International Review of Social Sciences Research
Volume 6 Issue 2 June 2026
DOI: https://doi.org/10.53378/irssr.353369

Data integrity in digital policing: Evaluating the quality of cybercrime statistics

[1]Ogochukwu Favour Nzeakor & [2]Godfrey Thenga

Abstract

Cybercrime has become one of the most harmful forms of crime in the world. By 2025, losses from cybercrime were projected to exceed $10.5 trillion annually, making it one of the largest economies in the world. Despite this alarming global menace, the South African Police Service (SAPS) continues to rely on outdated classification systems and fragmented approaches to digital evidence management, thereby obscuring the true extent of cyber-enabled crimes. This study assesses the integrity of SAPS cybercrime statistics from 2013 to 2022 using an interpretivist qualitative research design, with a particular focus on auditing key issues, including misclassification, institutional discretion, and sociotechnical system failures. The findings revealed three major issues. First, SAPS cybercrime data are largely incomplete due to widespread underreporting and the absence of a centralized reporting system. Second, common cybercrimes, such as phishing, ransomware, identity theft, and business email compromise (BEC), are systematically misclassified under broad categories such as fraud or commercial crime. Third, outdated digital infrastructure, inconsistent practices across police stations, limited technical capacity, and the slow implementation of the Cybercrimes Act significantly undermine data quality. The study recommends adopting the International Classification of Crime for Statistical Purposes (ICCS) standards, among other reforms. Although the use of secondary data limits insights into internal SAPS practices, the findings underscore the urgent need for coordinated sociotechnical reforms to enhance the effectiveness of digital-age policing in South Africa.

Keywords: *data integrity, crime statistics, digital-driven policing, underreporting, sociotechnical data governance*

Article History:

***Received**: March 17, 2026* ***Revised**: April 24, 2026*
***Accepted**: June 8, 2026* ***Published online**: June 10, 2026*

Suggested Citation:
Nzeakor, O.F. & Thenga, G. (2026). Data integrity in digital policing: Evaluating the quality of cybercrime statistics. *International Review of Social Sciences Research*, 6(2), 324-351. https://doi.org/10.53378/irssr.353369

About the authors:
[1]Corresponding Author. PhD in Criminology. Postdoctoral Research Fellow, Department of Police Practice, College of Law, Florida, Gauteng, University of South Africa. Email: enzeakof@unisa.ac.za
[2]PhD in Criminal Justice. Associate Prof., Department of Police Practice, College of Law, Florida, Gauteng, University of South Africa. Email: tshabg@unisa.ac.za

1. Introduction

The Fourth Industrial Revolution is data driven. In this sense, artificial intelligence, edge computing, and the Internet of Things depend on data being collected, classified, governed, and used effectively. In policing, data enables intelligence-led policing, evidence-based policing, crime mapping, hotspot strategies, and other data-driven interventions (Huey & Buil-Gil, 2024; Lee et al., 2024). As such, the quality of crime data is not merely a technical concern; it directly shapes what police agencies perceive as threats, how they prioritize resources, and whether policy decisions can be justified by evidence.

Globally, countries such as the United States, the United Kingdom, and Australia have increasingly adopted predictive analytics and more standardised crime reporting systems to improve transparency, accountability, and operational efficiency (UNODC, 2024; Lukens, 2025). However, South Africa continues to face persistent challenges in crime data quality, including underreporting, inconsistent classification, and limited disaggregation, particularly in cybercrime statistics (Mulaudzi & Molokomme, 2025; Ngcece & Mkhize, 2023). In South African Police Service (SAPS) publications, cybercrime is often grouped under broad categories such as “Other Serious Crimes” or “Crimes Detected as a Result of Police Action.” This aggregation obscures the scale and severity of online victimisation and limits analysts’ ability to identify specific patterns such as phishing, ransomware, identity theft, and hacking (Dupont, 2017; Emerson, 2025; Madondo et al., 2025; Newman, 2024). Poor data integrity is therefore a security and economic risk. Cybercrime is projected to cause global damages of approximately $10.5 trillion by 2025 (Emerson, 2025; Aphane, 2025). When cyber-enabled crimes are “swept under” broader labels such as fraud, policing agencies lose analytical clarity about emerging cyber threats and their operational signatures.

Underreporting further weakens cybercrime measurement. Victims may fail to report due to limited awareness, technical complexity, and reluctance stemming from reputational concerns (Maboa & Horne, 2024; Ngcece & Mkhize, 2023). In addition, SAPS faces technological and administrative challenges in its crime reporting systems, including delays in case registration and concerns about the reliability of digital infrastructure (de Kock, 2023). At the institutional level, critiques have also pointed to systemic weaknesses affecting the integrity and performance of SAPS crime data production. Reports by the FW de Klerk Foundation (Joosub, 2025) and the Institute for Security Studies (2024) cite political interference,

leadership instability, and limited transparency regarding crime statistics as factors that undermine effective crime control (Parliament of the Republic of South Africa, 2025).

Despite efforts to modernise crime statistics, including partnerships with Statistics South Africa, these reforms have not fully resolved systemic issues affecting cybercrime data integrity and categorisation (South African Police Service, 2023; South African Police Service, 2024). Cybercrime misclassification and insufficient disaggregation limit policy learning and evidence-based digital policing reforms. Furthermore, there is limited empirical research that links the quality of SAPS cybercrime data to its operational effectiveness. This study addresses these gaps by evaluating the integrity of SAPS cybercrime statistics for 2013–2022, identifying underrepresented cybercrime categories, and proposing a diagnostic sociotechnical framework to improve cybercrime data governance and reporting standards. Hence, the study would help to fill some of the most critical gaps in understanding and management of cybercrime data in the South African Police Service by responding to the following research questions:

1. To what extent is SAPS' cybercrime data on 2013-2022 complete, consistent and well-categorized?
2. Which forms of cybercrime are common in South Africa but are not adequately reported or captured in SAPS data?
3. Which institutional and technological issues lead to inconsistencies and underreporting of cybercrime data in SAPS?
4. Which structure can be created to enhance the integrity, classification, and disclosure of cybercrime information in SAPS?

2. Literature Review

2.1. Data-Driven Policing and the Dependence on Data Quality

The Fourth Industrial Revolution positions data as a foundational resource for modern technological systems and decision-making across sectors. For instance, in policing, data-driven strategies like intelligence-led policing (ILP), evidence-based policing (EBP), crime mapping, and hotspot policing depend on the availability of crime-related information that is accurate, complete, timely, consistent, and interpretable (Huey & Buil-Gil, 2024; Lee et al., 2024). These strategies operate on a core premise that police-recorded data provide a sufficiently reliable representation of criminal activity to support analysis, prioritisation, and learning.

Internationally, jurisdictions such as the United States, the United Kingdom, and Australia have expanded the use of predictive analytics and standardised crime reporting systems to improve operational transparency, accountability, and efficiency (UNODC, 2024; Lukens, 2025). While such reforms are often portrayed as enabling more effective policing, scholarship cautions that performance depends on governance conditions and data quality management, particularly when datasets are used for strategic targeting and evaluation (Lee et al., 2024; Huey & Buil-Gil, 2024). Accordingly, data-driven policing is not only a technological initiative but also an organisational and governance challenge.

