tools, extend monitoring, reduce anonymity, establish baseline for network behavior and performance, utilize place managers, conceal targets	Forensic accountant, organization's IT and security personnel, IT vendors, management, anti-fraud personnel, human resources representatives, data protection experts
3.	2 (High)	Threat or fraud to individual's or organization's computer system, network, and information technology infrastructure with high impact	Detection, response, and restoration	Reduce stress and frustrations, avoid disputes, neutralize pressure, discourage imitations, remove excuses	Forensic accountant, organization's IT and security personnel, IT vendors, management and legal teams, third-party risk management, anti-fraud personnel, human resources representatives, data protection experts
4	3 (Extreme)	Threat or fraud to individual's or organization's computer system, network, and information technology infrastructure with severe or extremely disruptive impacts	Detection, response, and restoration	Reduce stress and frustrations, avoid disputes, neutralize pressure, discourage imitations, remove excuses	All the anti-fraud capacities and stakeholders

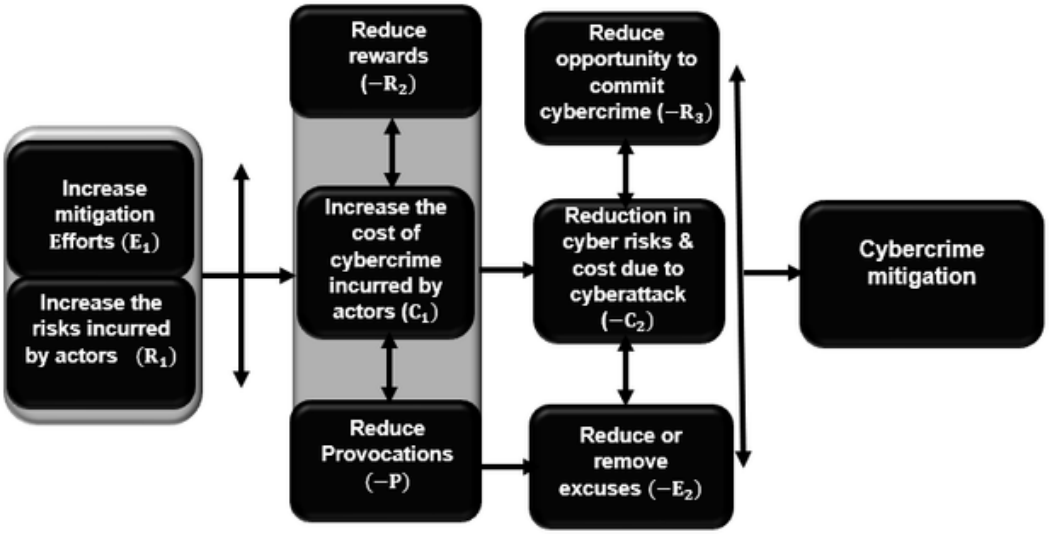
Note. Source: Authors, adapted from Akinbowale et al. (2024c).

Alternatively, when the risk is medium, high, or extreme, a comprehensive risk assessment will be required along with the implementation of preventive technical measures to harden the target based on the severity of the risk. In addition, the last two SCP strategies (reduced provocation and removal of excuses) will be applied. On the one hand, the implementation of the reduced provocation strategy aims to reduce negative tendencies within the organization that can spur the threat actors into further exploiting the opportunities for committing cybercrime. On the other hand, the implementation of the removal of excuses strategy aims to further discourage the threat actors from committing crimes and eliminate excuses that security personnel may present to justify the security failure.

If the risk level is still high after these efforts, the organization will need to implement risk response and recovery plans.

Figure 3 presents the mathematical formulation of the SCP. This can be employed for cybercrime mitigation.

Figure 3. Mathematical formulation of the SCP employed for cybercrime mitigation



Note. Source: Authors.

