Cybercrime Policing Collaboration in South Africa: Exploring A Stakeholder Approach

Motlalepule Zulu and Ryno Boshoff
Nelson Mandela University, Gqeberha, South Africa

tlale.zulu@gmail.com
Ryno.Boshoff@mandela.ac.za

Abstract: The sophistication of crimes committed using Information and Communication Technology (ICT) has become a policing challenge for law enforcement globally. The complexity with the policing of economic cybercrime is that law enforcement's primary orientation focuses on traditional crime, and processes on how to handle cybercrime are lacking. Conversely, policing cybercrime for organisations has a corporate governance aspect to it. This is because governance instruments such as the business continuity plan (BCP), disaster recovery plan (DRP) and response plans are necessary to ensure business continuity in case of any eventuality. For instance, after a cyber-incident, the organisation's priority is to restore operations and to protect critical ICT infrastructure. This has a negative bearing on policing because law enforcement might not get an opportunity to investigate timeously. The effective policing of economic cybercrime cannot be isolated to one entity. Cross sectoral partnerships between law enforcement and organisations in South Africa (SA) are required in addressing knowledge and capacity issues. However, collaboration between police and organisations is complex since both stakeholders have different interests. Organisations need to be profitable and satisfy their board members' interests. While law enforcement has a responsibility to satisfy the public interests by ensuring that there is order and that the law is being upheld. This research effort answers the question, "why is it important for law enforcement, ICT departments and ICT organisations to police cybercrime collectively?". Personal interviews conducted with cyber experts will provision insight as it pertains to the extent to which organisations are willing to commit in partnering with a stakeholder that does not explicitly contribute towards their value creation. Similarly, insight on how the enacted cyber related legislature has affected organisations in handling individuals' personal information will be gained. Furthermore, interviews with academics in the cybersecurity discipline will provision insight on the relevance of police and organisations' collaboration in addressing cybercrime in SA. Moreover, insight on how saturation of the collected data was attained will be provisioned.

Keywords: Cybercrime policing, Reporting, Collaboration, Stakeholder theory, Data saturation

1. Introduction

The cybercrime phenomenon is a complex issue for law enforcement and organisations globally. Economic Cybercrime (EC) which is a broad term described by Cook et al. (2023) as crimes whereby a computer, networks or a device connected to the network are used to expedite identity theft, distributed denial-of-service attack, online shopping fraud and phishing attacks, amongst others. The complexity with policing EC is that these attacks are wider in reach and scope (Nowacki & Willits, 2020). Similarly, the lack of proper tools and technical skills to handle cybercrime has resulted in the lack of confidence in law enforcement. Another complexity with the policing of EC is that the police's primary orientation focuses on traditional crime. Curtis and Oxburgh (2023) argues that the principle of policing does not change whether the crime is physical or virtual.

It is worth mentioning that the private sector plays the role of online policing and patrolling. This is because organisations are adequately equipped to (i) govern their environments, (ii) identify and (iii) detect anomalies, (iv) protect, (v) respond, and (vi) recover from threats and attacks (National Institute of Standards and Technology, 2024). Therefore, the concept of policing EC cannot be limited to law enforcement. Technology has extended policing to corporate entities particularly those in the ICT industry (Akdemİr, Sungur & Basaranel, 2020). Similarly, the effective policing of EC cannot be isolated to one entity. Cross sectoral partnerships are required in addressing knowledge and capacity issues in combatting cybercrime. Although cross sectoral partnerships between law enforcement (especially those in the cybercrime units) and organisations remain useful, they are complex, since stakeholders have different interests (Lee, 2022). Law enforcement and private sectors' priorities are not aligned, and adaptation is a challenge. For instance, police officials are not always given an opportunity by organisations to investigate cybercrime because the evidence might have been removed before law enforcement could intervene.

