South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Understanding the cost of economic cybercrime in South Africa: An ambidextrous approach

Authors:
Motlalepule Zulu[1]
Ryno Boshoff[2]

Affiliations:
[1]Business School, Faculty of Business and Economic Sciences, Nelson Mandela University, Gqeberha, South Africa

[2]Department of Information and Communications Technology Services, Nelson Mandela University, Gqeberha, South Africa

Corresponding author:
Motlalepule Zulu,
s9844550@mandela.ac.za

Dates:
Received: 14 May 2025
Accepted: 20 Oct. 2025
Published: 06 Dec. 2025

How to cite this article:
Nelwamondo, M. & Njenga, J.K., 2025, 'Understanding the cost of economic cybercrime in South Africa: An ambidextrous approach', *South African Journal of Information Management* 27(1), a2029. https://doi.org/10.4102/sajim.v27i1.2029

Copyright:
© 2025. The Authors. Licensee: AOSIS. This work is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0/).

Read online:
Scan this QR code with your smart phone or mobile device to read online.

Background: Economic cybercrime (EC) has been a real and growing problem in South Africa (SA), which cannot be ignored. Although EC has cost South African-based organisations billions of rands, it was addressed in silos. Information and Communication Technology (ICT) organisations' approach to cyber-related crimes was proactive, while the South African Police Services' (SAPS) approach was reactive. This article infers that stakeholder cooperation was necessary for addressing the scourge of EC in SA.

Objectives: This study's objective was to understand the cost of EC on organisations in SA and to determine how ICT organisations in SA could support SAPS in policing EC.

Method: An archival strategy was used to collect archives of news reports and YouTube videos available in the public domain from 2016 to 2023.

Results: The cost of EC on SA-based organisations was both explicit and implicit. The explicit cost of EC was in (1) financial loss, (2) data loss and (3) downtime. The implicit cost, on the other hand, includes possible remediation cost and reputational damage. Moreover, the South African Banking Risk Information Centre and Council for Scientific and Industrial Research, through their respective interventions, demonstrate that an organisation can extend itself and thereby avail its resources for cybercrime policing collaboration purposes.

Conclusion: This article made it apparent that EC was costly on the SA economy; therefore, tackling this problem collaboratively with the involvement of Internet Service Provider Association would be useful for making an indelible mark on this phenomenon.

Contribution: This article adds to theory in the cybercrime and/or cybersecurity field because they are emerging disciplines by provisioning insight into how ICT organisations could simultaneously explore and exploit their resources while aiding SAPS to address EC in SA.

Keywords: economic cybercrime; cost of cybercrime; collaboration; ambidexterity theory; archives.

Introduction

The cybercrime phenomenon is pervasive, and its cost to South Africa (SA)'s ailing economy is significant. The effects of cybercrime could be dire on organisations because these crimes may lead to loss of revenue, expenditures associated with remediation costs, intellectual property theft, downtime, disruption to cyber-physical systems, loss of customer details and reputational damage (Curtis & Oxburgh 2023; PWC 2024; PWC_Report 2020). These forms of crimes may also result in an organisation facing bankruptcy or insolvency. It is worth noting that the ultimate cost of cybercrime is its negative effect on a country's economic growth.

Similarly, to remain resilient against attacks and threats, organisations ensure that preventative measures are put in place. In addition, organisations' attitude towards cybercrime is that of ensuring that their data, systems and network environments are secure. It is noteworthy that despite these efforts, cybercriminals still gain access to organisations' network environments and/or websites and thus launch attacks against organisations.

This article provides insight on the utilisation of contextual ambidexterity for economic cybercrime (EC) policing collaboration between Information and Communication Technology (ICT) organisations and South African Police Services (SAPS). The contextual ambidexterity approach refers to the fact that an organisation can simultaneously explore and exploit organisational activities (Cannaerts, Segers & Warsen 2020). This means contextual ambidexterity is achieved by using the same resources for operational duties while allocating some time to attend to innovative activities (Syed, Blome & Papadopoulos 2020). This approach could be

useful because organisations have resource capabilities; SAPS, on the other hand, have challenges fulfilling their mandate to investigate cybercrime as per *Cybercrime Act* (CCA) (*Cybercrimes Act, 2020* 2021). Therefore, we infer that organisations' resources could be availed on an ad hoc basis for stakeholder empowerment; in this way, operations are unaffected. This article answers the research question: 'How are the assumptions held by both stakeholders framing the policing of EC in South Africa?'

Literature review

Similar work to this article is a study conducted by Ojedokun and Oshilaja (2022) through which they investigate cybercrime policing in Lagos, Nigeria. The authors posit that cybercrime cases (1) were handled differently and (2) were attended to regularly by cybercrime-trained police in Lagos; however, (3) there was no cybercrime unit in place (Ojedokun & Oshilaja 2022). They argued that although processes were in place to address cybercrime, the lack of adequate tools and financial issues often hindered their effectiveness (Ojedokun & Oshilaja 2022). Another similar study to this article investigated EC policing challenges in the United Kingdom (Akdemİr, Sungur & Basaranel 2020). The authors stated that the main challenges in EC policing were (1) international collaborations, (2) the lack of reporting and (3) the lack of cyber awareness (Akdemİr et al. 2020). Akdemİr et al. (2020) contended that although Public Private Partnerships (PPP) were considered ideal for combatting EC, police officers were sceptical of partnering with the private sector because of confidentiality concerns. Their study made it apparent that the reasons why there were minimal EC prosecutions were because of (1) the lack of evidence preservation and collection and (2) capacity issues to investigate EC (Akdemİr et al. 2020). The authors recommended stakeholder collaboration, stating that outsourcing alone was an ineffective solution for EC policing (Akdemİr et al. 2020).