According to Figure 3, the mathematical proof that justifies the significance of the proposed SCP framework is presented in Equation (1).

$$cybercrime\ mitigation = f\left(E_1, R_1, P, R_2, R_3, E_2, C_1, C_2\right) \quad (1)$$

Per the equation, cybercrime mitigation effort is expressed as a function of an increase in the cost of cybercrime perpetration incurred by the threat actors (C_1), reduction in cyber risks and its associated costs due to cyberattacks through effective management control systems (C_2), an increase in the efforts geared at cybercrime mitigation (E_1), an increase in the risks of committing cybercrime incurred by the threat actors (R_1), reductions in provocations (P), opportunities that can spur the threat actors into perpetrating cybercrime by reducing rewards (R_2) of the threat actors like opting for backed up data instead of the ransom for restoring the organization's database, reducing the opportunity or loopholes exploited by the perpetrators (R_3), and removing excuses (E_2) due to internal failures or vulnerabilities that the perpetrators can leverage for committing a cybercrime.

The total opportunity cost $\left(C_{op}\right)$ to launch a cyberattack is a function of the inherent risk incurred by the attackers (R_1), the rewards (R_2), the opportunity leveraged on by the attacker, and the cost of cybercrime perpetration incurred by the attacker (C_1) (Blasco & Fett, 2019). The cost combines both the financial and nonfinancial capabilities of the threat actor to launch a cyberattack, as expressed in Equation (2).

$$C_{op} = f\left(R_1, R_2, R_3, C_1\right) \quad (2)$$

When the reward of cyberfraud perpetration (R_2) and opportunity (R_3) exceeds the risks (R_1) and cost incurred by the threat actors for cybercrime perpetration (C_1), the organization's cyber infrastructure and dataset may be at risk, as expressed in Equation (3).

$$R_2, R_3 > R_1, C_1 \quad (3)$$

When the risk and cost incurred by the threat actors is low, the opportunity to commit cybercrime and the reward of perpetration may increase and vice versa.

The risk (R_1) and the cost (C_1) incurred by the threat actors can be increased by increasing E_1, reducing P,E_2 and C_2 to reduce the reward (R_2) and opportunity (R_3) of cyberfraud perpetration, as expressed in Equation (4).

$$R_1,\ C_1 > R_2,\ R_3 = f\left(E_1, -P, -E_2, -C_2\right) \tag{4}$$

By sign convention, the factors that must be reduced to increase the risk (R_1) and the cost (C_1) incurred by the threat actors are assigned a negative sign, as in Equation (4).

POLICY RECOMMENDATIONS

To increase efforts, it is recommended to target hardening techniques like the use of a firewall to block access into the targeted system or prevent cyber intrusion or cyberfraud. This will make it difficult for the threat actors to penetrate information systems and digital facilities.

To increase risks, the use of IDS and knowledge-based intrusion techniques like data mining, forensic accounting, and AI systems equipped with a global positioning system for tracking and detection of suspicious transactions or behavioral patterns in cyberspace are recommended. These techniques can also aid in clamping down on the perpetrators. Vieira et al. (2010) indicated that artificial neural networks with self-learning capabilities can be employed to identify suspicious and malicious behavioral patterns in cyberspace.

To reduce rewards, effective management control strategies must be implemented by the organization or government. The implementation of strict cybercrime laws will reduce benefits for the perpetrators. South Africa, for instance, needs to ensure the implementation of the newly enacted cybercrime law and other existing laws that proscribe cybercrime.

To reduce provocation, any elements that the threat actors can be perceive as attractive crime opportunities must be prevented. For instance, in the case hacking, the opportunities or loopholes could be in the form of opening unused ports for online communications, clicking on fake links, responding to unsolicited or junk e-mail, intrusion from Web applications, failure to update the firewall, improper installation and configuration of database and digital application server firewalls to secure an organizational database, and the use of the same host server for organizations and customers.

Last, to remove excuses, the justification or rationalization for cybercrime perpetration must be eliminated. A system with a sound ethical culture and standard operational and reporting procedures aligned with regulatory standards will be helpful.