Juxtaposing this reality with the South African context, the literature reveals persistent issues in crime data quality, including underreporting, inconsistent classification, and limited disaggregation. These challenges are particularly evident in cybercrime statistics (Mulaudzi & Molokomme, 2025; Ngcece & Mkhize, 2023). In this regard, cybercrime is frequently aggregated under broad reporting categories such as "Other Serious Crimes" or "Crimes Detected as a Result of Police Action." This reduces analytic sensitivity to specific cyber-offence typologies, such as phishing, ransomware, business email compromise, and identity theft, and limits the ability to detect patterns, allocate resources, and justify policy decisions based on evidence.

The literature further notes that underreporting is driven by factors related to victims' awareness, perceived complexity, and reluctance to report incidents due to reputational concerns (Maboa & Horne, 2024; Ngcece & Mkhize, 2023). At the same time, supply-side recording processes are affected by technological and administrative constraints, including delays in case registration and concerns regarding the reliability of digital infrastructure (de Kock, 2023). These issues contribute to measurement gaps, which, in turn, adversely affect ILP and EBP operations. Thus, the literature supports the need to evaluate police data not merely as records but as products of classification regimes, governance structures, and organisational practices.

2.2. Cybercrime Measurement Challenges in Policing

Cybercrime measurement barriers are widely discussed in the literature as arising from interacting demand-side and supply-side mechanisms. On the demand side, underreporting is frequently explained by limited awareness of reporting mechanisms, technical difficulties in documenting incidents, and victim reluctance to involve the police because of reputational and

economic concerns (Maboa & Horne, 2024; Ngcece & Mkhize, 2023). As a result, crime statistics may underestimate the scale of cyber victimisation and distort the apparent distribution of threats. On the supply side, inconsistencies in recording and categorisation are influenced by training, workload, and discretionary coding practices. Street-level bureaucracy theory explains that variability in classification and incomplete records may reflect structural responses to uncertainty and performance pressures rather than individual failure (Lipsky, 2010). Cybercrime reporting can be especially ambiguous because cyber offences may not align neatly with legacy categories designed for physical crime patterns, thereby increasing the likelihood of misclassification.

A further supply-side challenge concerns classification mismatch. Many recording systems historically evolved around physical, location-bound crime categories. Cyber offences, which are often digital, cross-jurisdictional, and technically mediated, may therefore not be adequately represented without behaviour-based typologies. Global measurement discussions argue that when classification frameworks do not align with cyber behavioural patterns, cyber offences remain hidden within broader fraud or general crime categories, limiting disaggregated analysis and cross-national comparability (UNODC, 2024; National Academies of Sciences, Engineering, and Medicine, 2025).

In the South African context, the literature suggests that cybercrime reporting may remain fragmented due to uneven station practices and weak integration across data systems (Ngcece & Mkhize, 2023; South African Police Service, 2024). The result is incomplete datasets and inconsistent category usage across reporting points. Additionally, institutional and legislative developments are relevant. Although cybercrime governance is supported by the Cybercrimes Act (2020) within the broader legal environment, its implementation has been argued to be slow and fragmented (Joosub, 2025; Snail ka Mtuze & Musoni, 2023). Such governance weaknesses may therefore affect reporting standardisation and the continuity of data integrity improvements.

2.3. Theoretical Framework: Data Integrity as Sociotechnical Governance Problem

This study uses the Sociotechnical Data Governance Model for Digital Policing (SDG-DP) to conceptualise cybercrime data integrity as co-produced through the alignment and interaction of (i) classification standards, (ii) data governance and quality management mechanisms, and (iii) organisational practice and policing paradigms (Ratcliffe, 2016;

Sherman, 1998; Zindi & Majam, 2025). The SDG-DP framework is sufficient to guide this research because it clarifies how data quality failures emerge. For instance, classification alignment determines which cyber offences are recorded and how they are represented. Similarly, governance and quality controls sustain integrity across the data lifecycle, including metadata management and quality monitoring (Wang & Strong, 1996; Wand & Wang, 1996). Furthermore, organisational practice shapes how frontline discretion and workload affect capture completeness and categorisation consistency (Lipsky, 2010; Sawyer & Jarrahi, 2013). SDG-DP further links data integrity to ILP and EBP. ILP depends on credible, granular data for threat pattern recognition and targeting, while EBP requires comparable data over time to evaluate intervention effectiveness (Ratcliffe, 2016; Sherman, 1998). Therefore, cybercrime data integrity failures can directly reduce operational and evidential value.

2.3.1. SAPS documentation as the empirical site for measuring integrity

Given that this study evaluates integrity through document-based analysis, the literature establishes why SAPS documents are a legitimate basis for assessing integrity outcomes. Crime statistics publications, annual reports, strategic plans, and policy documents are not mere reflections of reality; they function as social and institutional artefacts. Documentary records reveal how classification rules are operationalised, how data quality issues are acknowledged, and how governance reforms are implemented in practice (Bowen, 2009; Scott, 2014). In this sense, the document analysis literature supports treating institutional records as evidence of organisational sense-making and administrative practices (Bowen, 2009; Scott, 2014).

In this study, SAPS annual crime reporting documents provide material that can be analysed to determine how cybercrime is defined and grouped, whether disaggregation exists, whether cybercrime subtypes are explicitly recorded, whether data integrity concerns are transparently reported, and whether reforms (e.g., standardisation and governance initiatives) are documented. This approach aligns with Records Continuum theory, which posits that integrity is reflected in documentation choices and metadata-related practices embedded in record creation and reporting workflows (Upward, 1996).

2.3.2. Measurement indicators for data integrity in cybercrime statistics

To operationalise data integrity within the SDG-DP lens, the literature supports the use of recognised dimensions of data quality and governance indicators. Data quality research frames integrity using dimensions such as accuracy, completeness, consistency, timeliness, and

representational clarity (Wang & Strong, 1996; Wand & Wang, 1996). In cybercrime measurement, additional attention is required for classification representation and disaggregation. Accordingly, indicators suitable for document-based evaluation include:

Completeness indicators: These concern the extent to which cybercrime incidents are captured and reflected in SAPS statistics, including the presence or absence of central reporting mechanisms and explicit mention of undercounting patterns.

Consistency indicators: These relate to the stability of cybercrime categories over time and across references in different SAPS publications, including acknowledgement of classification drift or uneven station-level practices where documented.

Categorisation indicators: These concern the degree to which cybercrime typologies (e.g., phishing, ransomware, BEC, and identity theft) appear as explicit subcategories rather than being absorbed under broader fraud or generic categories.

Governance and quality indicators: These relate to evidence of governance controls, such as quality monitoring procedures, stewardship structures, metadata and lineage practices for records, and references to standard frameworks such as International Classification of Crime for Statistical Purposes (ICCS) (UNODC, 2024).

