The Cyber Threat Landscape in South Africa: A 10-Year Review

Heloise Pieterse
Senior Researcher and Cybersecurity Specialist, Information and Cybersecurity Centre, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-2908-4012

Abstract

The world is witnessing a rise in cyber-related incidents. As information technology improves and the reliance on technology increases, the frequency and severity of cyber incidents escalate. The impact is felt globally, and South Africa is not immune to the effects. The country's fast-paced technological evolution continues to increase the attack surface within the cyber domain. The increased attack surface is confirmed by recent cyberattacks affecting well-known and established South African organisations. This article reviews findings from an evaluation of South Africa's cyber threat landscape that analysed 74 cyber incidents identified as occurring between 2010 and 2020. The 74 incidents are categorised according to *incident type*, *affected sector*, *perpetrator type*, and *motivation*. It is found that the most common incident type is *data exposure*, the most-affected sector is the *public* sector, the most prevalent perpetrators are *hackers*, and the most common motivation is *criminal.* The article makes recommendations about how South Africa can reduce the risk factors in its cyber threat landscape.

Keywords

cybersecurity, cyber threats, cyberattacks, cyber incidents, attack surface, compromised websites, cybercrime, data exposure, system intrusion, denial of service

DOI: https://doi.org/10.23962/10539/32213

Recommended citation

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

1. Introduction

The prevalence of cyber incidents globally contributes to the ever-increasing cybersecurity concerns. Well-known and established organisations, such as Solar Winds (Willett, 2021) and Microsoft (Wyatt, 2021), have fallen victim to sophisticated cyberattacks. South Africa is not immune, and has witnessed a steady increase in cyberattacks in recent years. 2019 proved pivotal as South Africa experienced a cross-industry spike in cyber incidents (Mcanyana et al., 2020), a trend that continued in 2020 and was further driven by the COVID-19 pandemic.

The City of Johannesburg (CoJ), a metropolitan municipality responsible for local governance, suffered two noteworthy cyber incidents during 2019 (Moyo, 2019a). First, in July, a ransomware attack affected City Power, CoJ's electricity utility. Second, in October, a network breach was detected after a ransom note was received from a group called the Shadow Kill hackers. Both cyber incidents caused downtime to several customer-facing systems. Following the breach at CoJ, the South African Bank Risk Information Centre (SABRIC) confirmed that the banking sector had been targeted by a wave of distributed denial of service (DDoS) attacks (Moyo, 2019b).

In 2020 the COVID-19 pandemic caused a surge in cyber incidents as the pandemic created new opportunities for attackers to exploit. During May, an accidental data leak caused by changes to the Unemployment Insurance Fund (UIF) website—changes made to accommodate the Temporary Employee/Employer Relief Scheme (TERS)—exposed employers' confidential information. The issue causing the data leak was reported by a security researcher and subsequently resolved by the UIF (Vermeulen, 2020a). In June 2020, the second-largest private hospital operator in South Africa, Life Healthcare Group, fell victim to a cyberattack. Although the full extent of the attack remains unclear, Life Healthcare Group confirmed that the attack affected admissions systems, business processing systems, and e-mail servers (Mungadze, 2020). Two months later, South Africa suffered a massive data breach when Experian, a credit bureau agency, exposed personal information to a suspected fraudster. The exposed personal information affected approximately 24 million South Africans, as well as 800,000 business entities (Moyo, 2020a). The remainder of 2020 continued to witness various cyber incidents affecting South Africa's financial, public, construction, and telecommunication sectors.

In 2021, the attractiveness of South Africa as a cyber target was further demonstrated by the large-scale cyberattack that affected Transnet, the South African state-owned rail, port, and pipeline company (Moyo, 2021). According to Noëlle van der Waag-Cowling, a cyber programme lead at the Security Institute for Governance and Leadership in Africa, the incident has been described as an act of "cyber warfare" and serves as a warning to South Africa (Goldstuck, 2021; Slabbert & Peyper, 2021).

Shortly thereafter, the Department of Justice and Constitutional Development confirmed a security breach that affected its information technology system. The breach was the result of ransomware, causing all the department's systems to be encrypted and unavailable to both internal employees and members of the public (Ngqakamba, 2021).

Globally, cyber incidents are well-documented in peer-reviewed scholarly articles and research reports. In South Africa, however, despite the steady increase in cyber incidents, the formal reporting of such incidents is not common. Neither the South African Police Service (SAPS) nor the National Prosecuting Authority (NPA) offers resources or statistics pertaining specifically to local cyber incidents. The Cybersecurity Hub—South Africa's national Computer Security Incident Response Team (CSIRT)—provides a service for stakeholders to report cyber incidents, but it does not report such incidents to the general public. Furthermore, few peer-reviewed articles exist that have evaluated South African cyber incidents. One notable exception is the Van Heerden et al. (2016) review of 12 South African cyber incidents that occurred between 1994 and 2015. Van Heerden et al. (2016) presented a new visual classification scheme for cyber incidents, which facilitates the representation of the cyber incidents according to eight distinct classes: attacker, goal, mechanism, effect, motivation, target, vulnerability, and scenario (Van Heerden et al., 2016). Another noteworthy exception is Van Niekerk's (2017) presentation of a comprehensive high-level analysis of 54 cyber incidents that affected South Africa between 1994 and 2016. Van Niekerk (2017) classifies the incidents according to impact, perpetrator, and victim types, finding the leading perpetrators to be criminals and hacktivists, and the leading impacts of the cyber incidents to be data exposure and financial theft (Van Niekerk, 2017).

Although the two above-mentioned studies do offer insight into South Africa's cyber threat landscape, they only address incidents up to the end of 2015 and 2016 respectively. This article considers a full decade of cyber incidents, from 2010 to 2020, providing an analysis of 74 newsworthy cyber incidents that affected South Africa during that period. The cyber incidents considered are categorised according to *incident type*, *sector affected*, *perpetrator type*, and *motivation*. This categorisation permits a detailed trend analysis and a picture of South Africa's current cyber threat landscape.

2. Methodology

Data collection

Since information was not readily available from official sources (e.g., SAPS, the NPA, the national CSIRT), the cyber incidents analysed were identified by reviewing published peer-reviewed articles and media reports (e.g., reports published by *ITWeb*, *MyBroadband* and *BusinessTech*), as well as by conducting targeted online searches. The selection of cyber incidents was based on the following: the incident affected a South African organisation(s) or citizens; and the impact of the incident caused a breach (either network or data), affected services, or led to financial loss. A total of 74 cyber incidents occurring in the decade from January 2010 to December 2020 were identified.

Data analysis

Insight and guidance were taken from the approaches used by Van Heerden et al. (2016) and Van Niekerk (2017) in deciding how to categorise the 74 cyber incidents. A classification scheme was developed that consisted of four classifications, namely *incident type*, *sector affected*, *perpetrator type*, and *motivation*.