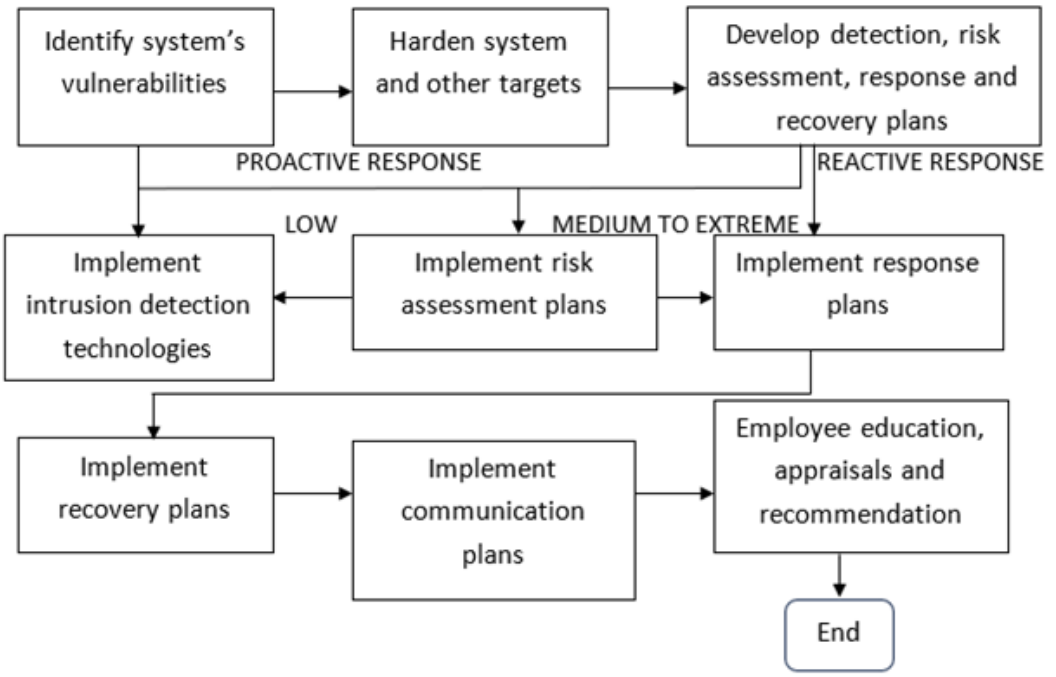
Figure 4 presents policy recommendations that can assist South African financial, business, and government organizations to develop cyber resilience to overcome various forms of cyberattacks.

As shown in Figure 4, individuals, businesses, and government organizations must identify their system vulnerabilities to develop resilience to cyberattacks. These are opportunities or loopholes within the target areas that can be exploited by the threat actors.

The threat actors usually target an organization's IT infrastructure, such as the computer system, database, server, input or output connections, endpoints, cloud applications, or networks. After checking for vulnerabilities, the targets need to be hardened to prevent intrusion. The list of technical and nontechnical measures to harden targets are described in Figure 4 and Table 4.

The next step is to focus on cyber risk detection, risk assessment, and response and recovery plans. These will enable effective and timely responses to a cyberattack, which can minimize the severity. Tactics include guidelines to detect and measure the severity of cyber risk, mitigation rules, and a plan to return the business to normal operations. Anti-fraud technologies, including the IDS and anti-threat software, will monitor unusual network activities. When a threat, suspicious behavior, or

Figure 4. Cyber-resilience policy framework



Note. Source: Authors.

potential security risk is suspected, the IDS will generate an alert or alarm like an e-mail or mobile phone alert. The IDS can identify intrusions, contain and control the breach, mitigate the damage, and alert authorized users and security personnel for further actions.

When potential risks are detected, its threat level will determine the type of incidence response used. Following the detection of the threat or breach, the priority is to mitigate the risk to prevent further damage or loss of data. Table 5 provides insight into how risk assessment and incidence responses can be carried out. In addition, any circumstances surrounding the breach must be investigated, including the impact and identified gaps.