Interpretability indicators: These concern whether SAPS reporting supports meaningful ILP and EBP use. For example, they assess whether data are sufficiently granular to guide intelligence products and evaluation.

These indicators allow the study to diagnose integrity weaknesses while remaining consistent with interpretivist assumptions and document-based evidence standards.

2.4. Consequences of Poor Cybercrime Data Integrity for ILP and EBP

The literature on data-driven policing demonstrates that the operational value of ILP and EBP depends on the quality of the inputs. If cybercrime is misclassified or underrepresented, ILP targeting may prioritise visible categories while neglecting cyber threats recorded under generic fraud groupings. This can limit the ability of analysts to recognise evolving threat signatures and develop credible intelligence outputs (Huey & Buil-Gil, 2024). For EBP, data integrity problems undermine evaluation design and interpretation. When categories change over time or when cybercrimes are aggregated differently across reporting periods, trend comparisons become difficult or misleading. This reduces the credibility of intervention assessment and constrains learning cycles in policing governance.

The literature further indicates that risk models and analytic tools may inherit biases embedded in upstream data. Thus, poor data integrity can produce feedback loops. In this regard, the enforcement attention may concentrate on categories that are more consistently recorded while underrepresented cyber threats remain invisible, affecting resourcing patterns and operational effectiveness (Lee et al., 2024). This risk is heightened when cybercrime measurement fails to provide disaggregated evidence. Therefore, the literature supports the conclusion that evaluating cybercrime data integrity is relevant not only for descriptive statistics but also for strategic policing decision-making.

2.5. Global Standards and Institutional Governance for Cybercrime Reporting

Global governance initiatives emphasise the importance of standardised classification, capacity building, and coordinated crime data systems. In this regard, UNODC promotes internationally consistent approaches to crime measurement and supports capacity building for statistical and analytical facilities (UNODC, 2024). Such initiatives are critical for improving comparability and reducing ambiguity in cybercrime categories. Comparative literature also highlights that jurisdictions with established audit cultures and methodological transparency tend to have stronger credibility in crime statistics. For example, methodological transparency and regulatory oversight are discussed in the UK context through statistical oversight structures (UK Statistics Authority, 2021). These governance conditions enhance trust in crime statistics and support the ethical legitimacy of data-driven policing.

While the specific empirical conditions vary, the shared lesson is that data-driven policing depends on the institutional capability to implement classification standards, governance controls, and organisational practice alignment (UNODC, 2024; Lee et al., 2024; Lukens, 2025). For South Africa, governance and institutional weaknesses including limited transparency, leadership instability, and the performance credibility of crime data systems are argued to undermine effective crime control (Joosub, 2025; Institute for Security Studies, 2024; Parliament of the Republic of South Africa, 2025). These critiques strengthen the relevance of sociotechnical governance evaluation for SAPS cybercrime statistics.

2.6. Research gap

Despite increasing attention to digital policing and cybercrime, the literature remains limited in how it connects the quality of SAPS cybercrime statistics to sociotechnical

mechanisms of data integrity. Existing research often concentrates on cybercrime trends, technological adoption, or general policing capacity without diagnosing how classification standards, data governance structures, and organisational recording practices jointly produce incomplete or inconsistent cybercrime records (Modise, 2025; Mpuru & Kgoale, 2026). Furthermore, the interpretivist document-based evaluation of cybercrime statistical integrity in SAPS, through a governance-centred framework such as SDG-DP, has not been sufficiently established. This creates a gap in empirical and conceptual diagnosis of how misclassification and underreporting are produced, and how these issues can be addressed through targeted reforms.

To address this gap, the present study evaluates the integrity of SAPS cybercrime statistics for 2013–2022, identifies underrepresented or misclassified cybercrime categories, diagnoses institutional and technological factors influencing data integrity using SDG-DP, and proposes a diagnostic framework to strengthen cybercrime classification, reporting governance, and evidence-based digital policing.

3. Methodology

3.1. Research Design

The research design used in this study was an interpretivist qualitative research design, which is ideal for investigating the implications of meanings, classifications, and institutional interpretations in the production of cybercrime statistics within the SAPS. The interpretivist paradigm presupposes that reality is socially constructed and can be most adequately understood through textual analysis, institutional practices, and contextual meanings rather than numerical measurement. Qualitative research avoids quantification and causal generalisation, instead concentrating on the nature, characteristics, and manifestations of events within their contexts (Creswell & Poth, 2016; Denzin & Lincoln, 2011; Tisdell, Merriam, & Stuckey-Peyrot, 2025).

The implementation of this interpretivist lens allowed for immersion in the world of SAPS crime statistics, policy documents, legislative frameworks, institutional reports, and scholarly literature. It provided an effective means of revealing the ways in which cybercrime is framed, classified, and reported within the police service, as well as the influence of institutional values and technical limitations on the construction of crime data. Additionally, interpretivism supports a critical analysis of how data practices influence policymaking,

operational priorities, and societal awareness of cybercrime trends in South Africa (Zikalala, 2025).

To complement this paradigm, the research adopted a desktop (document-based) research strategy that relied exclusively on secondary data. This method is particularly applicable to the analysis of cybercrime because many contemporary digital threats remain inadequately represented in traditional South African crime statistics, where behaviourally distinct cyber offences are often grouped under broad historical crime categories, including fraud, forgery, and other serious crimes. Desktop research supports the systematic examination of official documents, statistical reports, classification manuals, and policy texts as social artefacts that reflect how institutionalised recording practices may obscure the scale and heterogeneity of cyber-enabled and cyber-dependent crimes. Such practices often result in phishing, ransomware, business email compromise, and identity theft being subsumed under conventional crime categories, thereby distorting the prevalence, trends, and patterns of cybercrime. In this regard, document-based research is uniquely positioned to expose the statistical invisibility of contemporary cyber threats, not because they do not exist, but because they are concealed by legacy classification and record-keeping systems (Barbieri et al., 2025).

This study therefore employed an interpretivist qualitative approach through document analysis. This included an examination of SAPS annual crime reports from 2013 to 2022; a review of legislation governing cybercrime, such as the Cybercrimes Act; an analysis of institutional reports from the Institute for Security Studies (ISS), the United Nations Office on Drugs and Crime (UNODC), and civil society organisations; and a review of academic and policy literature on cybercrime and policing. Through document analysis, patterns, meanings, discourses, misclassifications, and systemic reporting weaknesses within SAPS cybercrime data were identified.

3.2. Analytical Techniques

The analysis of documents was guided by three qualitative analytical methods. First, content analysis was employed to investigate how cybercrime is defined, categorised, and represented in SAPS reports and related policy documents. Second, thematic analysis was used to identify recurring themes, including underreporting, institutional capacity constraints, outdated methodologies, and data integrity issues. Third, a policy and framework review was

conducted to evaluate SAPS data management structures, legislative alignment, and the extent to which reporting practices are consistent with international standards such as the ICCS.