Incident type

The first classification, *incident type*, classifies the cyber incident according to one of the following types:

- *Compromised website:* intentional or unintentional activity affecting the confidentiality, integrity, or availability of the website (Kumar et al., 2019);
- *Cybercrime*: criminal activity involving a computer, network device, or network causing financial impact (Brush, n.d.);
- *Data exposure*: disclosure or leakage of data or information within the public domain (Sabillon et al., 2016; Van Niekerk, 2017);
- *System intrusion*: unauthorised or illegitimate access to a system or network (Kakareka, 2014; Van Niekerk, 2017); or
- *Denial of service*: preventing authorised or legitimate users from accessing network resources or affecting operations (Sabillon et al., 2016; Van Niekerk, 2017).

Sector affected

The second classification, *sector affected*, classifies the incident in terms of the area of the economy in which it occurred, with the following potential classifications: *construction*, *financial*, *healthcare*, *information technology (IT)*, *leisure and hospitality*, *manufacturing*, *media*, *public*, *retail*, *telecommunications*, *transportation*, or *other.*

Perpetrator type

The third classification, *perpetrator type*, classifies the individual or group responsible for the cyber incident as being of one of the following types:

- *Hacktivist*: an individual or group of individuals affiliated with activists' groups promoting political agendas or social change (Sabillon et al., 2016; Van Niekerk, 2017);
- *Insider:* an individual with a trusted relationship, institutional knowledge, and legitimate access, but acting maliciously for personal gain (Van Heerden et al., 2012; 2016; Van Niekerk, 2017);
- *Hacker:* a well-versed or unskilled individual using tools developed by elite computer users to break security and infiltrate networks or information systems (Van Heerden et al., 2016; Van Niekerk, 2017);

- *Cybercriminal*: an individual or group of individuals affiliated to criminal groups motivated by financial gain (Van Niekerk, 2017);
- *Nation state*: state-sponsored sophisticated hackers who target the information systems or networks of other countries (Sabillon et al., 2016; Van Niekerk, 2017); or
- *Non-malicious individual*: a person causing internal or external disclosure of a security flaw or a vulnerability affecting an information system.

Motivation

The fourth classification, *motivation*, classifies the rationale behind the cyber incident according to one of the following motives:

- *Political*: driven by a political aspect, such as political reasoning, spreading propaganda, or attacking political enemies (Gandhi et al., 2011; Van Heerden et al., 2012);
- *Economic*: illegal actions driven by financial gain, e.g., deploying ransomware with the purpose of acquiring paid ransom (Gandhi et al., 2011; Van Heerden et al., 2012; 2016);
- *Fun/Personal*: driven by a desire to prove skills, to solve challenging problems, or to expose security flaws, i.e., driven by non-malicious intentions (Van Heerden et al., 2012; 2016);
- *Accidental*: unintentional or unexpected discovery of a security flaw or vulnerability; or
- *Criminal*: conscious decision to intentionally conduct wrongdoing or criminal intent (but lacking financial incentive), e.g., performing a system intrusion to access personally identifiable information (PII) (Van Heerden et al., 2012; 2016).

3. Findings

High-profile cyber incidents identified

Examples of high-profile cyber incidents identified include:

2012

A hacker called H4ksniper claimed responsibility for disrupting three South African government websites (*MyBroadband*, 2012). Subsequently, various other South African websites fell victim to either hacktivists or hackers.

2014

Unpatched security vulnerabilities resulted in the mass hacking of South African websites that were using outdated versions of web content management systems such as Joomla and WordPress (*MyBroadband*, 2014). The hacks involved the insertion of hidden links to international websites to improve the page rank of the websites on the Google and Bing search engines.

2013–2014

These two years saw several accidental exposures of confidential data. Security researchers found on multiple occasions the exposure of PII by South African mobile operator, Vodacom (Muller, 2013; *BusinessTech*, 2014). Such exposure of PII can have grave consequences for organisations, especially with the coming into force of South Africa's 2013 Protection of Personal Information Act (POPIA) on 1 July 2021 (RSA, 2013).

2016-2020

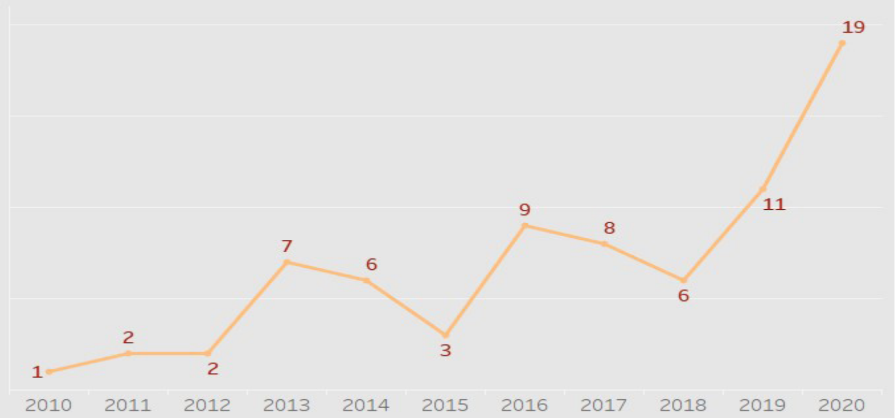
Compromised websites remained frequent in the second half of the decade (McKane, 2020a; Moyo, 2017; *MyBroadband*, 2018; Mzekandaba, 2019; Vermeulen, 2016). Also significant in this period was an increase in cyber incidents exposing data. While accidental exposure of data persisted (*MyBroadband*, 2016), data exposure was increasingly politically or criminally motivated (*BusinessTech*, 2016; Moyo, 2019c).

A global trend during the latter half of the decade was the frequent occurrence of ransomware attacks. During 2017, such attacks (WannaCry and NotPetya) were driven by EternalBlue, a Windows zero-day exploit targeting a vulnerability in the server message block (SMB) protocol (Trautman & Ormerod, 2019). Originally developed by the US National Security Agency (NSA), EternalBlue was leaked by the Shadow Brokers hacker group, causing a global cyberattack. Several South African organisations were also affected by large-scale ransomware attacks, including telecommunications provider, Telkom, the Office of the Chief Justice, and a stolen vehicle recovery company, Tracker (Moyo, 2020b; *MyBroadband*, 2017; Rawlins, 2017; Vermeulen, 2020b; 2020c).

Annual frequency of cyber incidents

As seen in Figure 1, the data revealed annual increases in cyber incidents for most (but not all) of the years studied, with a particularly sharp annual increase from 2019 (11 incidents) to 2020 (19 incidents).