All affected systems must be considered and concealed intrusions must be combed. Where applicable, the online attack must be blocked immediately while simultaneously rerouting network traffic. Furthermore, all identified compromised devices, systems, networks, Websites, and data must be isolated. Threats must be removed as the affected systems are restored to their normal working state.

An organization must recover the affected systems, data, or Websites from the threat actors to prevent continuous intrusion or demand for ransom. See Table 3 for a recovery list, including decoys, data backup, critical endpoints, systems, and servers. A back up will minimize losses and efficiently recover the data and infrastructure.

The recovery process may disrupt the normal operation of the business depending on the severity of the threat or intrusion. However, the unaffected services and operations may continue during the mitigation. A detailed investigation with forensic experts will help identify the opportunity exploited by the threat actors and the failure of security controls. The information gathered from the investigation will be useful for the review, training, and education of employees and clients, as well as the improvement of operational policies and procedures.

It will also be useful to develop robust incidence response and mitigation plans, as well as a communications plan. Honest disclosures must be made in a timely manner to the regulators and

other stakeholders, such as the customers, if the attack resulted in data loss, theft, or compromise. Law enforcement agencies must also be notified. A crisis manager should be hired if the reputation of the organization is at risk. In any event, it is crucial to implement an effective incidence response plan. The longer it takes to contain the attack, the more damaging and costlier it becomes.

The education of employees, clients, and the public is also a necessary step in a cyber resilience plan. This includes both proactive and reactive strategies, as presented in Table 4. Employees and the organization's security team should be trained to adhere to standard practices, deploying emerging software and anti-fraud technologies.

Finally, the performance of the cyber resilience plans and the responsible team members must be appraised. The implementation of performance measurements techniques will assist in identifying areas of strength and weaknesses, helping form recommendations for senior management.

CONCLUSIONS

This study aimed to apply the SCP technique to cybercrime mitigation using South African cybercrime incidences as a case study. This was achieved with the use of fraud theoretical frameworks and SCP strategies. The SCP strategies were explained and linked to both remote and online crimes. Prevalent cybercrimes perpetrated in South Africa were highlighted with hacking examples. The SCP technique was tailored toward the mitigation of hacking and its prevalent forms. The SCP fraud prevention hardening framework was developed and validated using hacking incidences in South Africa. Policy recommendations were made to promote cyber resilience.

Many works have been reported on the mitigation of cybercrime in South African financial institutions; however, the application of SCP frameworks has been inadequately highlighted within the existing literature. Another novelty of this study lies in the application of SCP strategies for mitigating remote and online crime.

The study presents a timely exploration of applying SCP techniques to cybercrime mitigation, focusing on South Africa's cybercrime incidents. This choice lends specificity and depth to the analysis, allowing for a more nuanced understanding of the challenges and opportunities in mitigating cybercrime within a particular context. Additionally, the development and validation of an SCP fraud prevention hardening framework represent a significant contribution to the field, offering a practical tool for addressing cybercrime within the South African context.

The inclusion of policy recommendations demonstrates a consideration of the practical implications and necessary actions to combat cybercrime. The application of the SCP technique to cybercrime mitigation using South African cybercrime incidences provides conceptual frameworks and guidelines for applying the strategies to remote and online crime for the mitigation of hacking.

The frameworks can assist decision makers tackle cybercrime by reducing the opportunities and rewards for perpetration and increasing the risks and difficulties in accessing an individual's or organization's digital infrastructure.

This study is limited to the application of the SCP technique to the mitigation of hacking and its prevalent forms. Future studies can consider the application of the SCP strategies to other forms of cybercrime like phishing and cyberstalking.

AUTHOR NOTE

- Competing Interests: The authors declare no conflict of interest.
- Funding: No funding was received.
- Authors Contributions: The conceptualization, methodology, analysis, writing-original draft, resources, visualization, and editing were the collective work of the authors.