3.3. Suitability of the Design

The research design is well suited to this study because cybercrime data in SAPS are not generated mechanically but rather reflect interpretative decisions made by officers during the processes of recording and classifying data. Therefore, institutional records help understand how crime categories, recording procedures, and data systems are socially and administratively constructed. For this reason, the evaluation of data integrity should be based on an exploration of these interpretative processes and contextual influences rather than on statistical outputs alone. A document-based qualitative design, grounded in interpretivism, offers the depth and richness required to evaluate the production, structure, and influence of SAPS cybercrime statistics.

Using a symbolic interactionist orientation, the study acknowledges that the construction of meaning occurs through daily interactions, routine organisational activities, and negotiated understandings among officers, administrators, and information systems. This perspective sensitised the analysis to consider the taken-for-granted assumptions inherent in classification decisions, the framing of cybercrime in official discourse, and implicit distinctions between serious and less visible forms of crime. Although this emphasis on meaning-making and discretion may understate the significance of purely quantitative patterns, the researcher acknowledges this limitation. Explicit reflexivity is therefore necessary to maintain transparency regarding the interpretative filters applied during the analysis.

3.4. Sources of Data

The study used secondary sources of data exclusively, which were collected from a broad range of institutional, legislative, and academic documents relating to cybercrime reporting and digital policing in South Africa. The document corpus included SAPS annual crime statistics, crime trend publications, quarterly reports, and strategic plans; national legislative and policy instruments, such as the Cybercrimes Act, the Protection of Personal Information Act (POPIA), and other digital policing frameworks; government and parliamentary documents, including oversight briefings, committee reports, audit findings, and internal performance assessments; reports from international organisations and research

institutions, such as UNODC, INTERPOL, SABRIC, the ISS, and government accountability bodies; peer-reviewed academic publications on cybercrime, data integrity, law enforcement practices, and digital transformation; sectoral policy analyses; think tank briefs; and professional commentaries on data governance and crime statistics (Ogwo-Ude, 2023).

Cybercrime reporting, digital policing, data integrity, cybersecurity governance, and SAPS data systems served as the primary search keywords. The search was limited to sources published between 2013 and 2025, as this period corresponds to the timeframe covered by the SAPS cybercrime statistics analysed in the study. The primary geographic focus was South Africa, although comparative examples were drawn from jurisdictions with more developed crime classification and cybercrime reporting systems, including the United Kingdom, the United States, and Australia. As part of methodological rigour, documents exhibiting apparent political bias, lacking verifiable evidence, or containing incomplete data were excluded from the study. Only sources with institutional provenance, clear methodological foundations, and credible authorship were retained for analysis.

3.5. Instrumentation and Data Gathering Process

The principal instrument of the study was a structured data extraction matrix that was used to tabulate and analyse all documents included in the study. The matrix was developed to capture critical attributes relevant to assessing the integrity of SAPS cybercrime statistics, including: Document metadata (title, date, author, and institution); Institutional and legislative factors influencing cybercrime reporting; Definitions and classifications of cybercrime presented in the documents; Methods used to collect, report, and classify data; Problems identified in the documents, such as underreporting, misclassification, technological constraints, and institutional limitations; and Recommendations relating to cybercrime governance, digital policing, or statistical reform.

The instrument was piloted using a small sample of SAPS annual crime statistics reports and academic literature. The matrix was subsequently refined to improve clarity and consistency before being applied systematically to the entire document corpus. Data were extracted from the selected sources, including academic literature, cybercrime legislation, SAPS policy manuals, crime statistics reports, international guidelines (e.g., UNODC), and evaluations conducted by oversight bodies and research institutions. Document analysis is widely used to examine institutional data practices, policy texts, and governance structures

(Bowen, 2009; Bryman, 2016; Scott, 2014; UNODC, 2024). Based on the inclusion and exclusion criteria, 63 documents were selected for analysis.

3.6. Ensuring Trustworthiness of the Study

To ensure methodological rigour, the study adhered to the trustworthiness criteria of credibility, dependability, confirmability, and transferability proposed by Lincoln and Guba (1985).

Credibility. Credibility was enhanced through the triangulation of multiple sources of evidence, including SAPS crime statistics, legislation, independent audits, oversight reports, scholarly literature, and sectoral analyses. This approach minimised reliance on any single institutional perspective and enabled the cross-validation of interpretations.

Dependability. Dependability was achieved through the maintenance of a comprehensive audit trail documenting all sources accessed, data extraction procedures, coding decisions, and analytical processes. This enhanced consistency and transparency throughout the development of interpretations.

Confirmability. Confirmability was strengthened through reflexive memo writing, systematic comparison of interpretations across documents, and the presentation of evidence-based conclusions.

Transferability. Transferability was supported through the provision of thick descriptions of the institutional context, SAPS reporting arrangements, and cybercrime data environment, enabling readers to assess the applicability of the findings to other policing or data governance settings. In addition, documents were evaluated based on the credibility of authorship, institutional authority, transparency of the procedures employed (particularly in evaluation reports), and internal consistency prior to inclusion in the dataset.

3.7. Data Analysis

The first step of the analysis involved a qualitative content analysis of all selected documents. This process systematically facilitated the identification, grouping, and mapping of explicit references to data integrity problems, cybercrime reporting, and statistical data recording practices in scholarly and institutional literature. The documents were analysed to determine how cybercrime was defined and discussed, how offences were classified, and how reporting procedures within SAPS were described or critiqued. Particular attention was given

to identifying patterns of underreporting, misclassification, inconsistencies, and infrastructural or procedural barriers affecting the quality of cybercrime statistics. Content analysis enabled the systematic tracking of recurring ideas, institutional discourses, and the prevalence of specific data-related issues across different types of documents.

Following the content mapping process, thematic analysis was employed to generate deeper interpretive insights into the institutional, technological, and methodological processes influencing SAPS cybercrime data. In accordance with Braun and Clarke's six-phase approach (Braun & Clarke, 2006), the analysis involved: familiarisation with the context and underlying assumptions of SAPS reports, policy documents, and academic literature through repeated reading; generation of initial codes by labelling significant text segments referring to data quality issues, classification challenges, technological gaps, or institutional constraints; organisation of codes into preliminary categories such as "outdated recording methodologies," "capacity limitations," "misclassification of cybercrimes," and "fragmented reporting systems"; review and refinement of themes to ensure internal consistency and clear distinctions between thematic categories; naming and defining themes to capture their conceptual essence and relevance to the research objectives; and the development of a narrative synthesis linking the refined themes to the broader objective of evaluating the integrity of SAPS cybercrime statistics.

The combined use of content analysis and thematic analysis enabled the study to achieve both systematic categorisation (content analysis) and interpretive meaning-making (thematic analysis). This integrated approach provided a comprehensive understanding of how cybercrime data are constructed, interpreted, and communicated within SAPS, and how institutional, technological, and procedural factors influence the overall quality of digital policing data in South Africa.

3.8. Research Ethics

Although the study did not involve human participants, ethical considerations were carefully observed. These included:

Publicly available information. All documents used in the study were publicly available or were obtained through legitimate institutional repositories.