Similarly, Paek, Nalla and Lee's (2020) article wherein they investigated police officers' attitudes in Korea as it pertains to PPP in policing EC is closest to this article. The study indicates that police officers deemed PPP necessary for addressing cybercrime (Paek et al. 2020). The authors infer that in cross-sectoral partnerships, it is important that power parities are considered and respected (Paek et al. 2020). As such, a memorandum of agreement or terms of reference (TOR) that clarifies each stakeholder's duty would be useful in guiding the partnership. It is worth mentioning that, to our knowledge, there is no literature whereby ambidexterity theory is used in an SA context, cross-sectorally between ICT organisations and SAPS for EC policing.

Research problem

The cybercrime phenomenon is a complex issue worldwide, which is costing SA's economy billions annually. The South African Banking Risk Information Centre (SABRIC) 2023 report indicates that the total potential losses reported to SABRIC were R23 723 099 523; actual losses equate to R3 357 849 785 (SABRIC 2023). Moreover, the Check Point 2024 African Perspectives on Cyber Security report estimated that cybercrime costs SA 1% of its gross domestic product (Khoza 2024). The report further indicates that on a weekly basis, SA government institutions experienced 3312 attacks, and there was a 90% increase in ransomware attacks (Khoza 2024). Similarly, the PWC 2024 report in which 94 SA organisations participated in the survey indicates that data leaks were a major risk and threat to organisations' reputations (PWC 2024). The report further indicates that the data breach cost to SA organisations over a 3-year period was between R1 759 000 and R8 794 982.41 (PWC 2024). As a result, 47% of the 94 organisations indicated that they were worried about cloud-related threats (PWC 2024). Thus, in an effort to be proactive, (1) 66% had risk mitigation investment, and (2) 29% planned to increase their cyber budget in 2025 (PWC 2024).

We understand that in SA crime in general is rampant, and, therefore, it is no surprise that there would be competing interests when it comes to policing EC. Conventional crime, as dubbed by Borwell, Jansen and Stol (2021), gets more attention in comparison to EC. For instance, if an individual goes to report a burglary at the police station, police will know what to do. However, when it comes to EC, the response at police stations is likely to be different. Notwithstanding, the CCA criminalises cybercrime; however, SAPS seem to perceive cybercrime as an add-on to their duties (*Cybercrimes Act, 2020* 2021). This article is premised on provisioning insight on mechanisms that can be explored to police EC in SA.

Ambidexterity theory

The theory of ambidexterity holds that an organisation ought to be able to balance out exploration and exploitation to remain competitive (Cannaerts et al. 2020). Exploration has to do with innovation, adaptation, audaciousness and the ability to search for new knowledge, ways and means to do something new or better, among others (March 1991), whereas exploitation is about improvement, efficiency, selection and implementation, among others (March 1991). Exploration focuses outwardly, whereas exploitation centres around internal activities (Syed et al. 2020). The pursuit of exploration with no consideration for exploitation could result in investments that yield low returns (March 1991; Vieru et al. 2021), whereas a sole focus on exploitation might result in monotony and low performance and could affect the organisation's competitiveness (Vettorello, Eisenbart & Ranscombe 2020; Vieru et al. 2021). Cannaerts et al. (2020) argue that the public sector is more prone to exploit than to explore, while the private sector is likely to apply both approaches. Syed et al. (2020) argue that although there are claims that small and medium enterprises either explore or exploit; however, such claims lack analysis. Therefore, to balance both concepts is a challenge for small and medium enterprises because they might not have enough resources for both.

The theory of ambidexterity is applied primarily within an organisation, inter-departmentally. It is worth mentioning that it is also applicable inter-organisational and cross-sectoral (Page et al. 2021; Westergren, Holmström & Mathiassen 2019). Similarly, when ambidexterity theory is applied from a cross-sectoral perspective, Page et al. (2021) posit that trust and support are as important as the other principles, which are alignment and adaptation when working collaboratively. Therefore, the lack of these ambidexterity theory principles could be a limitation and might frustrate the process of policing EC collaboratively in SA.

The three types of ambidexterity are discussed as follows:

- Structural ambidexterity: refers that organisations need to set up structures that focus on exploration and exploitation separately. By separating the departments, one department takes care of the day-to-day activities (exploit), while another department searches for new opportunities (explore) (Syed et al. 2020; Vieru et al. 2021).
- Temporal ambidexterity: refers to exploration and exploitation being pursued one after the other. The authors warn that this is not always the best approach because one approach can be exhausted at the expense of the other. Moreover, this approach could lead to unnecessary competition, which is not conducive to efficiency and adaptation (Syed et al. 2020).
- Contextual ambidexterity: this approach enables us to understand that exploration and exploitation are applied based on what the situation dictates. This approach is ideal for this article because when the situation arises in terms of a cyber-related attack, the affected organisation ought to attend to its operations while making means for SAPS to investigate. Syed et al. (2020) argue that a balance between exploration and exploitation is not always plausible, nor is it easy to achieve. We infer that if this approach is integrated into an organisation's policy, process or procedure, it is doable.

Research objectives

- To determine the cost of emerging cyber trends of threats and vulnerabilities in cyberspace.
- To provide insight on how ICT organisations could support SAPS in the policing of EC in SA.