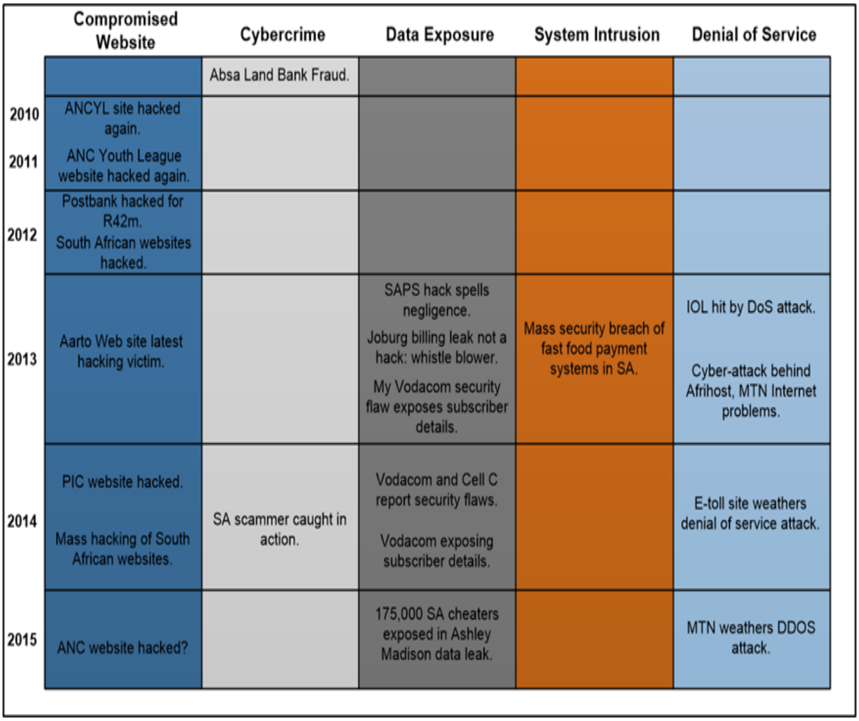
Figure 1: Annual cyber incident totals, 2010–2020



Incident type

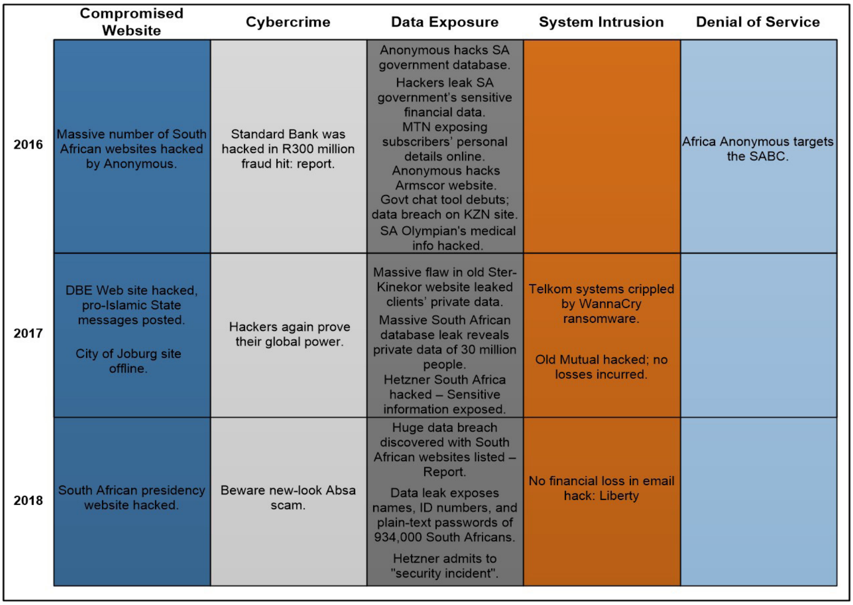
Figures 2 to 4 present the classification of the 74 cyber incidents according to incident type, in three periods: 2010–2015, 2016–2018, and 2019–2020. All the cyber incidents are represented by the actual title used in media reports.

Figure 2: Classification of cyber incidents by type, 2010–2015 (21 incidents)



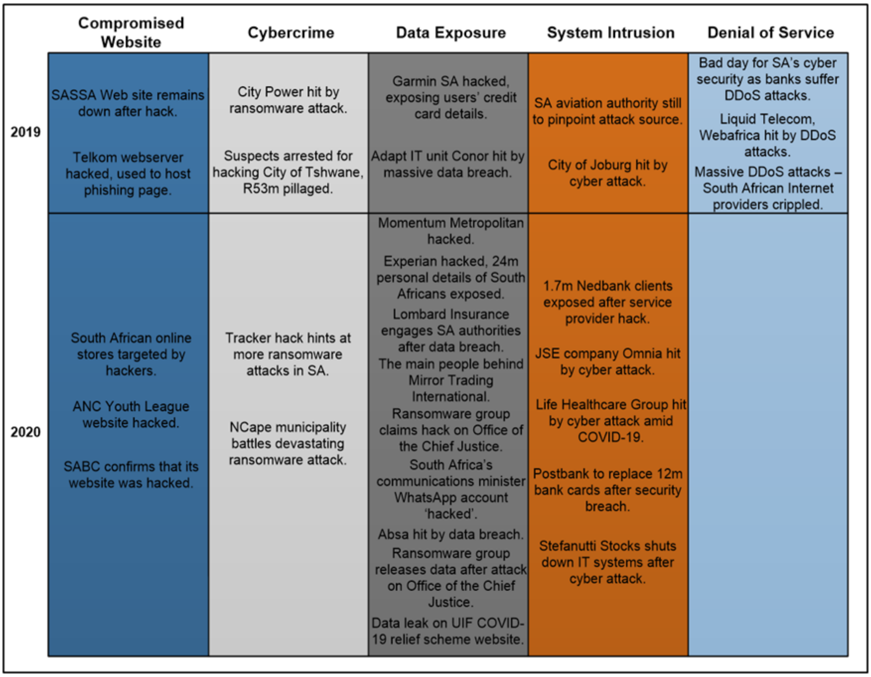
	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
		Absa Land Bank Fraud.			
2010 2011	ANCYL site hacked again. ANC Youth League website hacked again.				
2012	Postbank hacked for R42m. South African websites hacked.				
2013	Aarto Web site latest hacking victim.		SAPS hack spells negligence. Joburg billing leak not a hack: whistle blower. My Vodacom security flaw exposes subscriber details.	Mass security breach of fast food payment systems in SA.	IOL hit by DoS attack. Cyber-attack behind Afrihost, MTN Internet problems.
2014	PIC website hacked. Mass hacking of South African websites.	SA scammer caught in action.	Vodacom and Cell C report security flaws. Vodacom exposing subscriber details.		E-toll site weathers denial of service attack.
2015	ANC website hacked?		175,000 SA cheaters exposed in Ashley Madison data leak.		MTN weathers DDOS attack.