2. Related Work

A similar study to this paper investigates cybercrime policing involving public and private partnerships within a South Korean context. The study provisions insight into how attitudes and assumptions held by law enforcement and organisations hinders cybercrime policing collaboration (Paek, Nalla & Lee, 2020). The results of the study conducted by Paek et al. (2020) indicate that law enforcement felt that the segregation of duties needed to be

clarified. They argued that investigation was law enforcements' duty and not necessarily the private sectors' (Paek et al. 2020). Another similar work to this study, includes Pieterse's (2021) study through which a review of 74 cyber incidents which occurred over 10-year period (2010 – 2020) in SA was undertaken. The study addressed challenges which relate to non-reporting of cyber-related incidents and South African Police Service (SAPS) challenges. The study's findings made it apparent that organisations failed to invest in cybersecurity and that compliance was a problem. As such, the study recommended that organisations adopt risk minimisation practices such as enabling a cybersecurity centred culture and using threat intelligence. Similarly, Dlamini and Mbambo's (2019) work through which they endeavoured to understand the cybercrime policing phenomena within South African's context is essential to this study. Their study was limited to individuals from the community, staff members from one ICT organisation and SAPS officials from the Directorate of Priority Crime Investigation (DPCI) in the City of Durban. The DPCI is a division within SAPS, whereas Durban is a city in SA. Their study recommended the establishment of strategic partnerships between SAPS and the private sector in addressing cybercrime particularly in Durban. It is noteworthy that at the time, studies by Dlamini and Mbambo (2019) and Pieterse (2021) were conducted, the Protection of Personal Information Act (POPIA) and Cybercrime Act (CCA) were not fully enacted. POPIA and CCA are legislative instruments in SA, and both instruments were enacted in 2020. POPIA compels organisations in SA to report data breaches to SAPS and the information regulator. POPIA also compels organisations to inform those whose personal details might have been compromised during the breach. The CCA was developed to identify cybercrime related offences. The CCA makes the reporting of cybercrimes mandatory and addresses the role of SAPS.

3. Problem Definition

Since policing is generally law enforcement's duty, in SA, it is not clear where victims may report cybercrime incidents. As such, it is natural for victims to assume that, by reporting at a local police station, they might get the proper support from the police. However, local police do not perceive cybercrime as their duty and therefore, are unsure on how to deal with such cases (Curtis & Oxburgh, 2023). Similarly, the nature of policing in SA is that a criminal incident that is life threatening is likely to be prioritised over an economic crime. The challenge which SAPS has, is that their processes are geared towards handling traditional crime and not necessarily cybercrime (Dlamini & Mbambo, 2019). Therefore, it is no wonder that the SAPS strategic plan 2020 – 2025 does not make mention of cybercrime nor indicate how it will be addressed (South African Police Service, 2020).

Other factors that contribute to reluctance to report cyber-breaches are because organisations do not want to run the risk of incurring fines, losing competitive advantage to rivals and losing revenue (Tennis, 2020; Saban, Rau & Wood, 2021). Negative publicity is another factor that contributes to under-reporting of cyber-breaches and cyber-attacks experienced by organisations (Tennis, 2020). Pieterse (2021) argues that in SA, reporting cyber incidents is not normal practice. Dlamini and Mbambo (2019) contends that the high rates of cybercrime under-reporting particularly in SA, is a challenge and a limitation for policing because it does not give a complete presentation of the problem. POPIA addresses Dlamini and Mbambo's (2019) concern, because organisations are compelled to report cyber incidents through which personal information of individuals might have been compromised (Protection of Personal Information, Act 4 of 2013, 2013). It remains unclear the extent to which POPIA has influenced organisations attitudes as it pertains to disclosure of cyber-related incidents to SAPS.

Conversely, organisations' priorities differ from those of SAPS. For instance, after a cyber-incident, the organisation's priority will be to restore business operations and to protect critical ICT infrastructure. Policing EC for organisations has a corporate governance aspect to it, because governance instruments such as the BCP, DRP and response plans are necessary to ensure business continuity in case of any eventuality (Fani & Subriadi, 2019; Soni, 2020). Holt and Kennedy (2020) argue that most cyber experts work for organisations and have contractual agreements which prohibits them from sharing their findings as it pertains to large cyber-attacks. As a result, there are volumes of data within organisations, if shared, could be useful for strengthening the fight against cybercrime (Holt & Kennedy, 2020).