- Acknowledgement: The authors acknowledge the Tshwane University of Technology, Pretoria where this work was carried out

PROCESSING DATES

08, 2024

This manuscript was initially received for consideration for the journal on 03/12/2024, revisions were received for the manuscript following the double-anonymized peer review on 08/09/2024, the manuscript was formally accepted on 07/05/2024, and the manuscript was finalized for publication on 08/09/2024

REFERENCES

Accenture. (2020). *Insight into the cyber threat landscape in South Africa*. https://www.accenture.com/za-en/insights/security/cyberthreat-south-Africa

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020a). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime*, *27*(4), 1253–1271.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020b). Analysis of cyber-crime effects on the banking sector using balance score card: A survey of literature. *Journal of Financial Crime*, *27*(3), 945–958.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2021). The integration of forensic accounting and the management control system as tools for combating cyberfraud. *Academy of Accounting and Financial Studies Journal*, *25*(2), 1–14.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2022). Analytical hierarchy process decision model and pareto analysis for mitigating cybercrime in the financial sector. *Journal of Financial Crime*, *29*(3), 884–1008.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024a). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*, *31*(2), 287–301.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024b). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, *31*(1), 201–225.

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2024c). Development of a heuristic based mixed integer linear programming model for resources allocation during cyberfraud mitigation. *Operations Research Forum, 5*(2), 1–27.

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024d). The development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, *10*(e23491), 1–17. PMID:38187322

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring fraud: The internal auditor's perspective.* The Institute of Internal Auditors, Research Foundation.

Allen, K. (2021). *South Africa lays down law on cybercrime*. https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime

Armitage, R. (2018). Burglars' take on crime prevention through environmental design (CPTED): Reconsidering the relevance from an offender perspective. *Security Journal*, *31*, 285–304.

Back, S., & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 25–47.

Beebe, N. L., & Rao, V. S. (2005). Using situational crime prevention theory to explain the effectiveness of information systems security. In *Proceedings of the 2005 SoftWars Conference* (pp. 1–18).

Blasco, N. J., & Fett, N. A. (2019). Blockchain security: Situational crime prevention theory and distributed cyber systems. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 44–59.

Brantingham, P., & Brantingham, P. (1999). A theoretical model of crime hot spot generation. *Studies on Crime & Crime Prevention*, *8*(1), 7–26.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Situational crime prevention. In *Cybercrime prevention* (pp. 17–33). Springer International Publishing.

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1–11.

Clarke, R. (1995). Situational crime prevention. In M. Tony & D, Farrington (Eds.), *Building a safer society: Strategic approaches to crime prevention* (pp. 91–150). The University of Chicago Press.

Clarke, R. V., & Cornish, D. (1985). Modeling offender's decisions: A framework for research and policy. In Tonry, M., & Morris, N. (Eds.), *Crime and justice: An annual review of research* (*Vol. 6*, pp. 147–185). The University of Chicago Press.

Clayton, M. M. (2011). Investigative techniques. In Golden, T. W., Skalak, S. L., Clayton, M. M., & Pill, J. S. (Eds.), *A guide to forensic accounting investigation* (2nd ed., pp. 271–281). John Wiley & Sons.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Coles-Kemp, L., & Theoharidou, M. (2010). *Insider threat and information security management.* In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider threats in cyber security* (pp. 45–71). Springer.

Cressey, D. R. (1973). *Other people's money: A study in the social psychology of embezzlement*. Patterson Smith.

Cyber Exposure Index. (2020) https://cyberexposureindex.com/country-statistics/

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology Hacking Technology*, *15*, 277–305.

Decker, D., Blanc, A., Loveland, J., & Clayton, M. (2011). Data mining analysis of structured and unstructured information. In Golden, T. W., Skalak, S. L., Clayton, M. M., & Pill, J. S. (Eds.), *A guide to forensic accounting investigation* (2nd ed., pp. 333–362). John Wiley & Sons.