Figure 3: Classification of cyber incidents by type, 2016–2018 (23 incidents)



	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
2016	Massive number of South African websites hacked by Anonymous.	Standard Bank was hacked in R300 million fraud hit: report.	Anonymous hacks SA government database. Hackers leak SA government's sensitive financial data. MTN exposing subscribers' personal details online. Anonymous hacks Armscor website. Govt chat tool debuts; data breach on KZN site. SA Olympian's medical info hacked.		Africa Anonymous targets the SABC.
2017	DBE Web site hacked, pro-Islamic State messages posted. City of Joburg site offline.	Hackers again prove their global power.	Massive flaw in old Ster-Kinekor website leaked clients' private data. Massive South African database leak reveals private data of 30 million people. Hetzner South Africa hacked – Sensitive information exposed.	Telkom systems crippled by WannaCry ransomware. Old Mutual hacked; no losses incurred.	
2018	South African presidency website hacked.	Beware new-look Absa scam.	Huge data breach discovered with South African websites listed – Report. Data leak exposes names, ID numbers, and plain-text passwords of 934,000 South Africans. Hetzner admits to "security incident".	No financial loss in email hack: Liberty	

Figure 4: Classification of cyber incidents by type, 2019–2020 (30 incidents)



	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
2019	SASSA Web site remains down after hack. Telkom webserver hacked, used to host phishing page.	City Power hit by ransomware attack. Suspects arrested for hacking City of Tshwane, R53m pillaged.	Garmin SA hacked, exposing users' credit card details. Adapt IT unit Conor hit by massive data breach.	SA aviation authority still to pinpoint attack source. City of Joburg hit by cyber attack.	Bad day for SA's cyber security as banks suffer DDoS attacks. Liquid Telecom, Webafrica hit by DDoS attacks. Massive DDoS attacks – South African Internet providers crippled.
2020	South African online stores targeted by hackers. ANC Youth League website hacked. SABC confirms that its website was hacked.	Tracker hack hints at more ransomware attacks in SA. NCape municipality battles devastating ransomware attack.	Momentum Metropolitan hacked. Experian hacked, 24m personal details of South Africans exposed. Lombard Insurance engages SA authorities after data breach. The main people behind Mirror Trading International. Ransomware group claims hack on Office of the Chief Justice. South Africa's communications minister WhatsApp account 'hacked'. Absa hit by data breach. Ransomware group releases data after attack on Office of the Chief Justice. Data leak on UIF COVID-19 relief scheme website.	1.7m Nedbank clients exposed after service provider hack. JSE company Omnia hit by cyber attack. Life Healthcare Group hit by cyber attack amid COVID-19. Postbank to replace 12m bank cards after security breach. Stefanutti Stocks shuts down IT systems after cyber attack.	

The most prevalent incident type across the ten years studied (see Figure 5) was *data exposure* (39.19% of incidents), followed by *compromised website* (21.62%), *system intrusion* (14.86%), *cybercrime* (13.51%), and *denial of service* (10.81%). The finding on the prominence of data exposure aligns with the finding from research conducted by Van Niekerk (2017) on the period 1994 to 2016, which found data exposure to be the most prominent impact caused by cyber incidents in South Africa. Meanwhile, this study's finding that denial of service was the type of cyber incident present in 10.81% of incidents marks a decrease in percentage share compared to the research results reported by Van Niekerk (2017) for the period 1994 to 2016. This decrease in denial of service attacks can potentially be attributed to the increase in other cyber incident types, such as *cybercrime* using ransomware (Trend Micro, 2017). Finally, the findings in this study show a significant increase in system intrusion incidents (14.86%) compared to the research results presented by Van Niekerk (2017) for the period 1994 to 2016, which found system penetration to be the least common impact type. The increase merely demonstrates an increase in cyber incidents affecting organisations that release such information to the general public.

Figure 5: Cyber incidents by type, 2010–2020

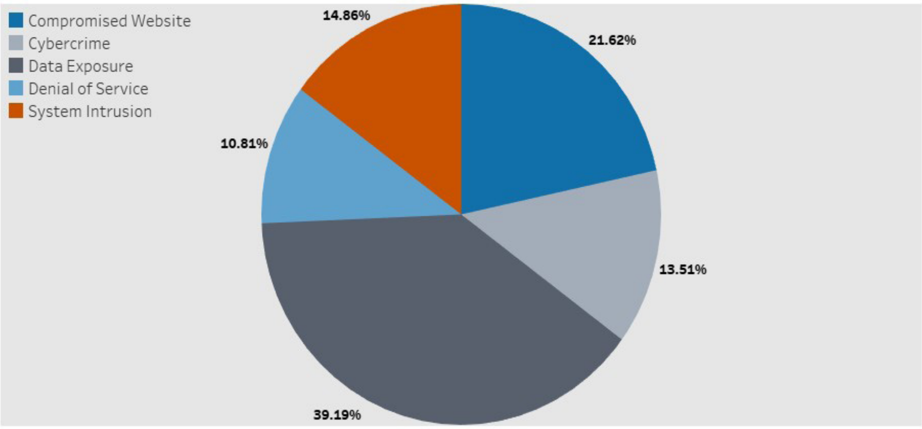
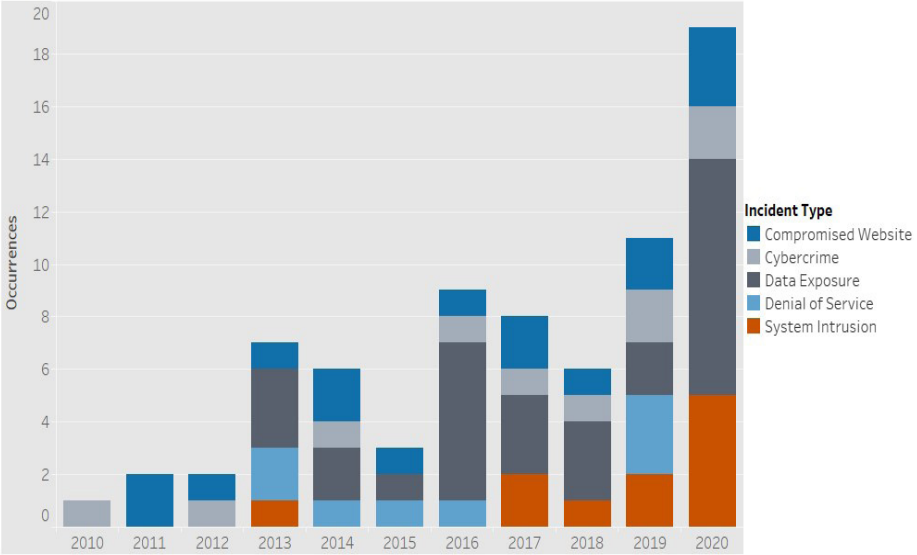