4. Stakeholder Theory

A stakeholder is described as any individual or group which contributes to value creation in an organisation (Phillips et al. 2019). There are different types of stakeholders those who directly contribute towards value creation in an organisation such as customers, suppliers, shareholders and employees (Phillips et al. 2019). Whereas the other types of stakeholders are those which influences the organisation indirectly such as competitors, regulators and the government (Phillips et al. 2019). In this study's context, law enforcement is a

secondary stakeholder meaning, those with an interest as it pertains to EC reporting and information sharing. However, the dilemma is that organisations don't see the need to report cyber-attacks and breaches because the perception is that the police are not going to investigate (Curtis & Oxburgh, 2023). Organisations are also reluctant to report because they do not want to be "*named and shamed*" (Tennis, 2020). Similarly, the lack of trust and confidence between both stakeholders is among the key challenges in policing cybercrime collaboratively (Page et al. 2021).

Cross sectoral partnerships are necessary for the policing of EC. There is no study which explores the stakeholder theory to foster partnerships between the police and ICT organisations from a SA context. The study hopes to better understand the extent to which ICT organisations are willing to commit in partnering with a stakeholder that does not explicitly contribute towards their value creation. Moreover, there is limited knowledge on stakeholder perceptions as it pertains to collaborations towards cybercrime policing (Paek et al. 2020).

5. Methodology

This study employed the qualitative method because it enables us to understand the deep narratives held by the two stakeholders concerning their roles in policing cybercrime in SA. Moreover, to gain a broader perspective on how collaboration might be attained, the study uses two datasets (i) a YouTube video and (ii) personal interviews. Thus, for the collection of the first dataset, YouTube videos of interviews with experts, whereby cybercrime was discussed were sought and listened to. The search criteria used was "cybercrime in South Africa". The Storm Guidance virtual panel discussion video archived on YouTube titled "Cybercrime and its impact on businesses in South Africa" was ideal for answering this study's research question. All questions used were from the YouTube video. Table 1 illustrates profile details of the panellists.

Table 1: Panellists Details

Title	Expert	Role
Mr	IT Online Newspaper Editor	Facilitator
Prof	Information Regulator's Office Representative	Panellist
Mr	SAPS Brigadier	Panellist
Mr	Cybersecurity Expert	Panellist

Purposive sampling was used to select the suitable sample for the study. The sample includes 4 individuals from ICT organisations and 3 academics from SA universities with expertise in cybercrime and/or cybersecurity discipline. For confidentiality reasons, data for interviews conducted with the 3 members of SAPS is omitted from this study. Personal interviews consisted of semi-structured questions; the interviews were conducted face to face via Microsoft Teams. Table 2 illustrates details of participants who agreed to participate voluntarily in the study.

Table 2: Personal Interview Participants' Profiles

Title	Job Title	Years of Experience in Position	Years of Experience in Cybercrime/ Cybersecurity Discipline
Mr	Cybersecurity Solutions Architect	11	6
Mr	CEO, Owner	10	5
Mr	CEO, Owner	40	20
Mr	Cybersecurity Business Development Manager	5	7
Dr	Senior Lecturer	10	10
Mr	Senior Lecturer	9	5
Prof	Professor	11	23

This sample size was decided upon based on (i) its diversity, (ii) ethics requirements and (iii) the data saturation concept which posit that saturation is a point at which no new or extra data is forth coming (Guest, Namey &

Chen, 2020). The authors suggest that data saturation is attainable at a minimum of 4 to 6 participants (Guest et al. 2020). However, a higher degree of data saturation is attainable at a maximum of 12 participants (Guest et al. 2020). This study adopts Braun and Clarke's (2021) reflexive thematic analysis approach which they posit that saturation cannot be predetermined. The authors argue that saturation should be an analysis driven process and not a data collection driven process (Braun & Clarke, 2021). Data saturation was attainable after analysing the personal interviews' dataset. Whereas a higher degree of saturation was attainable across the data corpus. The two datasets were captured on separate worksheets in Microsoft Excel and imported to NVivo 14 for analysis. Analysis of each dataset was done separately as illustrated on Figure 1.