Research methods and design

This article is premised on the qualitative research design because we envisaged to gain deeper insight of EC experienced by organisations in SA from 2016 to 2023 by exploring archives. The qualitative research method enabled us to gain a better understanding of cyber-related threats, attacks and breaches, which occurred from 2016 to 2023 (Creswell & Creswell Báez 2021). Moreover, the qualitative method is useful when we envisage ways to probe and understand meanings and preferences that relate to the EC phenomena (Creswell & Creswell Báez 2021). Similarly, the archival strategy was employed to gain insight on the effects of cyber-related attacks, such as ransomware and breaches, on organisations in SA.

Google was the main search engine used to gather information from both local and international websites. The key words used to search for data from 2016 to 2023 were (1) cyber-attacks in SA, (2) cyber incidents experienced by South African organisations, (3) insider threats in SA, (4) data breaches in SA, (5) data leaks in SA and (6) ransomware attacks in SA. Table 1 illustrates sources of information through which cyber incidents, cyber-attacks, data breaches and/or leaks were reported and/or discussed. The 25 sources illustrated in Table 1 provisioned 73 archives. Table 1 shows the 12 online newspapers, which were the main sources of information for this article.

Archives of cyber-related incidents from 2021 to 2023 were sourced from the various YouTube channels illustrated in Table 2. Table 2 further refers to the STORM Guidance panel discussion, which involved a SAPS representative, the SA Information Regulator representative, a cyber expert from STORM Guidance and an SA lawyer. The two YouTube videos from the SA news broadcasters referred to in Table 2 involved interviews between their respective news anchors with cyber experts. The other interview on ENCA was a panel discussion pertaining to the cybercrime agreement between France and SA. The panellist consisted of the French ambassador, an SA representative and a cybersecurity adviser. Table 2 also refers to the CSIRNewMedia video, which contains a discussion pertaining to the Designated Point of Contact (DPOC) project at the Council for Scientific and Industrial Research (CSIR).

TABLE 1: Sources of information for archives.

Media	Source
Online newspaper	BusinessTech
	MyBroadband
	ITWeb
	News24
	BleepingComputer
	BusinessLive
	Timeslive
	Stuff
	Daily Maverick
	Citizen
	GroundUp
	Amabhungane
YouTube videos	SABC News
	ENCA
	Newzroom Afrika
	Storm Guidance Panel Discussion
	CSIRNewMedia
Reports	Accenture
	National School of Government (NSG)
	Information Regulator
Company website	Isite
	ABSA
Magazine	CPO Magazine
Scholarly article	Pieterse (2021)

SABC, South African Broadcasting Corporation; ENCA, eNews Channel Africa; CSIR, Council for Scientific and Industrial Research; CPO, Magazine: Chief Privacy Officer.

All archives relating to the study, except the YouTube videos were first saved in folders based on the year the incident occurred. The author later captured the archival data on Microsoft Excel, and worksheets were named by year from 2016 to 2023. The data were categorised accordingly on each worksheet based on data source, publishing date, organisation that suffered attack, incident description, incident type, vulnerability type, perpetrator and post-attack action. Similarly, the YouTube videos were listened to and captured word for word on Microsoft Excel. For trustworthiness purposes, a verbatim excerpt of the comment made by the SA Information Regulator representative follows. *One of the first breaches that was reported to the regulator was an insurance company; they were moving applications for insurance policies from one Rustenburg office to Johannesburg and the robbers got the wrong tip-off; they then went and hijacked that truck. They sold 14 000 applications of insurance policies that include IDs and bank accounts. These incidents are rising by the numbers*. Each YouTube video was captured on a separate worksheet. The data corpus was later imported to the NVivo 14 application. Because this study employs Braun and Clarke's (2021) reflexive thematic analysis phases, data familiarisation, which is the first phase of the reflexive approach in thematic analysis, was used (Braun & Clarke 2021). Data familiarisation was useful to provide insight into the (1) type of incidents launched against organisations and (2) the cost of cyber-related incidents on organisations in SA from 2016 to 2023. This phase was followed by the coding of data, which lead to the generation of initial themes (Braun & Clarke 2021).

Ethical considerations

Ethical clearance to conduct this study was obtained from the Nelson Mandela University (NMU) Research Ethics Committee (Human) (REC-H) (No. H23-BES-BUS-072). The NMU permits its students to collect data once they have attained ethical clearance from the institution. The author and co-author both attended the Training and Resources in Research Ethics Evaluation online as required by the NMU REC-H. Moreover, the author and co-author completed modules 1–3 of the Training and Resources in Research Ethics Evaluation training. The author submitted the ethical clearance application at the NMU. The application was accepted and approved at the NMU, thus enabling the researcher to proceed with data collection. The duration of the clearance was for the period 28 September 2023 – 28 September 2024.

Results and discussion

The archives will enable the researchers to identify and know the type of attacks experienced by organisations in SA from 2016 to 2023. Moreover, insight into vulnerabilities that were exploited to gain access to the organisation's environment and thereby launch attacks from the 2016–2023 archives will be provisioned. Furthermore, a discussion on the cost of attacks and immediate challenges faced by organisations in SA because of the compromise will ensue. Similarly, insight into the responses undertaken by organisations post-attack will be provisioned. Moreover, responses undertaken by organisations to contain the attack will be discussed. In addition, insight pertaining to collaborations undertaken by (1) SAPS with the banking industry, (2) the CSIR and (3) the French and South African governments' cybercrime agreement, respectively, to address cybercrime in SA will ensue.