Figure 6 shows the year-by-year trends in incident type identified in this study. The most prominent incident type, *data exposure*, had notable increases in 2016 and 2020. Reporting of such incidents is expected to grow even further with the aforementioned implementation of POPIA, which requires mandatory reporting of data breaches involving personal information (Dullabh & Gabryk, 2021). Less prominent than data exposure incidents but recurring continually between 2011 and 2020 were incidents leading to *compromised websites*. Also illustrated is the small yet notable increase in the annual total of *cybercrime*-related incidents between 2018 and 2019, with 2020 maintaining the relatively high level of such attacks. These findings confirm the increasing move towards *criminally* motivated cyber incidents (see "motivation" sub-section below). Another notable trend illustrated in Figure 6 is the recent rise of cyber incidents of the *system intrusion* type. Identified reports on such incidents confirmed illegitimate access to a system or internal network but restricted the disclosure of information describing the incident's impact (e.g., data leakage, affected services or operations, encryption of data).

Figure 6: Yearly trends in incident types, 2010–2020

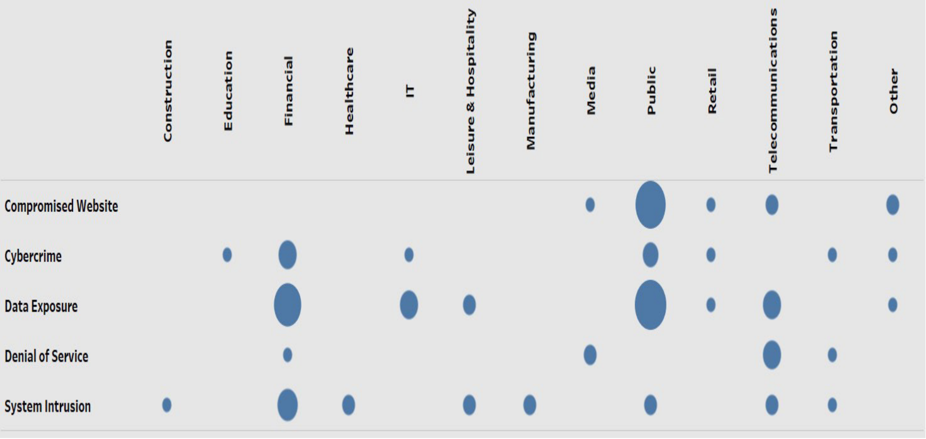


Sector affected

The findings captured in Figure 7 show that the three South African sectors most affected by the past decade's cyber incidents were the *public*, *financial*, and *telecommunications* sectors. The public sector, which consists of state-owned, publicly controlled, or publicly funded entities, often fell victim to cyber incidents causing *compromised websites* or *data exposure*. Notably, the websites of the African National Congress (ANC) and the ANC Youth League (ANCYL) were regularly targeted by hackers, negatively affecting the reputation of the organisations. Other entities in the public sector affected by cyber incidents include, but are not limited to, the Office of the Chief Justice, the Social Security Agency of South Africa (SASSA), the Administrative Adjudication of Road Traffic Offences (AARTO), the Department of Basic Education, Armscor, SAPS, and several municipalities (Nama Khoi, eThekwini, Tshwane, and Johannesburg).

In comparison to the public sector, the financial sector suffered fewer cyber incidents. However, the incidents impacted commercial banks, insurance companies, and financial institutions. While cyber incidents affecting the financial sector are expected to be primarily *economic* in motivation, the past decade witnessed an increase in incidents leaking sensitive information (see "motivation" sub-section below). Although such incidents do not have any financial implications, affected clients can still incur financial loss due to the misuse of such exposed information. The value associated with sensitive information as a commodity on the dark web can be expected to cause a steady rise in cyber incidents targeting the financial sector.

Figure 7: Sector affected per cyber incident type, 2010–2020



Finally, the telecommunications sector of South Africa, which includes mobile operators and internet service providers (ISPs), fell victim to several cyber incidents causing *denial of service*. More specifically, the sector experienced two significant DDoS attacks during 2019. In the first attack, Liquid Telecom and Webafrica suffered a large-scale volumetric DDoS attack from international sources (Moyo, 2019d). Mitigation controls were applied, and traffic volumes returned to normal. A few weeks later, South African ISPs, RSAWEB and Cool Ideas, suffered severe DDoS attacks (Vermeulen, 2019). The co-founder of Cool Ideas confirmed that the attack exceeded 300 Gigabytes per second (Gbps). The telecommunication sector also endured several cyber incidents causing *data exposure*. On closer inspection, the exposure of the data in these cases was accidental and caused by *non-malicious individuals* (see "perpetrator type" sub-section below). Although less affected than the public and financial sectors, entities in the telecommunication sector can expect to continue being targeted by cyber incidents.

Perpetrator type

Figure 8 presents trends associated with perpetrator types. *Hackers* were found to be the most common perpetrator type, responsible for more than 50% of the cyber incidents that occurred in the past decade. While responsible for the largest subset of cyber incidents, hackers became most prevalent only in 2017. More dominant between 2012 and 2018 were *hacktivists*, who were responsible for 11 cyber incidents during the same period.

Figure 8: Trends in perpetrator type, 2010–2020

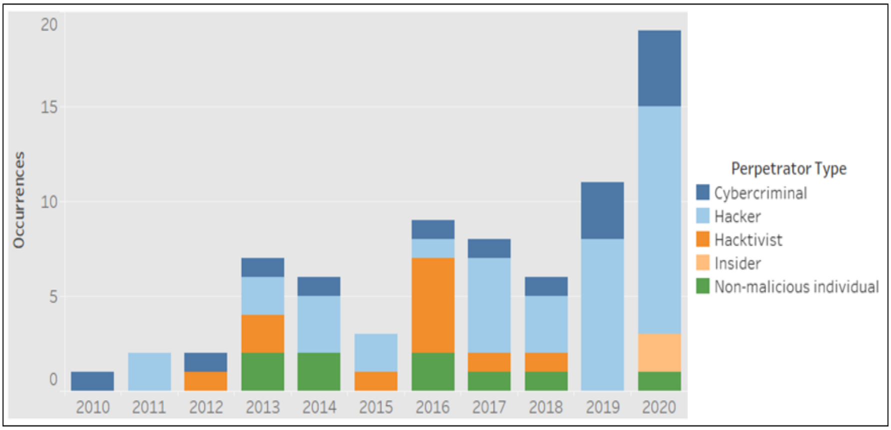
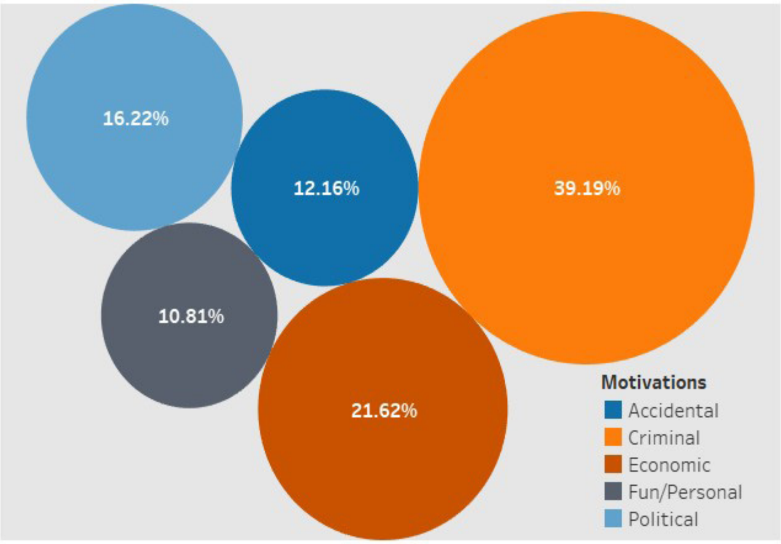