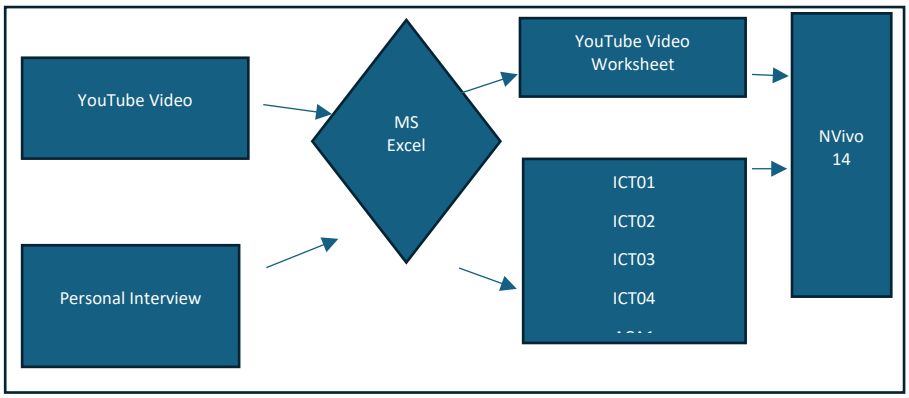

Figure 1: Datasets Analysis

6. Results

This section presents results of the data collected for the personal interviews and YouTube video. Participants from ICT organisation will be referred to as ICTO1, ICTO2, ICTO3 and ICTO4. Similarly, participants from academic institutions will be referred to as ACA1, ACA2 and ACA3. Moreover, participants from the YouTube video will be referred to as SAPS Representative, IRO Representative and Org Representative. Within this section, insight on (i) the importance of reporting, (ii) POPIA and (iii) collaboration will be gained. Participants were asked this question "*Why is it important for organisations to report cyber-attack to SAPS?".* The following responses were provisioned in relation to this question:

> *ICTO1: For prosecution purposes, evidence gathering and hardening the prosecutor's case against the threat actor.*
>
> *ICTO2: So that there is a register of what type of attacks are in the market.*
>
> *ICTO3: For statistical purposes. Current statistics are not true. Statistics makes people aware.*
>
> *ICTO4: It's very important.*
>
> *ACA1: For us to be able to predict or protect, we need to work on some history pertaining some event. We need to see some trends on what has been happening. Non-reporting will make cybercrime seem like a minor problem in their sector, and this will affect their budgeting. Reporting will also help other organisations to be able to safeguard because they will be able to see what is happening to other organisations within the same field/locality.*
>
> *ACA2: It would be in the organisation's best interest to report cybercrime as soon as possible because you build up this body of evidence.*
>
> *ACA3: If we in SA have a database of attacks that are happening that is up to date, the minute cybercrime occurs, and it is serious, at least everyone will know about it.*

The response from the interviews indicates that reporting is essential to give police an opportunity to gather evidence for prosecution purposes. Similarly, reporting is essential for transparency and is useful in enabling us to realise the depth of the problem. Statistics and trends would enable SA organisations and law enforcement to know the prevalent threats and attacks. Moreover, there is an inference that reporting will be useful in highlighting skills' gap and thus inform budget planning in SAPS.

Table 3: The Issue of Non-Reporting

Source	Expert	Disclosure
Storm Guidance (2021)	SAPS Representative	It is important to have a response protocol and the intervention strategy. Businesses who are victims of business email compromise should report those matters as soon as possible to the authorities. Ensure that the evidence material is secure. By the time a matter is reported to law enforcement you try to find the evidential material on the instrument. You would find that the technician responsible for the company cyber security has removed the evidence. Don't destroy evidence.
	IRO Representative	If you are affected report your incidents and if there are criminal acts to it go and report it to SAPS. There is a cybercrime unit, and they deal with these complaints effectively, they even have prosecution of these complaints. Although there are no numbers published it is not indicative that criminals are not prosecuted for cybercrime in SA.
	Org Representative	Preservation of evidence is key. With a lot of these incidents suffered by businesses they have a real problem because they need to prioritise recovery and sometimes the recovery is prioritised over the maintenance of evidence. Mostly that is because the people they are using to do that work are IT staff who do not appreciate the need to preserve evidence. Businesses needs to know what they can appreciate from law enforcement, law enforcement just like any crime has a limited responsibility. They are there to investigate the crime but are not there to help the organisation to recover.