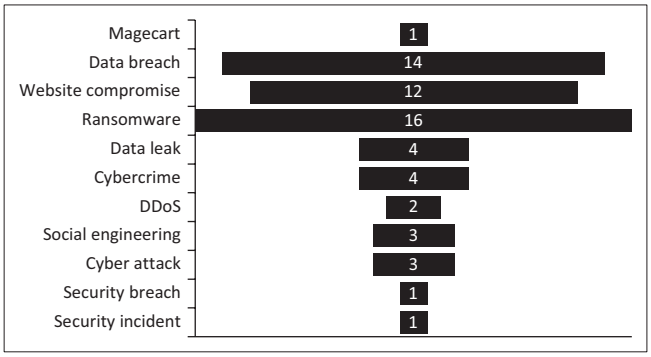
Figure 1 illustrates the 11 types of cyber-related incidents that were experienced by 57 organisations in SA from 2016 to 2023. Figure 1 further depicts that the most predominant incidents between 2016 and 2023 were ransomware attacks, followed by data breaches and then website compromises. This information is consistent with the Checkpoint 2024 African Perspectives report, which indicated that on a weekly basis, SA government institutions experienced 3312 attacks, and there was a 90% increase in ransomware attacks (Khoza 2024). Figure 1 also shows that data breaches were the second largest form of attack experienced by organisations in SA. The data are congruent with Bisogni and Asghari's (2020) assertions that data breaches were predominant mechanisms used by cybercriminals to gain unauthorised access. Because this is a qualitative study, we understand that although the numbers in Figure 1 might not look significant, financial losses associated with these disruptions were huge.

TABLE 2: YouTube archives.

Year	YouTube channel	Video title	Link
2021	STORM Guidance	Cybercrime and its impact on businesses in South Africa	https://www.youtube.com/watch?v=BLgCwenGs4s&list=PPSV
2022	SABC News	Interpol's concerns over increase in cybercrimes in Africa: Jan Vermeulen	https://www.youtube.com/watch?v=zbhiUawfI-M&list=PPSV
2023	ENCA	Cybercrime in SA 'Personal info data breaches rife in SA'	https://www.youtube.com/watch?v=-kmIPSJkeJs&list=PPSV
2023	ENCA	Panel Discussion | Cybercrime Agreement	https://www.youtube.com/watch?v=WLUvZmTQAG0&list=PPSV
2023	CSIRNewMedia	Cybercrime and South Africa: An Introspective Look'	https://www.youtube.com/watch?v=9yuv8DUZCKs&list=PPSV

Note: Please see the full reference list of this article, Nelwamondo, M. & Njenga, J.K., 2025, 'Understanding the cost of economic cybercrime in South Africa: An ambidextrous approach', *South African Journal of Information Management* 27(1), a2029. https://doi.org/10.4102/sajim.v27i1.2029, for more information

SA, South Africa; SABC, South African Broadcasting Corporation; ENCA, eNews Channel Africa; CSIR, Council for Scientific and Industrial Research.



DDoS, Distributed Denial of Service.

FIGURE 1: Incident type 2016–2023.

Figure 2 illustrates the nine types of vulnerabilities that were exploited by attackers to gain access to 54 organisations' systems, network or websites in SA from 2016 to 2023. Moreover, Figure 2 shows that most vulnerabilities exploited were categorised as Unknown; those were vulnerabilities that were unclassified in the archives. Similarly, Figure 2 shows that unauthorised access was a vulnerability used to gain access to seven organisations' networks and websites, among others. Figure 2 also shows that Access Privileges and Passwords were vulnerability explored twice to gain unlawful entry. Kayes et al. (2020) confirm that data breaches sometimes occurred because of weaknesses in access control. Likewise, the Ponemon 2024 report indicates that 16% of the malicious breaches occurred because of stolen or compromised credentials (IBM & Ponemon Institute 2024).

Table 3 illustrates costs which the organisations had to bear because of attacks being launched against them. Moreover, Table 3 shows that EC affected organisations in the private sector, public sector and even academic institutions in SA from 2016 to 2023. Attacks launched against Hetzner SA and Telkom, as illustrated in Table 3, prove that even ICT organisations were not immune from cyber-related crime. Financial losses incurred were as follows: *Standard Bank – R300 million; City of Tshwane – R53 million; in 2020, Postbank had to replace 12 million cards and the estimated cost was R1 billion*. Similarly, on two separate incidents in 2022, *Postbank lost R18 million* and *R90 million*. What is unfortunate is that there is no clarity on whether the perpetrators at Postbank were found and subjected to disciplinary action. Liberty's financial losses were estimated to be around *R1.68 billion; their market share dropped by 4%*, and the incident could have potentially threatened their reputation. Meanwhile, the University of Mpumalanga lost R2989.75. In 2023, TransUnion and Experian were both attacked, and a *ransom of R562 500 000 was demanded* from each organisation.

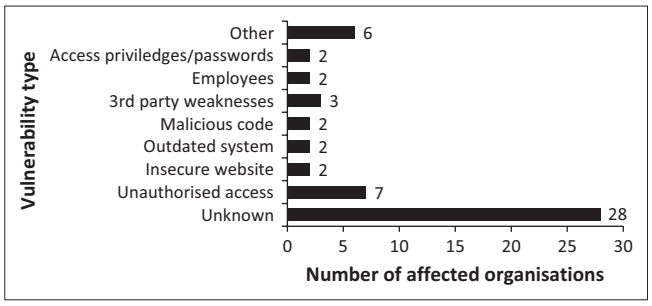


FIGURE 2: Vulnerability type 2016–2023.

Craig (2021) claimed that organisations in SA lose approximately R2 billion annually to cyber-related attacks and/or breaches. The SABRIC 2023 report indicated that actual cybercrime-related losses were approximately R3 billion (SABRIC 2023). According to the empirical findings, the cost of EC to SA organisations was in billions, only in 2018, 2020 and 2023, as illustrated in Table 3. Similarly, Table 3 illustrates that the financial losses incurred were in millions in the years 2016, 2019, 2021 and 2022. Notwithstanding, the cost of EC on SA organisations is concerning because SA (1) is an emerging economy and (2) the unemployment rate is high.