Intellectual property and proper attribution. All sources were properly acknowledged through appropriate citation and referencing to prevent plagiarism.

Integrity and accuracy. Interpretations were based on the analysed materials and presented accurately without misrepresenting the findings.

Sensitivity to the institution. The findings were presented in an objective and respectful manner, particularly when discussing sensitive assessments or institutional performance reviews.

Transparency. An audit trail was maintained throughout the study to ensure methodological transparency and accountability.

3.8. Study Limitations

The use of secondary data may limit access to internal SAPS processes and direct institutional perspectives. Publicly available documents and institutional reports may also be subject to certain limitations, including potential bias and the limited availability of disaggregated cybercrime statistics. Nevertheless, this qualitative approach provides a robust framework for critically analysing the integrity of cybercrime data within SAPS and identifying institutional reforms that may enhance digital policing in South Africa.

4. Findings

4.1. Completeness, Consistency, and Categorization of SAPS Cybercrime Data

Table 1

Overall assessment of SAPS cybercrime data from 2013 - 2022

Dimension	Score	Explanation
Completeness	Low	Extensive underreporting, no central system, cybercrime not disaggregated.
Consistency	Low–Moderate	Uneven station practices, outdated systems, weak digital capacity.
Categorization	Poor	Misclassification, non-standard taxonomies, no ICCS adoption.

Table 1 shows that SAPS cybercrime statistics cannot be relied upon to accurately quantify the extent of cybercrime or effectively guide digital policing strategies. This is because the data are inherently affected by systemic flaws, structural anomalies, and outdated classification frameworks. The weaknesses identified reflect persistent deficiencies in the

completeness, consistency, and categorisation of SAPS cybercrime statistics between 2013 and 2022. According to recent reports, SAPS cybercrime statistics remain incomplete due to ongoing underreporting, limited victim awareness, and the absence of a centralised national cybercrime reporting system, which results in fragmented datasets that distort the true prevalence of digital crimes (Faisal et al., 2025; Ngcece & Mkhize, 2023).

The problem of incompleteness is further exacerbated by institutional and technological constraints, including outdated digital infrastructure, unreliable reporting systems, and administrative delays, which hamper effective and timely data capture (de Kock, 2023; Mulaudzi et al., 2025). In terms of consistency, SAPS reporting has historically varied across stations and provinces, a situation that has only recently been addressed through revised standard operating procedures under the Cybercrimes Act. Reporting practices have also long been influenced by legacy crime-recording methods rooted in nineteenth-century English policing models (Kriegler, 2025; Modise, 2025). As a result, similar cyber incidents may be classified differently by individual officers, police stations, or technological systems, and may have created conflicting and sometimes incompatible datasets.

The SAPS cybercrime categorisation is not fit for purpose, as offences such as phishing, ransomware, identity theft, and business email compromise are routinely subsumed under broad categories such as “fraud,” “commercial crime,” or “other serious crimes,” thereby preventing disaggregated analysis and obscuring the behavioural and technological dimensions that define contemporary digital offences (Ogwo-Ude, 2023; Matsaung & Masiloane, 2025). This categorical inadequacy reflects SAPS’s failure to adopt international behaviour-based standards such as the ICCS, which would facilitate standardised, granular, and internationally comparable cybercrime statistics (UNODC, 2024; NASEM, 2025).

4.2. Prevalent Cybercrime Types in South Africa That Are Underrepresented or Misclassified in SAPS Statistics

Based on Table 2, a wide range of cybercrime types are prevalent in South Africa, yet they remain grossly underrepresented or miscategorised in SAPS crime statistics due to the use of outdated taxonomies and inadequate recording practices. These cybercrime types include:

Phishing and online scams, which constitute the most common forms of cyber-enabled victimisation, are frequently subsumed under broad categories such as fraud or commercial

crime, thereby obscuring their distinct digital modus operandi (Matsaung & Masiloane, 2025; Ngcece & Mkhize, 2023).

Table 2

Prevalent but underrepresented or misclassified cybercrimes in SAPS Statistics

Cybercrime Type	Description / Nature of Offense	How SAPS Misclassifies or Underrepresents It
Phishing & Online Scams	Deceptive emails/SMS/websites used to steal credentials or financial information.	Recorded mainly as general fraud or commercial crime, without indicating digital origins.
Ransomware & Digital Extortion	Malware that encrypts systems and demands payment for restoration; affects businesses and municipalities.	Often categorized under malicious damage to property or vaguely under computer-related crime; not separately listed.
Business Email Compromise (BEC)	Manipulation of business communication to divert payments through fraudulent emails.	Buried under fraud statistics, failing to capture the digital manipulation involved.
Identity Theft & Data Breach-related Fraud	Use of stolen personal data to impersonate victims or commit financial fraud.	Grouped under impersonation or forgery, obscuring cyber-enabled elements.
Romance Scams & Online Investment Fraud	Social engineering tactics using emotional manipulation or fake investment platforms.	Recorded as fraud with no indication of online or psychological components.
Malware & System Intrusions (Hacking, Botnets, Spyware)	Unauthorized access, system compromise, or malware deployment.	Categorized broadly under computer-related crime, lacking subcategories for attack types.
AI-driven Cybercrimes (Deepfakes, Synthetic Identity Attacks)	Use of AI-generated voices, images, or identities to deceive or commit financial theft.	Not officially recognized or categorized in SAPS databases due to outdated taxonomies.
Cyber-enabled Financial Fraud	Fraud facilitated entirely through digital platforms and online banking.	Merged with traditional financial fraud, masking digital vectors.

Ransomware and digital extortion, which increasingly target municipalities, critical infrastructure, and private firms, including high-profile attacks on City Power and the City of Johannesburg, are not recorded as separate categories and are often classified under unrelated categories such as malicious damage to property or generic computer-related crime (Modise, 2025; Vermeulen, 2025).

Business Email Compromise (BEC) is a major source of financial losses in the banking and corporate sectors, yet it is routinely aggregated within traditional fraud statistics, which

obscures its complexity and the technical channels through which offenders exploit digital communication systems (Ogwo-Ude, 2023; Kriegler, 2025).

Identity theft and data breach-enabled impersonation, which have increased due to the growing exposure of personal information, are often categorised alongside traditional impersonation or forgery offences. This prevents analysts from distinguishing between conventional forms of identity-related crime and digitally mediated forms of identity compromise (Ngcece & Mkhize, 2023).

Romance scams and online investment fraud, which have become increasingly prevalent through the use of social engineering techniques, are similarly absorbed into broad fraud categories without recognition of their online, psychological, and cross-border characteristics (Maboa & Horne, 2024).

In addition, malware-related crimes, including botnets, spyware, and unauthorised system access, are generally classified under broad computer-related crime categories, providing insufficient detail to distinguish between different technical attack vectors and forms of system compromise (Masiloane & Matsaung, 2025).

There also remains a significant gap in the adoption of contemporary cyber-threat taxonomies within national crime statistics. Emerging threats, including AI-mediated impersonation, deepfake-enabled fraud, and synthetic identity attacks, have not yet been formally recognised or classified within SAPS reporting frameworks (UNODC, 2024).