Table 3 illustrates views expressed by experts in relation to why organisations chose not to report. Interestingly the IRO representative mentioned the existence of the cybercrime unit and its success in prosecution cases. It is unclear why there is secrecy and the lack of transparency in how cybercrime is being dealt with in SA. Furthermore, Table 3 makes it apparent that, in an effort to recover from an incident, organisations remove evidence, thus making it impossible for law enforcement to investigate effectively. Therefore, organisations need to strike a balance between continuity while allowing SAPS to do their job.

This section addresses assumptions held by academics in relation to POPIA effect on organisational disclosure. Similarly, insight on how the ICT experts suppose POPIA has influenced the manner in which personal data was handled will be provisioned. Academics were asked *"How do you suppose POPIA has affected the reporting of cyber related incidents and data breaches to SAPS by organisations?".* Responses provisioned in relation to this question follows.

> *ACA1: Their reporting does not cover all their breaches because some of them might get on the wrong when it comes to POPIA. It can be thought that there's been a reduction in breaches but there could be a reduction in reporting. Although POPIA has influenced how organisations deal with personal data, it has not led to increased reporting. Organisations would rather not report.*
>
> *ACA2: In POPIA, there is a provision for information to be shared in case of investigation. POPIA makes it clear that for purposes of criminal investigation, companies need to assist in whatever way they can.*
>
> *ACA3: POPIA has been a positive law that we have instituted because it has made companies to think about what they do with people's data, and this is very important. People are more protected based on what we see with POPIA. Organisations withhold information as far as they can - it's all about reputation. When the company suffers a breach or have any problems, they try not to report them and keep it as quiet as possible. But if you do not have laws in place to force people to report wrongdoing, it's unlikely that they would do it from their freewill.*

The responses provisioned by academics suggest that organisations were not totally transparent about the breaches. The lack of transparency was guided by the fear of bad publicity and that the IRO might discover that organisations were non-compliant. Moreover, there was inference that POPIA has been useful because it had affected the way organisations deal with personal data.

Table 4: POPIA Receptiveness

Source	Expert	Organisation's Response to POPIA
Storm Guidance (2021)	IRO Representative	The private sector has been receptive to POPIA, they engage the regulator pertaining to their breaches and have been guided by the regulator's office. It needs to be understood that self-reporting is the law.

The information illustrated on Table 4 indicates that the private sector has adopted a pro-active approach, and there was willingness to know how they could fulfil POPIA requirements. However, it was unclear whether the public sector followed the same approach.

An understanding on whether POPIA had influenced organisational processes in relation to the handling of personal data was sought. Similarly, insight on how ICT experts perceived POPIA was sought. We wanted to understand whether organisations perceived POPIA as a useful and binding instrument. As such cyber experts were asked *"How has POPIA affected the way your organisation handles personal details?"*. The following answers were provisioned by the participants:

> *ICTO1: POPIA has enforced additional policies as well as much stricter segmentation of information systems processing of personal information. It has also enforced legal framework documentation and limitation on periods of data storage to comply with organisation's policies (system and management policies).*
>
> *ICTO2: Very much from a processing point of view, personal details are not kept in the environment. Processes were changed, the data were kept secure, processes of how to handle the data are well outlined. POPIA has affected their environment.*
>
> *ICTO3: Its ineffective because thus far no one has been arrested for non-compliance. However, it can be useful, but it depends on the context.*
>
> *ICTO4: It's a lot more thorough. It has influenced how information is shared across Enterprise Resource Planning and Customer Relationship Management systems.*

Responses from ICT organisations made it apparent that POPIA has contributed to internal policy enactment and has influenced how personal data was processed. However, one participant questioned POPIA's effectiveness indicating that it has not led to any arrests. In 2023, the department of Justice and Constitutional Development incurred a R5 000 000 fine from the IRO for non-compliance due to an attack in 2021 (Moyo, 2023). What remains unclear is whether SA would witness more penalties being imposed on those who fail to comply.