Moreover, the findings that pertain to data leaks made it apparent that personal details of (1) individuals in SA, such as *names, identity numbers, contact numbers and banking details*, and (2) organisations in SA were compromised. Table 3

TABLE 3: Cost of threat.

Year	Financial loss (Rands)	Data leak (Records)	Downtime	Possible remediation costs	Threat to brand reputation
2016	Standard Bank (R300m)	GCIS (1500 records) Ethekwini	N/A	Armscor	N/A
2017	N/A	Jigsaw Holdings (75 m records) Old Mutual Hetzner SA	Telkom	Telkom	Jigsaw Holdings
2018	Liberty (R1.68 billion)	Liberty Government (934 000 records)	N/A	N/A	Liberty
2019	City of Tshwane (R53m)	Eskom Garmin (6700 records)	City Power Garmin City of Johannesburg SASSA	N/A	N/A
2020	Postbank (R1 billion)	Postbank Nedbank (1.7 m records) Experian (24 m and 800 000 records)	Life Healthcare Group Tracker The National School of Government	Lombard Insurance Life Healthcare Group	Experian
2021	DoJCD (R5m) University Of Mpumalanga (R2989.75)	DoJCD (1200 records) DebtIn Consultants (1.4 m records)	DoJCD Transnet	N/A	DebtIN Consultants
2022	Postbank (R18m) Postbank (R90m)	TransUnion Dischem	N/A	TransUnion Dischem	TransUnion
2023	Experian (R562.5m) TransUnion (R562.5m)	Experian TransUnion Vumacam Tshwane University of Technology DBSA Clicks	N/A	N/A	N/A

SA, South Africa; GCIS, Government Communication and Information System; DoJCD, Department of Justice and Constitutional Development; DBSA, Development Bank of Southern Africa; SASSA, South African Social Security Agency.

illustrates the organisations that were hacked or attacked, and, as a result, personal details were leaked or exposed. The biggest data compromise contained *75 million records at Jigsaw Holdings*, followed by *54 million records at TransUnion*, as illustrated in Table 3. It is worth noting that the cost of data loss or compromise is that its confidentiality, integrity and availability cannot be determined. It is worth mentioning that no penalties were imposed prior to 2021 because the *Protection of Personal Information Act* was enacted on 01 July 2020, and organisations had a 1-year grace period to comply. However, in 2023, the *Department of Justice and Constitutional Development was served with an R5 million penalty for failing to comply* (Moyo 2023).

Table 3 further illustrates that 10 organisations suffered downtime during the attacks. It is worth mentioning that City Power, City of Johannesburg, Life Health Group and Transnet evoked their business continuity. Although for some organisations, continuity was employing manual processes so operations could continue. It is worth noting that the cost of downtime cannot be estimated. Similarly, archives indicate that part of the response of organisations shown under possible remediation costs in Table 3 was to call in external cyber and forensic experts after the incidents. There are remedial costs associated with calling in experts, which the organisation pays to get their systems up and running.

In this instance, the archives did not categorically mention that such costs were incurred, but there is a high likelihood that the organisations paid such; however, the estimate of such costs cannot be made. Moreover, incidents that were launched against Jigsaw Holdings, Experian, DebtIn Consultants and TransUnion whereby millions of South African citizens' personal data were leaked and, in other instances, exposed could cost their brand reputation significantly because some clients would feel that their data would not be safe if they gave those organisations business.

The literature aligns with the findings and therefore makes us understand that the cost of EC could be attributed to (1) loss of revenue, (2) expenditures associated with remediation costs, (3) intellectual property theft, (4) downtime and/or disruption to cyber-physical systems, (5) loss of customer details and (6) reputational damage (Curtis & Oxburgh 2023; PWC 2024; PWC_Report 2020). Interestingly, Holt and Kennedy (2020) argued that organisations' lack of transparency regarding an attack or breach could be guided by the fear of (1) losing customers and (2) encountering a decline in share price. Thus, in an effort to avoid humiliation over data loss, an organisation may attempt to conceal or not fully disclose the extent of the compromise (Holt & Kennedy 2020).

Post-attack challenges and responses

It is noteworthy that system or website inaccessibility and the lack of robust responses were the two overlapping challenges as suggested by the data archives. In Telkom's case, the system's inaccessibility was because of the WannaCry attack. The Department of Environmental Affairs, on the other hand, had their website defaced. Moreover, the data from the archives indicate that (1) in City Power's case, *there were delays in response to outages*, (2) Life Healthcare Group clients were subjected to *administrative delays* and (3) *Transnet was up only after a week*. Moreover, mitigation processes undertaken include:

- cyber experts conducting a forensic analysis to determine the full extent of the incident
- more stringent controls being implemented
- vulnerability being fixed or patched
- robust defensive strategies being invoked across the industry
- revoking all third-party access to information systems and
- immediate invoking of standby cyber and information technology protection protocols.

Similarly, archives showed that in containing the attack, (1) systems were shutdown, (2) the organisation immediately took its systems offline, (3) *we have agreed with them that they shut themselves off from the Internet*, (4) *we deleted all the Nedbank data off their server*, (5) access to the Information Technology infrastructure was immediately restricted across the business and (6) Transnet *users were urged to refrain from accessing the network, which includes no email access and could not even use Microsoft Teams on mobile devices*. Moreover, archives made us understand that post-attack, an *incident briefing* is important *to ensure that executive management and the technical staff all understand what happened and how they can avoid the situation in the future*.