Figure 8 further illustrates the prevalence of incidents caused by *cybercriminals*. The year 2019 witnessed a sharp increase in such incidents, apparently driven partly by the rise of ransomware-related attacks. Another reality seen is the figure is the reappearance in 2020 (after being absent in 2019) of security flaws or misconfigurations generated by *non-malicious individuals*. (In total, nine such incidents were disclosed in the decade reviewed.) Also noteworthy in Figure 8 is the appearance, in 2020 and for the first time in the decade reviewed, of two cyber incidents caused by *insiders*. There were two such incidents in 2020. The first was a security breach at Postbank in which its employees stole the bank's encrypted master key (*ITWeb*, 2020). The master key provides access to Postbank's systems and enables the manipulation of captured information. The second incident was caused by internal data theft that exposed the personal information of Absa banking clients to external parties (McKane, 2020b). Absa notified affected clients and confirmed that all suspicious transactions will be reviewed in order to protect clients' interests.

Motivation

Figure 9 shows that the most common motivation found for cyber incidents in South Africa in the decade reviewed was *criminal* (39.19%). Cyber incidents driven by *economic* intent constituted 21.62% of the recorded incidents, while 16.22% of the incidents were *political* in motivation. The two least common motives, *accidental* (12.6%) and *fun/personal* (10.81%), still, when taken together, represented nearly a quarter of the identified incidents.

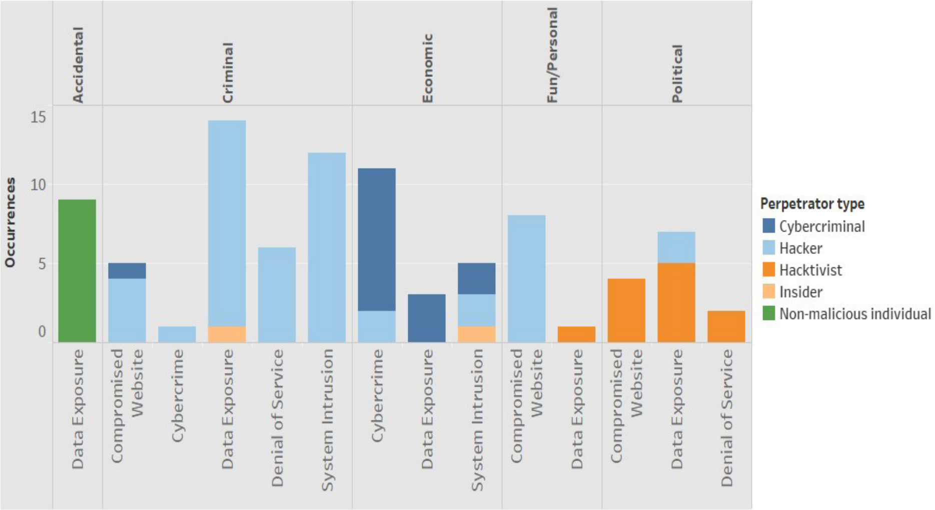
Figure 9: Motives behind cyber incidents, 2010–2020



Relationships between incident type, perpetrator type, and motivation

Figure 10 shows that a strong relationship between perpetrator type and motivation was found between *hackers* and *criminal* motivation. And, when driven by criminal intent, hackers were found to cause cyber incidents primarily leading to *data exposure* or *compromised websites* (17 incidents across these two classifications). A smaller number of hackers were motivated by *fun/personal* intentions, and these hackers were involved in seven cyber incidents causing *compromised websites.*

Figure 10: Relationships between incident type, perpetrator type, and motivation



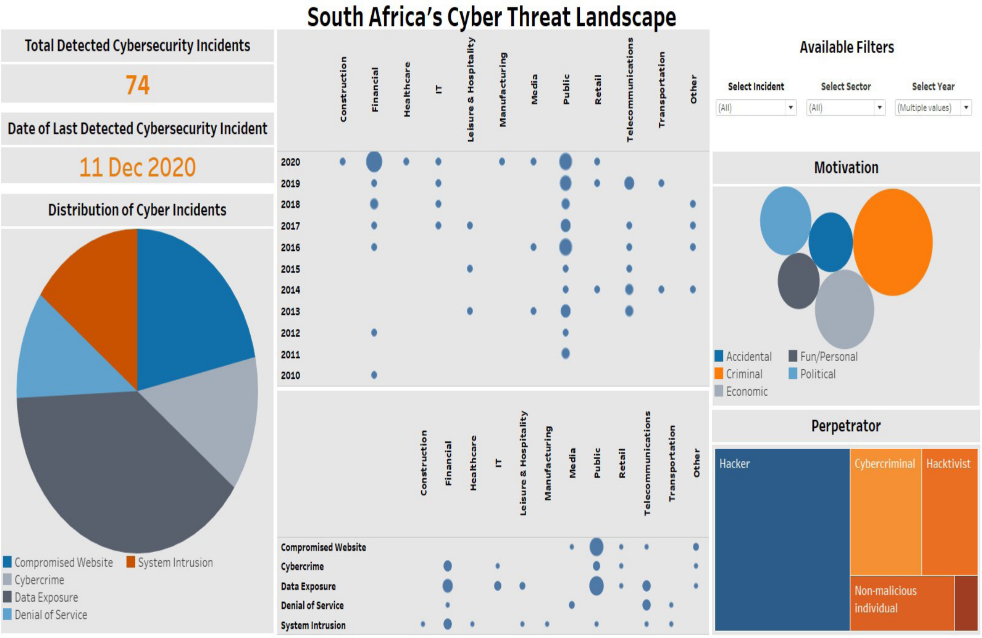
As also seen in Figure 10, *cybercriminals* were, unsurprisingly, found to be primarily driven by *economic* motives (13 incidents) and strongly associated with *cybercrime* incidents (eight incidents). The remaining five cyber incidents caused by cybercriminals, while also driven by economic incentives, resulted in *data exposures* and *system intrusions*. In these five cyber incidents, the cybercriminals either attempted fraud (using acquired or exposed credit card information) or requested ransom in the form of bitcoin (due to ransomware attacks).