Many of the most harmful forms of cybercrime in South Africa are either not recorded separately or are aggregated under legacy crime categories. Consequently, the accuracy, analytical utility, and policy relevance of SAPS cybercrime statistics are significantly compromised.

4.3. Institutional and Technological Factors Contributing to Inconsistencies and Underreporting in SAPS Cybercrime Data

As Table 3 indicates, the SAPS faces significant institutional and technological shortcomings that contribute to the continued underreporting and misclassification of cybercrime. At the institutional level, SAPS lacks a unified and standardised cybercrime reporting system across its stations, resulting in inconsistent reporting practices and varying interpretations of similar cases by different officers (Ngcece & Mkhize, 2023). This fragmentation is further compounded by the absence of a centralised national cybercrime

reporting system, which results in parallel and, in many cases, incompatible data streams that hinder effective national data aggregation. From a technological perspective, SAPS continues to rely on outdated and unreliable digital infrastructure, including ageing communication systems (VSAT), poorly integrated databases, and malfunctioning command-and-control platforms, all of which undermine the accuracy and timeliness of case registration (de Kock, 2023).

Table 3

Identified factors contributing to inconsistencies and underreporting in SAPS cybercrime data

Factor Category	Specific Factor	Description of Impact on Cybercrime Data Quality
Institutional	Fragmented Reporting Protocols	Lack of standardized procedures across stations leads to uneven classification and inconsistent reporting of cyber incidents
Institutional	Absence of a Centralized Cybercrime Reporting System	Cybercrime data is collected through disjointed channels, resulting in incomplete national
Institutional	Limited Staff Capacity and Training	Officers lack digital forensic skills and up-to-date knowledge of cybercrime investigation, causing misclassification and incomplete data capture.
Institutional	Bureaucratic Resistance and Slow Reform Implementation	Resistance to technological modernization and slow adoption of Cybercrimes

These shortcomings contribute to delays, data loss, and inconsistencies in the recording of critical digital evidence. Moreover, the organisation faces significant capacity and training challenges, as many officers lack the technical skills required to conduct digital investigations, classify cybercrimes, and manage electronic evidence effectively. Outdated forensic software licences and limited access to cyber intelligence tools further constrain investigative capabilities (Modise, 2025; Matsaung & Masiloane, 2025).

Together with bureaucratic inertia, institutional resistance to technological change, and political interference, these challenges slow modernisation initiatives, undermine the implementation of updated Standard Operating Procedures under the Cybercrimes Act, and reduce the effectiveness of SAPS information systems. Consequently, public confidence in SAPS's ability to respond to cybercrime may be weakened, further reinforcing underreporting. At the same time, internal structural and technological inefficiencies continue to compromise the integrity, completeness, and consistency of official cybercrime statistics.

4.4. Framework for Improving Integrity, Categorization, and Reporting of Cybercrime Data Within SAPS

A robust framework for enhancing the integrity, categorisation, and reporting of cybercrime data within the SAPS should incorporate behaviour-based classification standards, enterprise data governance disciplines, and organisational practice reforms within a unified sociotechnical framework. Fundamentally, SAPS should adopt the ICCS and develop a national correspondence table that maps existing offence categories (e.g., fraud, commercial crime, and computer-related crime) to ICCS cyber-dependent and cyber-enabled subtypes (e.g., phishing, business email compromise, ransomware, identity theft, and system intrusion), supported by published counting rules (NASEM, 2025; South African Police Service, 2023; South African Police Service, 2024; UNODC, 2024).

Furthermore, to ensure that improved categories translate into reliable statistics, SAPS should institutionalise data governance through the principles of DAMA-DMBOK and COBIT 2019 (Adams, 2024). This would involve establishing stewardship responsibilities across national and station levels, enforcing metadata and lineage standards (e.g., offence vector, targeted asset, harm, and evidence source), and implementing automated data quality (DQ) controls and scorecards based on the core dimensions of accuracy, completeness, consistency, timeliness, and validity. Since cybercrime records also function as evidentiary artefacts, the Records Continuum Model should be embedded within the framework to ensure that provenance, chain of custody, and contextual metadata remain attached to digital evidence throughout the processes of capture, analysis, and public reporting (Upward, 1996).

These governance mechanisms should be operationalised through a centralised cybercrime reporting and case management platform that integrates public and business reporting channels with station-level data capture, incorporates ICCS classification prompts at the point of entry, securely integrates with banks, internet service providers (ISPs), and SABRIC for data reconciliation and deduplication, and provides near-real-time dashboards for monitoring data quality and supporting intelligence-led policing (Ogwo-Ude, 2023).

Lastly, organisational practice reform is essential for sustainable improvement. This includes the implementation of national standard operating procedures aligned with the Cybercrimes Act, continuous training in ICCS coding and digital forensics, supervisory review of ambiguous cases, and performance incentives linked to inter-rater agreement and improvements in data quality. Such measures would make accurate and granular recording the

path of least resistance, thereby generating the trustworthy data required for ILP and EBP (Lipsky, 2010; Ratcliffe, 2016; Modise, 2025; Matsaung & Masiloane, 2025).

5. Discussion

This study examined the integrity of SAPS cybercrime statistics through the Sociotechnical Data Governance Model for Digital Policing (SDGDP). It linked empirical findings directly to four research concerns: data completeness, cybercrime misclassification, institutional and technological constraints, and implications for policing effectiveness. The discussion demonstrates that deficiencies in SAPS cybercrime data are systemic and arise from misalignment across classification standards, data governance mechanisms, and organisational practices rather than from isolated technical or human errors.

The findings show that SAPS cybercrime data are substantially incomplete, driven by pervasive underreporting and fragmented data capture mechanisms. From a sociotechnical perspective, underreporting is produced not only by victim reluctance but also by the absence of a centralised national cybercrime reporting platform, weak public-facing intake mechanisms, and inconsistent internal registration practices. Within the SDGDP framework, this indicates failure at Layer 2 (Data Governance and Quality). In the absence of formal stewardship, metadata standards, and lifecycle accountability, cybercrime records deteriorate in terms of completeness and timeliness. This is consistent with prior national and international findings (see ISS, 2024; UNODC, 2024; Ngcece & Mkhize, 2023), which indicate that cybercrime is systematically undercounted in official SAPS statistics. This governance gaps structurally produce empirical invisibility.

The findings further show that high-impact offences, such as phishing, ransomware, business email compromise, and identity theft, are frequently subsumed under broad categories such as “fraud” or “commercial crime.” Persistent misclassification is best explained by Layer 1 of the SDGDP framework (Classification Standards), combined with frontline discretion. SAPS continues to rely on legalistic, outcome-based taxonomies developed for pre-digital crime patterns. In the absence of ICCS-aligned, behaviour-based classifications, officers lack clear conceptual distinctions between cyber-enabled and conventional offences. Drawing on Street-Level Bureaucracy Theory, officers operating under workload pressures and ambiguous rules may rationally default to familiar fraud classifications. Misclassification therefore represents an institutional adaptation rather than ignorance or negligence. This finding

challenges assumptions in the cybercrime measurement literature that improved awareness or technology alone can resolve classification failures.