Deloitte. (2016). *Beneath the surface of a cyberattack*.https://www2.deloitte.com/us/en/pages/risk/articles/hidden-businessimpact-of-cyberattack.html

Delport, J. (2020). *Cybercrime has increased by 33*. IT News Africa., itnewsafrica.com/2020/05/cybercrime-has-increased-by-33-report-shows/

Fearn, N. (2017). *Critical lack of skills could be the biggest security challenge*. http://www.idgconnect.com/abstract /25505/criticallackskills-biggest-security-challenge

Global Cybersecurity Index. (2020). http://cybersecuritymag.africa/index.php/global-cybersecurity-index-2020-classsement-pays-africans?locale=en Global Cybersecurity Index, ITU Publications, Studies and Research (2018). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*, 383–402.

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational crime prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, *115*(102611), 1–23.

Hooper, M. J., & Pornelli, C. M. (2010). *Deterring and detecting financial fraud: A platform for action*. http://www.thecaq.org/docs/reports-andpublications/deterring-and-detecting financialreporting-fraud-aplatform-for-action.pdf

International Criminal Police Organization. (2021). INTERPOL report shows alarming rate of cyberattacks during. *COVID*, *19*, ●●●. https://www.interpol.int/en/Ww

IT News Africa. (2013). *MTN victim of cyber attack*.https://www.itnewsafrica.com/2013/08/mtn-victim-of-cyber-attack

Kaspersky. (2023). *Africa remains one of the regions most targeted by cybercrime in 2023*.https://kaspersky.africa-newsroom.com/press/africa-remains-one-of-the-regions-most-targeted-by-cybercrime-in-2023?lang=en#:~:text=In%20QQ3%202023%2C%20according%20to,ICS%20machines%20in%20Q3%202023

Kelly, P., & Hartley, C. A. (2010). Casino gambling and triangle, workplace fraud: A cautionary tale for managers. *Management Research Review*, *33*(3), 224–239.

Kenyon, W., & Tilton, P. D. (2011). Potential red flags and fraud detection technique. In Golden, T. W., Skalak, S. L., Clayton, M. M., & Pill, J. S. (Eds.), *A guide to forensic accounting investigation* (2nd ed., pp. 231–269). John Wiley & Sons.

Kirwan, G., & Power, A. (2013). Child predation and child pornography online. In Power, A., & Kirwan, G. (Eds.), *Cybercrime: The psychology of online offenders* (pp. 126–146). Cambridge University Press.

Kumudha, S., & Rajan, A. (2017). A critical analysis of cyber phishing and its impact on the banking sector. *International Journal of Pure and Applied Mathematics*, *119*(17), 1557–1569.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of Covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. PMID:36540648

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.

Lister, L. M. (2007). A Practical Approach to Fraud Risk: Comprehensive risk assessments can enable auditors to focus antifraud efforts on areas where their organization is most vulnerable. *Internal Auditor*, *64*(6), 61–66.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security : ... International Conference, ICISS ... : Proceedings*, *16*, 195–202.

Mcanyana, W., & Brindley, C. (2020). *Insight into the cyberthreat landscape in South Africa*. https://www.accenture.com/za-en/insights/security/cyberthreat-south-Africa

Miller, F. R., & Martson, D. L. (2011). Building a case: Gathering and documenting evidence. In Golden, T. W., Skalak, S. L., Clayton, M. M., & Pill, J. S. (Eds.), *A guide to forensic accounting investigation* (2nd ed., pp. 175–189). John Wiley & Sons.

Mittal, P., Kaur, A., & Gupta, P. K. (2021). The mediating role of big data to influence practitioners to use forensic accounting for fraud detection. *European Journal of Business Science and Technology*, *7*(1), 47–58.

Mngadi, M. (2018). *Presidency website up and running after hacking attack.*https://www.news24.com/news24/breaking-presidency-website-hacked-20180707

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), 135–143.

National Cyber Security Index. (2018). https://ncsi.ega.ee/ncsi-index/?order=-ncsi

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569.

Onodi, B. E., Okoye, E. I., & Egbunike, P. A. (2017). Application of fraud box-key model in the determination of fraud risk factors: Evidence from banks in Nigeria. *Journal of Global Accounting*, *5*(1), 99–112.