Another relationship identified was between *hacktivists* and *politically* motivated cyber incidents. In total, ten cyber incidents occurred that were driven by political incentives. Half of the incidents were caused by hacktivists affiliated with Anonymous, a decentralised international activist/hacktivist movement driven by political agendas (Mikhaylova, 2014), and the remaining incidents were claimed by the hacktivist groups H4ksniper, Team Hack Argentino, World Hacker Team, Team System DZ, and Black Team. A final relationship detected in the data was between *data exposure* due to the accidental misconfiguration or disclosure by benevolent individuals (nine incidents).

A threat landscape dashboard

Figure 11 summarises the findings of this study in the form of a dashboard constructed to enable a bird's eye view of South Africa's cyber threat landscape.

Figure 11: Dashboard visualisation of South Africa's cyber threat landscape



4. Discussion

South Africa's perilous cyber threat landscape

In response to the increase in cyber incidents in South Africa, iDefense, an Accenture security intelligence company, investigated notable cyber incidents and trends during 2019. iDefense found that several factors were contributing to South Africa's increasingly perilous cyber threat landscape (Mcanyana et al., 2020). Based on the findings captured in the iDefense report and the findings from this study, it can be concluded that the following elements are negatively impacting South Africa's cybersecurity and increasing its attack surface:

Lack of investment in cybersecurity

South Africa, as a country with a developing economy, continually faces insurmountable challenges. Investment in cybersecurity practitioners is not always possible, and this influences South Africa's ability to prevent and defend itself against cyberattacks. The analysis performed confirmed that the public sector is a prime target for cyberattacks, emphasising the need for more investment in cybersecurity in this sector.

Slow development of cybercrime legislation

In general, South Africa has been slow to adopt cybercrime legislation. However, in 2021, PoPIA came into full effect and the Cybercrimes Bill was also signed into law (Act 19 of 2020) (Bhagattjee, Govuza, & Westcott, 2021). Both PoPIA and the Cybercrimes Act should influence the ability to conduct illegal operations. For example, disclosure of data breaches, as required by PoPIA, will offer more insight into the tactics deployed by such cyberattacks, which can guide the deployment of defensive measures in the future. Such insights are of great importance due to the considerable increases in cyberattacks causing data leakage in recent years.

Lack of awareness of cyber threats

As the use of technological solutions rises, more South African citizens are exposed to cyber threats—confirmed by the increase in cyber incidents witnessed in the past decade. Such an increase in cyber incidents, especially incidents causing accidental data exposure or compromised websites, shows that South Africans are inexperienced and lack technical alertness when operating in the cyber domain. Such a lack of awareness causes South Africans to be ideal targets for cyber attackers.

Increasing use of IT

Reliance on IT by South Africans increases the cyber threat landscape. Insights drawn from the analysis performed revealed that IT systems within the telecommunication sector fell victim to security flaws on several occasions. Such technologies, applications, and infrastructure pose a significant risk, especially if used inappropriately (e.g., default configurations or unpatched security weaknesses), with limited knowledge, or without the necessary approval (e.g., legacy systems).

Cyber attackers taking notice

The continual exposure of South Africa's vulnerable cyber threat landscape will undoubtedly grab the attention of other, more advanced cyber attackers. Based on the growth shown in Figure 4, cyber incidents affecting South Africa are expected to increase. While previous cyber attackers primarily targeted the public sector, attackers are widening their attack plane to other sectors such as construction, manufacturing, and healthcare. South Africa's cyber threat landscape is, therefore, expected to remain diverse and complex.

Reducing risks in the cyber threat landscape

The factors outlined above show that South Africa is currently positioned, in many respects, as an ideal target for cyberattacks. Nevertheless, some steps can be taken to reduce the number of risk factors present in South Africa's cyber threat landscape and thus reduce the attack surface:

Adopt a defence-in-depth approach

A military strategy often used in information security, defence in depth, offers a multi-layered security approach. The approach relies on the use of various security controls strategically placed throughout an IT system. The multiple security controls offer redundancy, in case a single security control fails, or a vulnerability is exploited. Redundancy is achieved by incorporating physical (e.g., locks and security guards), technical (e.g., firewalls and intrusion detection systems), and administrative (e.g., policies and procedures) controls.

Promote a security-focused cyber culture

Regular training, education, and user awareness sessions are necessary to promote a security-focused cyber culture. Not all employees are cyber-savvy and might be unaware of the potential risks associated with their online behaviour in the cyber domain. It is, therefore, important to teach employees best practices about cybersecurity, as well as the procedures to follow should an attack occur.

Utilise threat intelligence

Originally only available to well-funded organisations, threat intelligence has become more accessible due to open-source feeds. However, the providers of threat intelligence have little to no presence in South Africa. Insights derived from the threat intelligence are heavily slanted towards developed countries and might not be relevant to the South African context. The Council for Scientific and Industrial Research (CSIR) is developing a technological solution that aims to function as the primary source for cybersecurity data collection in South Africa (Burke et al., 2021). The threat intelligence derived from the collected cybersecurity data sets will have a strictly South African focus, offering a valuable source of information to better understand threats and anticipate attacks.

Focus on compliance

The first step to ensure protection against cyberattacks is to apply recommended standards and best practices (e.g., the NIST Cybersecurity Framework or ISO/IEC 27001). Furthermore, the development of an appropriate cybersecurity policy, which outlines detailed plans, rules, and practices regulating access to an organisation's system and information source, is imperative. Finally, an incident response plan must be put in place to ensure employees can respond appropriately should an incident occur.

Collaborate and report

South Africa's economic challenges can cause cybersecurity to receive less attention than required. For example, the public sector—affected by 36% of the cyber incidents identified by this study in the period 2010–2020—requires improved cyber defences but lacks financial stability. Collaboration, often described as the future of cybersecurity, offers a cost-effective means to share cyber threat information, improve preparedness, and overcome cybersecurity skill shortages. The national CSIRT is ideally situated to drive collaboration concerning cybersecurity within South Africa.