Moreover, obsolete infrastructure, fragmented reporting protocols, uneven training, and the slow implementation of the Cybercrimes Act jointly undermine data integrity. These constraints operate across all SDGDP layers but are most visible at Layer 2 (Data Governance) and Layer 3 (Organisational Practice). From a sociotechnical systems perspective, technology and practice are mutually constitutive. Infrastructure limitations shape recording behaviour, while organisational routines repurpose digital systems in ways that reproduce legacy practices. As a result, technological upgrades without governance reform and workflow redesign merely digitise existing data failures. Such outcomes have been consistently observed in international policing contexts (see UNODC, 2024; Lee et al., 2024).

Data failure emerges from misalignment across all SDGDP layers. For example, outdated classification standards create ambiguity; weak governance permits drift and inconsistency; and discretionary organisational practices fill gaps through administrative shortcuts. None of these failures alone explains poor data quality, but their interaction does. This layered explanation confirms the SDGDP proposition that cybercrime data integrity is a sociotechnical outcome requiring coordinated reform.

Poor data integrity has direct consequences for ILP and EBP. ILP depends on accurate and granular data to detect emerging threats and prioritise harm. Misclassification and undercounting distort threat assessments and limit cyber intelligence development. Similarly, crime mapping and trend analysis become unreliable when cyber incidents are effectively invisible. For EBP, inconsistent data undermine intervention evaluation and strategic learning. Resource allocation is likewise distorted because recorded demand fails to reflect actual cybercrime prevalence. These deficiencies also weaken public accountability, eroding trust in official crime statistics and limiting meaningful oversight.

South Africa mirrors global trends in which cybercrime victimisation has outpaced crime-recording reform but diverges from jurisdictions that have adopted centralised reporting platforms and standardised cybercrime classifications. The study contributes to global debates on cybercrime measurement by empirically demonstrating how misclassification and underreporting are institutionally produced. It further advances digital policing scholarship in the Global South, where empirical analyses of cybercrime data integrity remain limited, by applying the SDGDP framework to a real-world policing system.

Finally, reliance on secondary data and the lack of access to internal SAPS workflows limit direct observation of recording practices. However, this interpretive constraint highlights the value of document-based analysis in revealing systemic patterns embedded within institutional texts and statistical reports. The findings should therefore be understood as diagnosing structural dynamics rather than individual failures.

6. Conclusion

The current SAPS cybercrime reporting is incomplete, inconsistently applied, and poorly categorised due to outdated taxonomies, the absence of disaggregated reporting systems, and limitations in the collection and management of digital evidence. These constraints mirror international challenges, where crime-recording systems developed to address physical, location-bound offences struggle to capture digital crimes, particularly in an environment where cybercrime victimisation has become comparable to, or even exceeded, many forms of traditional crime. These challenges are further exacerbated by institutional factors, including political interference, leadership instability, outdated infrastructure, and the slow implementation of reforms. However, improving cybercrime data integrity is not merely a technical undertaking but a sociotechnical transformation requiring alignment among classification standards, governance mechanisms, and organisational practices, precisely the integration envisioned by the SDG-DP framework. Enhancing data integrity is therefore a fundamental requirement for effective digital policing, improved public accountability, and the restoration of confidence in South Africa's crime statistics system.

7. Recommendations

Increase the use of standardised classification frameworks in cybercrime reporting. To make cybercrime statistics more useful and actionable, SAPS should adopt and standardise ICCS-aligned crime classifications, ensuring that cyber-dependent and cyber-enabled crimes are recorded consistently across all stations. This would reduce misclassification and enable more targeted policy responses. Specific classification guidelines, correspondence tables, and counting rules should also be developed and enforced nationally to promote classification rigour at all levels of data capture.

Enhance data quality management and governance structures for digital policing. To clarify roles, decision-making authority, and accountability mechanisms relating to cybercrime data, SAPS should formalise a comprehensive data governance framework based on the principles of DAMA-DMBOK and COBIT. This should include the implementation of regular data quality management processes focusing on accuracy, completeness, consistency, timeliness, and metadata compliance to strengthen data integrity and organisational accountability.

Strengthen capacity for digital evidence management and cybercrime investigation. To address existing capacity constraints, SAPS should implement structured and continuous training programmes in cybercrime investigation, ICCS classification, digital forensics, and electronic evidence management. Capacity-building initiatives should also be extended to supervisors and analysts to ensure organisation-wide data quality oversight and reduce reporting disparities across stations.

Expand digital-era service delivery through centralised and integrated reporting systems. SAPS should establish a centralised national cybercrime reporting and case management platform that integrates public-facing reporting channels, business incident reporting systems, and internal police support systems. The platform should be formally integrated with banks, internet service providers (ISPs), SABRIC, and Computer Security Incident Response Teams (CSIRTs) to improve situational awareness, facilitate real-time intelligence sharing, and enhance responsiveness to cyber threats.

Improve accountability, transparency, and trust in cybercrime statistics. To strengthen credibility and public oversight, SAPS should ensure that cybercrime statistics are published in a timely manner and accompanied by methodological notes and data quality indicators. Independent audits, public dashboards, and regular external reviews should be implemented to increase transparency and reinforce the principles of accountable digital policing.

Advance digital policing through participatory and multi-stakeholder approaches. SAPS should formalise public-private partnerships and stakeholder engagement mechanisms to facilitate cyber intelligence sharing, strengthen collaborative reporting, and improve responsiveness to emerging digital threats. These initiatives should be supported by public awareness programmes that encourage reporting and address chronic underreporting resulting from technical complexity and public distrust.

Address systemic barriers to evidence-based cybercrime governance. Reform efforts should focus on structural barriers that impede evidence-based policing, including leadership instability, political interference, outdated infrastructure, and slow implementation processes. Strengthening institutional stability and modernising digital infrastructure are essential to achieving the alignment of classification, governance, and organisational practice envisioned by the SDG-DP framework.

Promote continuous improvement through research and evaluation. Collaboration among government agencies, academic institutions, and civil society research organisations should be encouraged to support empirical research on underreporting, classification accuracy, and emerging cybercrime typologies. Further evaluation is needed to assess how SDG-DP reforms influence data quality, ILP, public trust, and the overall effectiveness of digital policing, thereby ensuring that cybercrime governance remains adaptive and evidence-based.

Disclosure statement

The authors declare no potential conflict of interest.

Funding

This work received no funding.

AI Declaration

The research utilised a range of AI-assisted tools to enhance its rigour, clarity, and efficiency. Microsoft Copilot and Grammarly were used to support literature searching, refine academic writing, and improve the overall readability and tone of the manuscript. Human-authored text was also refined using AI tools, specifically wording, structure, and formatting. The author retained full responsibility for reviewing, verifying, and editing all AI-assisted content to ensure its accuracy, appropriateness, and compliance with academic standards.