Required interventions for cybercrime policing

This section enables us to understand the EC problem from the policing point of view. Moreover, insight on the required interventions and mechanisms to address EC will be provisioned. Similarly, insight from the STORM Guidance panellist, the SABC News interview and the ENCA interview based on their respective experiences will be provisioned accordingly. The findings from the STORM Guidance panel discussion follow:

The *SAPS representative* indicated that SAPS is mandated by the CCA to satisfy its requirements by ensuring that there is (1) *internal capacity building*, (2) a *DPOC*, (3) *a reliable and effective policing model in the short, medium and long term* and (4) a *multi-disciplinary task team* (*Cybercrimes Act, 2020* 2021). The *SAPS representative* further indicated *that cybercrime requires highly specialised law enforcement response. South African Police Services and law enforcement on* their *own cannot address cybercrime successfully.* The *SAPS representative* further added that *SAPS requires an online reporting mechanism and a rapid response protocol. Moreover, a stakeholder partnership where people within the industry that has the necessary expertise* could *assist law enforcement in addressing the criminal value chain* is required. *Stakeholder partnership for law enforcement is extremely important, and this is where the business fraternity can come in and assist SAPS. What the police are doing is to have a unique policing model in terms*

of cybercrime that is unique, given the specific circumstances in SA. We have done a lot of research pertaining to different policing throughout the world.

Similarly, the STORM Guidance *cyber expert* indicated that *law enforcement budgets* targeted *cyber criminals higher up the chain. They want to spend the money where they can make a biggest difference. They are trying to take out the big cyber-criminal groups and that means that they have limited capability to help individual organisations.*

The *Information Regulator representative* inferred that *on a capacity scale, government needs to put in more money into training more people in the police services.*

The cyber expert who was interviewed on SABC News indicated:

W*e have waited for* cybercrime *to become a crisis before addressing the issue. Members of the industry have warned for a long time that now* there are *hacking groups* informing the *media* that *SA is a playground for cybercriminals.* These cybercriminals *can get people's personal information, including that of President Cyril Ramaphosa, with ease, and it is because* the government has not invested enough in cybersecurity. *More investment has been made in the private sector, especially businesses that rely on the safety of their online systems, like banks, etc. The government is unfortunately very far behind, and they handle incredibly sensitive information of its citizens.*

However, the cyber expert who was interviewed on ENCA indicated that:

W*e do not have enough people trained. That is why it is important for the police to partner with cybersecurity experts and learn about the latest models. It is very crucial for the police to* receive *continuous professional education and* attend *workshops so they can know the latest models and modus operandi when it comes to these types of crimes. It helps them to know case by case what they are dealing with.*

The findings confirm Ojedokun and Oshilaja's (2022) assertions that cybercrime policing requires law enforcement to (1) be trained, (2) have adequate tools, (3) address capacity issues and (4) have the necessary funding. The authors identified the above-mentioned challenges as hindrances in the policing of cybercrime (Akdemİr et al. 2020; Ojedokun & Oshilaja 2022). Moreover, the findings are consistent with literature and thereby indicate that increased collaboration is paramount because the private sector has infrastructure, tools and expertise that are useful for the effective policing of EC (Koziarski & Lee 2020; Paek et al. 2020).

Stakeholder empowerment initiatives

Furthermore, this article enabled us to grasp that the banking industry works collaboratively through SABRIC. South African Banking Risk Information Centre supports the banking industry by addressing industry-related matters such as financial fraud and/or crime; this includes cyber-related financial crime (BASA 2023). In essence, SABRIC provides information on what is happening in the banking industry, and that information is available on their website (BASA 2023). For instance, to confirm that there is information sharing in the banking industry, in response to the attack, *the DDoS attack targeting the banking industry started with a ransom note*; however, *robust defences were* implemented *across the banking industry to minimise the impact* on its *customers* (Moyo 2019). Moreover, the data enabled us to understand that through its Financial Forensic Analysis Centre, the Banking Association of South Africa and SABRIC have also collaborated with the Directorate for Priority Crime Investigation (DPCI), which is a division in SAPS (BASA 2023). The collaboration *provides insight and skills to 40 DPCI investigating officers on various software, and it is aimed at quickening incident response*. Similarly, the *collaboration is intended to drive high ethical and professional standards and innovation* among the stakeholders (BASA 2023). It is noteworthy that this collaboration was guided by the need to have SA *removed from being grey listed by the Financial Action Task Force*, among other things (BASA 2023). Although the TOR guiding the collaboration is unknown, BASA (2023) made it apparent that DPCI maintains its independence, principles and transparency. Notwithstanding, a collaboration of this nature confirms that contextual ambidexterity is plausible for policing purposes. We infer that more initiatives of such a nature are necessary; however, more proactive approaches are required because the collaboration seems to have been brought about by the Financial Action Task Force issue.

Similarly, insight was also gained that the CSIR, which is an entity of the Department of Science and Innovation, worked collaboratively with SAPS to put the DPOC in place. The DPOC project is an initiative guided by the CCA through which cybercrime will be reported at a central place. *The SAPS team is being housed at the CSIR campus; CSIR is providing SAPS with expertise and support in designing and implementing the DPOC. South African Police Services is offered forensic and cybercrime/cybersecurity expertise to collaboratively ensure that the DPOC will serve* SA. This information was shared in 2023; it is not known when the DPOC will commence its services. What is known is that the DPOC will become a SAPS internal process, individuals will still be required to report cybercrime at local police stations and the call will be logged internally to DPOC. It can be argued that CSIR has resource capabilities to engage in such projects. We infer that an organisation is not bound to replicate CSIR methodology, but flexibility can be exercised in how collaboration is undertaken.