Policing cybercrime in silo is considered ineffective therefore, it was important to understand perceptions and attitudes that participants had pertaining to collaboration. Similarly, it was useful to understand barriers and hindrances to cybercrime policing in SA. Participants were asked "What *is the importance of collaboration between SAPS and organisations in addressing cybercrime in SA?".* Participants responses below give us insight on how they believe collaboration could be attained.

> *ICTO1: It is important. It can work, because any information shared is better than none. SAPS is not ready to address cybercrime. At present it is more of a one way or one-sided endeavour from ICT organisations or other corporates but nothing from SAPS side.*
>
> *ICTO2: Collaboration between SAPS and organisations is very important, that is the only way we can win against cybercrime.*
>
> *ICTO3: Cybercrime is going to collapse our economy if they don't work together to curb, investigate, solve crime and prevent crime.*
>
> *ICTO4: There needs to be a division in SAPS that deal with cybercrime. SAPS is ill equipped, skills-wise and tools-wise to prevent cybercrime. Even to carry out an investigation, tools are needed to trace an Internet Protocol (IP) or a Media Access Control (MAC) address. It would be great if the government invested in a cybercrime division and special technologies were used.*
>
> *ACA1: SAPS might not know of breaches, infringements or cybercrime that might be happening until it is reported. There is a need for a collaboration because organisations are the first eyes of the cybercrime before SAPS can be aware of it.*

ACA2: SAPS can only learn from information gathering, questioning certain things from that information or the evidence and they can only get that information from companies or persons where cybercrime was committed.

ACA3: We need to work together - SAPS and organisations to find the source of the problem. If there is no collaboration in that context, the police will not be able to deal with it and organisations would be left to deal with it alone, and they do not always do the right thing - they just want to get out of it. Collaboration is required because of the nature of the crime.

Table 5: Meaningful Collaboration

Source	Expert	Stakeholder Relationship
Storm Guidance (2021)	SAPS Representative	SAPS and law enforcement on its own will not be able to succeed to address cybercrime. Stakeholder partnership for law enforcement is extremely important and this is where business fraternity can come in and assist SAPS.

Some participants were of the view that collaboration was important in the policing of cybercrime in SA. Participants' responses made it apparent that each stakeholder's role pertaining to their contribution to the collaboration ought to be clear. Organisations must disclose cybercrime to SAPS. However, it must be clear what happens after an organisation has reported an incident to SAPS. Since organisations are better equipped to deal with cybercrime, it would be useful if they could share their skills and resources with SAPS. This will be useful in ensuring that both stakeholders are on par, and therefore, instil confidence on SAPS's ability to deal with cybercrime. This inference was underpinned by the view expressed in Table 5, that successful collaboration requires co-operation from both stakeholders.

7. Recommendations

This paper made it apparent that although organisations were compelled by law to report cybercrime. There was no clarity as to where organisations could report cybercrime because there was a perception that SAPS were ill-equipped to address EC. Moreover, this paper indicated that organisations' response after the attack were to restore operations. As such, evidence would be removed which then prohibited police from investigating. Thus, it is recommended that organisations find a balance between continuity while enabling SAPS to do their job. This study recommends that both stakeholders work collaboratively in addressing this phenomenon. Thus, it is important that both stakeholders understand that successful collaboration requires cooperation from both sides.

For future work, we recommend a study which examines policing methodologies that SAPS could adopt to strengthen its response time to cyber-related incidents. Similarly, a study which investigates how SAPS could implement a central cybercrime repository for organisation without infringing on POPIA would be useful. We further recommend a study which investigates mechanisms which could be useful for collaboration between internet service providers in SA and SAPS in combatting cybercrime.