References

Adams, N.-R. (2024, September 19). *COBIT 2019: IT governance framework*. ITLawCo. https://itlawco.com/cobit-2019-it-governance-framework/

Aphane, M. P. (2025). Policing cybercrime in South Africa: Issues and challenges. *International Journal of Research in Business and Social Science, 14*(6), 415–421. https://doi.org/10.20525/ijrbs.v14i6.4148

Barbieri, M., Catania, G., Hayter, M., Aleo, G., Zanini, M., Sasso, L., & Bagnasco, A. (2025). Desk review as a methodological approach for identifying policies and gray literature: A case study. *Nursing Outlook, 73*(6), Article 102547. https://doi.org/10.1016/j.outlook.2025.102547

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). Sage.

de Kock, C. (2023, September 30). Overcoming technological hurdles in South African Police Service's crime reporting. *Cape Town Today*. https://tinyurl.com/yc42ndzp

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The Sage handbook of qualitative research* (4th ed.). Sage.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change, 67*(1), 97–116. https://doi.org/10.1007/S10611-016-9649-Z

Emerson, B. D. (2026). Complete cybercrime statistics: Global trends, costs, and key data. *BD Emerson*. https://www.bdemerson.com/article/complete-cybercrime-statistics

Faisal, M., Kumar, S., Mahmood, F., & Talha, M. (2025). *Cyber Bulletin October Edition 2025*. Zenodo. https://doi.org/10.5281/zenodo.17571160

Huey, L., & Buil-Gil, D. (2024). *The crime data handbook*. Bristol University Press.

Joosub, I. (2025). *Integrity and oversight in South Africa's law enforcement (1994–2025)*. FW de Klerk Foundation.

Kriegler, A. (2025, October 22). Crime statistics belong to the public, not the police. *Institute for Security Studies*. https://issafrica.org/iss-today/crime-statistics-belong-to-the-public-not-the-police

Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of big data-driven predictive policing: Systematic review. *Justice Evaluation Journal, 7*(2), 127–160. https://doi.org/10.1080/24751979.2024.2371781

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Lipsky, M. (2010). *Street-level bureaucracy: Dilemmas of the individual in public service* (30th anniversary ed.). Russell Sage Foundation.

Lukens, P. (2025). Unintended exposure: The risks of searchable ChatGPT conversations for police departments. *Philip Lukens Substack*. https://philiplukens.substack.com

Maboa, M., & Horne, J. (2024). Bridging the gap: Unpacking the role of the SAPS Crime Information Management and Analysis Centre in advancing evidence-based policing in South Africa. *OIDA International Journal of Sustainable Development, 17*(12), 137–150.

Madondo, N., Khosa, D., & Abdulkareem, K. (2025). Unveiling the efficacy of the SAPS's approach to tackling contact crime in the Ethekwini district through crime statistics analysis. *International Journal of Business Ecosystem & Strategy, 7*(4), 177–186. https://doi.org/10.36096/ijbes.v7i4.895

Matsaung, P., & Masiloane, D. T. (2025). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review, 34*(2), 152–167. https://doi.org/10.1080/10246029.2024.2421225

Modise, J. M. (2025). The impact of capacity building initiatives on the SAPS's ability to investigate and prosecute cybercrime. *IRASS Journal of Arts, Humanities and Social Sciences, 2*(2).

Mpuru, L., & Kgoale, C. (2026). Recognizing the evolving cybercrime threats in South Africa. *African Security, 19*(1), 36–60. https://doi.org/10.1080/19392206.2025.2515302

Mulaudzi, M. J., & Molokomme, R. T. (2025). The crisis behind police crime data: Unreported crime and challenges related to crime statistics in South Africa. *International Journal of Innovative Research and Scientific Studies*. https://doi.org/10.53894/ijirss.v8i12.11109

National Academies of Sciences, Engineering, and Medicine. (2025). *Cybercrime classification and measurement*. National Academies Press. https://doi.org/10.17226/29048

Newman, G. (2024). Cybercrime victimization: Global patterns and local realities. *Journal of Cybersecurity Studies, 9*(1), 1–18.

Ngcece, S., & Mkhize, S. M. (2023). An exploratory study of the South African Police Services (SAPS) systems in combating cybercrime. In S. O. Ehiane, S. A. Olofinbiyi, & S. M. Mkhize (Eds.), *Cybercrime and challenges in South Africa* (pp. 159–175). Palgrave Macmillan. https://doi.org/10.1007/978-981-99-3057-9_7

Ogwo-Ude, O. (2023). Business email compromise challenges to medium and large-scale firms in USA: An analysis. (2023). *Open Journal of Applied Sciences, 13*(6), 803–812. https://doi.org/10.4236/ojapps.2023.136064

Parliament of the Republic of South Africa. (2025, November 4). Media statement: Weaknesses in SAPS supply chain management is a breeding ground for corruption and leads to wastage. https://tinyurl.com/mw899b6j

Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge. https://doi.org/10.4324/9781315717579

Sawyer, S., & Jarrahi, M. H. (2013). Sociotechnical approaches to digital work. *The Information Society, 29*(4), 249–253.

Scott, J. (2014). *A matter of record: Documentary sources in social research* (2nd ed.). Polity Press.

Sherman, L. W. (1998). *Evidence-based policing*. Police Foundation.

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review, 4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

South African Police Service. (2023). *Cybercrime prevention tips*. https://www.saps.gov.za

South African Police Service. (2024). *Annual crime statistics report*. https://www.saps.gov.za

Tisdell, E. J., Merriam, S. B., & Stuckey-Peyrot, H. L. (2025). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

UK Statistics Authority. (2021). *Annual report and accounts 2020/21*. https://uksa.statisticsauthority.gov.uk/publication/annual-report-and-accounts-2020-21/

UNODC. (2024). *International classification of crime for statistical purposes (ICCS)*. United Nations Office on Drugs and Crime.

Upward, F. (1996). Structuring the records continuum—Part one: Postcustodial principles and properties. *Archives and Manuscripts, 24*(2), 268–285. https://publications.archivists.org.au/index.php/asa/article/view/8583

Vermeulen, J. (2025, October 26). South Africa is under cyber attack. *MyBroadband*. https://mybroadband.co.za/news/security/615523-south-africa-is-under-cyber-attack.html

Wand, Y., & Wang, R. Y. (1996). Anchoring data quality dimensions. *Communications of the ACM, 39*(11), 86–95. https://doi.org/10.1145/240455.24047

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems, 12*(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099

Zikalala, N. I. (2025). The perceptions of safety and police visibility among secondary victims of gender-based violence in Soweto Township, Gauteng Province, South Africa. *International Review of Social Sciences Research, 5*(4), 157–176. https://doi.org/10.53378/irssr.353292

Zindi, B., & Majam, T. (2025). Advancing public service professionalism: A path towards effective governance in South Africa. *International Review of Social Sciences Research, 5*(4), 260–285. https://doi.org/10.53378/irssr.353296