The France and SA governments have entered into a cybercrime agreement with the intention to aid *the private and public sectors to boost SA cyber defences.* The SA representative enabled us to understand that *the anti-corruption academy, which* would *be at the* Special Investigation Unit (SIU), would *be open to train firstly 20 SIU staff. These staff members will then*

become trainers; the training will be extended to young staff members in law enforcement that deals with investigations. The SIU project's ultimate goal is *to benefit Africa at large*. These three projects somewhat challenge the notion that SAPS is not interested in addressing cybercrime; however, in SA, more of these initiatives are required between both organisations and SAPS.

Recommendations

While efforts undertaken by the banking industry and CSIR are welcomed, we assert that more work needs to be done to address cybercrime in SA. The Internet Service Provider Association (ISPA) has a role to play; they are supposed to be spearheading these efforts because Internet Service Providers (ISPs) facilitate the distribution of Internet traffic into SA. Thus, visibility of the ISPA is necessary to narrow the existing gap between ISP and SAPS in policing cybercrime. Because the DPOC go-live is still pending, we infer that the ISP could support SAPS with infrastructure to operationalise the DPOC. Moreover, ISPA could play a crucial role by informing and/or assisting SAPS to broadcast trends of known and emerging attacks on the cybercrime repository. The cybercrime repository could be availed to organisations in SA through read-only access.

A meaningful collaboration between ISP and SAPS can be facilitated by the ISPA. Moreover, collaboration could be made possible through a Memorandum of Agreement or TOR to ensure that all stakeholders understand their roles and responsibilities. The Memorandum of Agreement or TOR could address stakeholders' concerns around (1) confidentiality, (2) trust and (3) resource allocation and (4) segregation of duties, but not be limited to them.

Limitations

The lack of response from the cybersecurity hub deprived the study information and insight of the depth of the cybercrime problem in SA. Therefore, no insight could be gained pertaining to how cybercrime cases were escalated to the cybersecurity hub. Similarly, insight into how many cases were reported and the type of attacks that were predominant could not be gained. The researcher could only make use of information available in the public domain.

Future studies

We acknowledge that Metropolitan Municipalities in SA are hubs for economic activity. Therefore, for future work, we suggest that a case study which investigates cybercrime policing readiness at the Metropolitan Municipalities level be undertaken. Furthermore, a study that investigates how SAPS could implement a central cybercrime repository wherein information on new, emerging and predominant attacks would be made accessible to organisations without infringing on the *Protection of Personal Information Act* (*POPIA*) would be useful.

Conclusion

In answering the research question '*How are the assumptions held by both stakeholders framing the policing of EC in South Africa?*' This article made it apparent that although EC is costly for SA organisations, it is not adequately addressed. The current approach adopted by organisations and SAPS, respectively, is linear; the EC problem demands collaboration. Although the organisation's approach is proactive in that they ensure that they have adequate security tools in place, their focus seems to be solely on operations restoration. It is worth noting that this article does not seek to undermine significant losses, which an organisation might incur because of a cyber-related attack. This article infers that organisations can make a meaningful contribution by addressing cybercrime collaboratively with SAPS. South African Police Services, on the other hand, is mandated by the CCA to investigate cybercrime; however, they do not embrace their role because of capacity and capability challenges. We understand that the DPOC project is underway, and we trust that it will serve SA adequately. It is apparent that the banking industry's role and contribution are evident; we infer that ISPA visibility is imperative for cybercrime policing in SA. A safe cyberspace is conducive for economic growth and is important for SA organisations to thrive.

Acknowledgements

The research presented in this article formed part of Motlalepule Zulu's postgraduate studies and was originally conducted as part of their Doctoral thesis titled 'Cybercrime policing collaboration in South Africa: An Exploratory Study', Faculty of Business and Economic Sciences, Nelson Mandela University in 2025, under the supervision of Ryno Boshoff and Cecil Arnolds. The thesis will be submitted in partial fulfilment of the requirements for the PhD degree. The manuscript has been revised and adapted for journal publication.

This article is based on a conference paper originally presented at the 20th International Conference on Cyber Warfare and Security (ICCWS 2025), held in Williamsburg, Virginia, USA, on 28–29 March 2025. The conference paper, titled 'Cybercrime Policing Collaboration in South Africa: Exploring A Stakeholder Approach', was subsequently expanded and revised for this journal publication.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

CRediT authorship contribution

Motlalepule Zulu; Writing – original draft. Ryno Boshoff; Supervision. All authors reviewed the article, contributed to the discussion of results, approved the final version for submission and publication, and take responsibility for the integrity of its findings.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that supports the findings of this study are available from the corresponding author, M.Z. upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

AkdemİR, N., Sungur, B. & Basaranel, B.U., 2020, 'Examining the challenges of policing economic cybercrime in the UK', *Güvenlik Bilimleri Dergisi Şubat* 113–134. https://doi.org/10.28956/gbd.695956

BASA, 2023, *Financial forensic analysis centre*, p. 1, BASA, viewed 11 March 2025, from https://www.banking.org.za/news/financial-forensic-analysis-centre/?cn-reloaded=1.