8. Conclusion

This paper explored whether ICT organisations were willing to commit in partnering with a stakeholder that does not explicitly contribute towards their value creation. This paper clarified the complexity of EC policing from organisations and SAPS perspectives. Although organisations have a responsibility to report cybercrimes, this paper makes it apparent that they require assurance from SAPS that an investigation would follow. Similarly, both stakeholders have legislative obligations when it comes to EC. Organisations are compelled by POPIA to inform the authorities and affected individuals after an incident. Whereas SAPS are mandated by the CCA to investigate cybercrime cases.

Similarly, interviews provisioned insight pertaining to the importance of reporting, POPIA and collaboration. Furthermore, the process followed to attain data saturation was discussed. The data analysis results indicated that EC reporting was essential for transparency, statistics and for trend analysis. Moreover, the results of the interviews suggested that POPIA had influenced how organisations handled personal data. Thus, it can be deduced that the successful policing of EC lies in stakeholder engagements through skills development and information sharing.

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

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. In *Qualitative Research in Sport, Exercise and Health* (Vol. 13, Issue 2, pp. 201–216). Routledge. https://doi.org/10.1080/2159676X.2019.1704846

Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., & Williams, M. L. (2023). Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory. *The British Journal of Criminology*, *63*(2), 384–406. https://doi.org/10.1093/bjc/azac021

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

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1–13. https://doi.org/10.1080/23311886.2019.1675404

Fani, S. V., & Subriadi, A. P. (2019). Business continuity plan: Examining of multi-usable framework. *Procedia Computer Science*, *161*, 275–282. https://doi.org/10.1016/j.procs.2019.11.124

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLoS ONE*, *15*(5), 1–17. https://doi.org/10.1371/journal.pone.0232076

Holt, T. J., & Kennedy, J. P. (2020). The Handbook of White-Collar Crime. In M. Rorie (Ed.), *The Handbook of White-Collar Crime* (First, pp. 451–468). John Wiley & Sons, Inc.

Lee, J. R. (2022). Cyberpolicing. *Oxford Research Encyclopedia of Criminology and Criminal Justice*, *October 2022*, 1–29. https://doi.org/https://doi.org/10.1093/acrefore/9780190264079.013.729

Moyo, A. (2023). InfoReg slaps justice department with historic R5m fine. *ITWeb*. https://www.itweb.co.za/article/inforeg-slaps-justice-department-with-historic-r5m-fine/o1Jr5MxPmm2MKdWL

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Nowacki, J., & Willits, D. (2020). An organizational approach to understanding police response to cybercrime. *Policing: An International Journal*, *43*(1), 63–76. https://doi.org/10.1108/PIJPSM-07-2019-0117

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*, 1–29. https://doi.org/https://doi.org/10.1080/15309576.2021.1937243

Phillips, R. A., Barney, J. B., Freeman, R. E., & Harrison, J. S. (2019). Stakeholder Theory. *Contributions to Management Science*, 1–8. https://doi.org/10.1007/978-3-030-70428-5_1

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

Protection of Personal Information, Act 4 of 2013, Pub. L. No. 37067, Government Gazette 1 (2013).

Saban, K. A., Rau, S., & Wood, C. A. (2021). "SME executives' perceptions and the information security preparedness model". *Information and Computer Security*. https://doi.org/10.1108/ICS-01-2020-0014

Soni, V. D. (2020). Disaster Recovery Planning: Untapped Success Factor in an Organization. *SSRN Electronic Journal*, *June*, 1–11. https://doi.org/10.2139/ssrn.3628630

South African Police Service. (2020). Strategic Plan 2020 - 2025. In *SAPS Corporate Communication* (Issue 1, pp. 1–34). http://www.afpe.org.uk/physical-education/wp-content/uploads/afPE-Strategic-Plan-2016-2020.pdf

Tennis, Mickellea. M. (2020). A United Nations Convention on Cybercrime. *Capital University Law Review*, *48*(2), 189–236.