Padayache, K. (2015). A framework of opportunity-reducing techniques to mitigate the inside threat. In *2015 Proceedings of the information Security for South Africa, South Africa* (pp. 1–8).

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10 year review. *The African Journal of Information and Communication*, *28*, 1–21.

Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal*, *23*(2), 104–124.

Rasha, K., & Andrew, H. (2012). The new fraud triangle. *Journal of Emerging Trends in Economics and Management Science*, *3*(3), 87–94.

Rasool, F. (2012). *Postbank hacked for R42m.*https://www.google.com/amp/s/www.itweb.co.za/amp/content/nYZRM9JmKnqOgA8

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization prevention tactics for internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99–118.

Rick Crouch and Associates. (2020). *Cybercrime and South Africa.*https:rickcrouch.co.za/wp/cyber-crime-and-south-africa/

Rose, M. (2020). *Be wary of 'Coronamania' cybercrimes.*https://www.bizcommunity.com

Song, S. (2017). *African Undersea Cables – Interactive. Many Possibilities Blog.*https://manypossibilities.net/african-undersea-cables-interactive

South African Banking Risk Information Centre (SABRIC). (2021). *Annual Crime Statistics*https://www.sabric.co.za/media/5dlnhnyj/sabriccrimestats2021_fa.pdf

South African Institute of Chartered Accountants. (2021). *Protection of Personal Information Act.*https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPers onalInformationAct/tabid/3335/language/en-ZA/Default.aspx

Surfshark. (2022). *Cybercrime statistics.*https://surfshark.com/research/data-breach-impact/statistics

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

Timeslive. (2023). *41,000 Nedbank clients' cell phone no retrieved in cyber attack.*https://www.google.com/amp/s/www.businesslive.co.za/amp/bd/national/2023-03-24-4100 nedbank-clients-cellphone-numbers-retrieved-in-cyberattack/

Toona, M. (2022). *How the South African cybercrimes Act 19 of 2022 will affect individuals and businesses*. https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-business

United Nations Office on Drug Crime. (2013). *Comprehensive study on cybercrime*. https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Uppal, D., Mehra, V., & Verma, V. (2014). Basic survey on malware analysis, tools and techniques. *International Journal on Computational Sciences & Applications*, *4*(1), 103–112.

Van Zyl, G. (2016). *Standard bank computer system was hacked in R300 m ATM fraud hit.*https://www.news24.com/fin24/archive/tech/cyber-security/standard-bank-computer-was-hcked-in-r300m-atm-fraud-hit-report-20160630

Vidal, C., & Choo, K. K. R. (2018). Situational crime prevention and the mitigation of cloud computing threats. *Lecture Notes of the Institute for Computer Sciences*. *Social Informatics and Telecommunications Engineering*, *239*, 218–233.

Vieira, K., Schulter, A., Westphall, C., & Westphall, C. (2010). Intrusion detection for grid and cloud computing. *IT Professional*, *12*(4), 38–43.

Vona, I. W. (2008). *Fraud risk assessment: Building a fraud audit programme*. John Wiley & Sons.

Wilson, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communications of the ACM*, *52*, 133–138.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38–42.

Writer, S. M. (2023). *South Africa ranked 5th on global cybercrime density list*. https://www.itweb.co.za/content/KA3WwMdz1nBvrydZ

Oluwatoyin Esther Akinbowale is a postdoctoral research fellow at the Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa. Her research interests include forensic account, strategic management accounting, information and cybersecurity. Corresponding Author's Email: oluwatee01@gmail.com - https://orcid.org/0000-0001-5886-3018

Prof. Mulatu Fekadu Zerihun is a Professor of Economics and the Head of Economics Department at the Tshwane University of Technology, Pretoria, South Africa. Email: zerihunmf@tut.ac.za - https://orcid.org/0000-0003-4797-928X

Prof. Polly Mashigo is a Professor of Economics and the Executive Dean, Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa. Email: mashigomp@tut.ac.za - https://orcid.org/0000-0002-0810-1506