Bisogni, F. & Asghari, H., 2020, 'More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws', *Journal of Information Policy* 10, 45–82. https://doi.org/10.5325/JINFOPOLI.10.2020.0045

Borwell, J., Jansen, J. & Stol, W., 2021, 'Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions', *Journal of Digital Social Research* 3(3), 85–110. https://doi.org/10.33621/jdsr.v3i3.66

Braun, V. & Clarke, V., 2021, 'Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches', *Counselling and Psychotherapy Research* 21(1), 37–47. https://doi.org/10.1002/capr.12360

Cannaerts, N., Segers, J. & Warsen, R., 2020, 'Ambidexterity and public organizations: A configurational perspective', *Public Performance and Management Review* 43(3), 688–712. https://doi.org/10.1080/15309576.2019.1676272

Craig, N., 2021, 'Cybercrimes on the up, with SA annually losing about R2.2 billion', *IOL*, 04 December, viewed 13 March 2023, from https://www.iol.co.za/sunday-tribune/news/cybercrimes-on-the-up-with-sa-annually-losing-about-r22-billion-974c9f5c-40f4-46fa-9a36-2ac9678463bb.

Creswell, J.W. & Creswell Báez, J., 2021, *30 essential skills for the qualitative researcher*, 2nd edn., Sage Publications, Thousand Oaks, CA.

Curtis, J. & Oxburgh, G., 2023, 'Understanding cybercrime in "real world" policing and law enforcement', *Police Journal* 96(4), 573–592. https://doi.org/10.1177/0032258X221107584

Cybercrimes Act, 2020, 2021, Pub. L. No. 44651, vol. 672, Government Gazette, viewed 15 January 2022, from https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf.

Holt, T.J. & Kennedy, J.P., 2020, 'The handbook of white-collar crime', in M. Rorie (ed.), *The handbook of white-collar crime*, pp. 451–468, John Wiley & Sons, Inc., New Jersey.

IBM & Ponemon Institute, 2024, *Cost of a data breach report 2024*, viewed 09 May 2025, from https://www.ibm.com/reports/data-breach.

Kayes, A.S.M., Hammoudeh, M., Badsha, S., Watters, P.A., Ng, A., Mohammed, F. et al., 2020, 'The proposed access control approach to countermeasure data breaches', in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, The Printing House, Doha, Qatar, 02–05 February, pp. 498–503.

Khoza, L., 2024, 'Africa confronts an avalanche of cyber-attacks', *ITWeb*, viewed 25 November 2024, from https://itweb.africa/content/lwrKx73Ygxrqmg1o.

Koziarski, J. & Lee, J.R., 2020, 'Connecting evidence-based policing and cybercrime', *Policing: An International Journal* 43(1), 198–211. https://doi.org/10.1108/PIJPSM-07-2019-0107

March, J.G., 1991, 'Exploration and exploitation in organizational learning', *Organization Science* 2(1), 71–87. https://doi.org/10.1287/orsc.2.1.71

Moyo, A., 2019, 'Bad day for SA's cyber security as banks suffer DDoS attacks', *ITWEB*, viewed 11 March 2025, from https://www.itweb.co.za/article/bad-day-for-sas-cyber-security-as-banks-suffer-ddos-attacks/LPp6V7r4OVzqDKQz.

Moyo, A., 2023, 'InfoReg slaps justice department with historic R5m fine', *ITWeb*, 04 July, viewed 18 September 2024, from https://www.itweb.co.za/article/inforeg-slaps-justice-department-with-historic-r5m-fine/o1Jr5MxPmm2MKdWL.

Ojedokun, U.A. & Oshilaja, S.I., 2022, 'Cybercrime policing in the Lagos state command of the Nigeria Police force', *SALUS Journal* 10(2), 34–50.

Paek, S.Y., Nalla, M.K. & Lee, J., 2020, 'Determinants of police officers' support for the public-private partnerships (PPPs) in policing cyberspace', *Policing: An International Journal* 43(5), 877–892. https://doi.org/10.1108/PIJPSM-06-2020-0088

Page, S.B., Bryson, J.M., Middleton Stone, M., Crosby, B.C. & Seo, D., 2021, 'Ambidexterity in cross-sector collaborations involving public organizations', *Public Performance & Management Review* 44(2), 1–30. https://doi.org/10.1080/15309576.2021.1937243

Pieterse, H., 2021, 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication* 28(28), 1–21. https://doi.org/10.23962/10539/32213

PWC, 2024, *Global digital trust insights survey 2025: South Africa and Africa report*, viewed 25 November 2024, from https://www.pwc.co.za/en/publications/digital-trust-insights.html.

PWC_Report, 2020, *PwC's global economic crime and fraud survey*, viewed 14 June 2021, from https://www.corruptionwatch.org.za/wp-content/uploads/2020/06/global-economic-crime-survey-20201.pdf.

SABRIC, 2023, *Annual crime statistics – SABRIC*, viewed 25 November 2024, from https://www.scribd.com/document/879377844/Sabric-Annual-Crime-Stats-2023-2.

Syed, T.A., Blome, C. & Papadopoulos, T., 2020, 'Resolving paradoxes in IT success through IT ambidexterity: The moderating role of uncertain environments', *Information and Management* 57(6), 103345. https://doi.org/10.1016/j.im.2020.103345

Vettorello, M., Eisenbart, B. & Ranscombe, C., 2020, 'Paradoxical tension: Balancing contextual ambidexterity', *Proceedings of the Design Society: DESIGN Conference* 1, 1385–1394. https://doi.org/10.1017/dsd.2020.74

Vieru, D., Klein, S., Bourdeau, S. & Ntakirutimana, J.B., 2021, 'Developing ambidextrous routines in the IT service provider industry', in T.X. Bui (ed.), *Annual Hawaii International Conference on System Sciences*, January, pp. 6452–6461, HICSS, Hawaii.

Westergren, U.H., Holmström, J. & Mathiassen, L., 2019, 'Partnering to create IT-based value: A contextual ambidexterity approach', *Information and Organization* 29(4), 1–18. https://doi.org/10.1016/j.infoandorg.2019.100273