Reporting functions can include maintenance of a publicly available cyber threat dashboard of the kind provided above in section 3. This kind of visualisation of cyber incidents offers an overview of South Africa's cyber threat landscape and enables trend analysis. Such consolidated information can be used to extract intelligence to better prepare and defend against potential cyberattacks. It is recommended that a dashboard of this sort be established, published via appropriate platforms (e.g., the national CSIRT), and regularly updated, to enable all stakeholders in South Africa to have insight into the country's existing cyber threat landscape.

Be prepared for when, not if

For South African organisations, it is not a question of *if* a cyberattack will occur, but rather a question of *when*. Organisations must ensure that the required people, processes, and technologies are in place to identify, protect, detect, respond to, and recover from cyberattacks.

5. Conclusion

The purpose of this study was to investigate South Africa's current cyber threat landscape by reviewing noteworthy cyber incidents that have occurred in the past decade. In total, 74 cyber incidents were analysed. As the reliance on IT infrastructure and internet connectivity increases, South Africa's potential exposure to cyber threats will also continue to rise. As shown by this study, the most common type of cyber incident affecting South African organisations in the past decade was found to be incidents causing *data exposure*. The most frequent perpetrators were found to be a *criminally* motivated *hackers*. And the sector most often targeted was the public sector (27 known incidents between 2010 and 2020).

The prevalence of cyber incidents can be expected to continue in the coming years. South African organisations need to be cognisant of cyber threats and prepare financially viable defences. However, the inadequate reporting of cyber incidents is creating a void that limits our understanding of South Africa's cyber threat landscape. Improved collaboration with regard to the collection, analysis, and reporting of cyber incidents, guided by appropriate authorities such as the National CSIRT, is required.

The insights produced by this study, as summarised in the proposed dashboard, offer a starting point for collaborative efforts that can enable South African organisations to be better prepared and better defended against forthcoming cyberattacks.

References

Bhagattjee, P., Govuza, A., & Westcott, R. (2021, June 9). Regulating the Fourth Industrial Revolution - South Africa's Cybercrimes Bill is signed into law. Cliffe Dekker Hofmeyr.

Bing, C., & Kelly, S. (2021, May 8). Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. *Reuters*. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Brush, K. (n.d.). Cybercrime. TechTarget. https://searchsecurity.techtarget.com/definition/cybercrime

Burke, I., Motlhabi, M., Netshiya, R., & Pieterse, H. (2021). Lost packet warehousing service. In *Proceedings of the 16th International Conference on Cyber Warfare and Security* (pp. 501–508). ACI.

BusinessTech. (2014, October 30). Vodacom exposing subscriber details. https://businesstech.co.za/news/mobile/72054/vodacom-exposing-subscriber-details/

BusinessTech. (2016, February 16). Hackers leak SA government's sensitive financial data. https://businesstech.co.za/news/government/112817/hackers-leak-sa-governments-sensitive-financial-data/

Duffy, C. (2021, March 10). Here's what we know so far about the massive Microsoft Exchange hack. *CNN*. https://edition.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html

Dullabh, R., & Gabryk, N. (2021, April 13). *South Africa: Preparing for POPIA: Data breach response*. *Mondaq*. https://www.mondaq.com/southafrica/data-protection/1055314/preparing-for-popia-data-breach-response

Eaton, C., & Volz, D. (2021, May 19). Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom. *Wall Street Journal*. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

Gandhi, R. A., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. A. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. https://doi.org/10.1109/MTS.2011.940293

Goldstuck, A. (2021, August 1). Transnet cyber hack a warning of risk to SA. *BusinessLive*. https://www.businesslive.co.za/bt/business-and-economy/2021-08-01-transnet-cyber-hack-a-warning-of-risk-to-sa/

ITWeb. (2020, June 14). Postbank to replace 12m bank cards after security breach. https://www.itweb.co.za/content/nWJadvbekrmqbjO1

Kakareka, A. (2014). Detecting system intrusions. In J. R. Vacca (Ed.), *Network and system security* (2nd ed.) (pp. 1–27). Syngress. https://doi.org/10.1016/B978-0-12-416689-9.00001-0

Kumar, R., Raj, P., & Perianayagam, J. (2019). A framework to detect compromised websites using link structure anomalies. In S. Omar, S. W. Haji, & S. Phon-Amnuaisuk (Eds.), *Advances in intelligent systems and computing: Proceedings of the Computational Intelligence in Information Systems conference (CIIS 2018)* (pp. 72–84). Springer. https://doi.org/10.1007/978-3-030-03302-6_7

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *Insight into the cyberthreat landscape in South Africa.* Accenture.

McKane, J. (2020a, November 10). ANC Youth League website hacked. *MyBroadband*. https://mybroadband.co.za/news/government/374940-anc-youth-league-website-hacked.html

McKane, J. (2020b, November 30). Absa hit by data breach. *MyBroadband*. https://mybroadband.co.za/news/security/378358-absa-hit-by-data-breach.html

Mikhaylova, G. (2014). *The "Anonymous" movement: Hacktivism as an emerging form of political participation.* Texas State University, San Marcos.

Moyo, A. (2017, June 29). DBE web site hacked, pro-Islamic State messages posted. *ITWeb*. https://www.itweb.co.za/content/x4r1lyMRgpjqpmda

Moyo, A. (2019a, October 25). City of Joburg hit by cyber attack. *ITWeb.* https://www.itweb.co.za/content/dgp45qaG8gZ7X9l8

Moyo, A. (2019b, October 25). Bad day for SA's cyber security as banks suffer DDoS attacks. *ITWeb*. https://www.itweb.co.za/content/LPp6V7r4OVzqDKQz

Moyo, A. (2019c, September 13). Garmin SA hacked, exposing users' credit card details. *ITWeb*. https://www.itweb.co.za/content/O2rQGMApY5G7d1ea

Moyo, A. (2019d, October 28). Liquid Telecom, Webafrica hit by DDoS attacks. *ITWeb.* https://www.itweb.co.za/content/GxwQDM1A339MlPVo

Moyo, A. (2020a, August 19). Experian hacked, 24m personal details of South Africans exposed. *ITWeb*. https://www.itweb.co.za/content/rxP3jqBmNzpMA2ye

Moyo, A. (2020b, February 5). Tracker hack hints at more ransomware attacks in SA. *ITWeb*. https://www.itweb.co.za/content/LPp6VMr4YxNvDKQz

Moyo, A. (2021, July 22). Transnet suffers "disruption" of IT systems. *ITWeb*. https://www.itweb.co.za/content/wbrpOqgYAwY7DLZn

Muller, R. (2013, December 30). My Vodacom security flaw exposes subscriber details. *MyBroadband*. https://mybroadband.co.za/news/security/94234-my-vodacom-security-flaw-exposes-subscriber-details.html

Mungadze, S. (2020, June 9). Life Healthcare Group hit by cyber attack amid COVID-19. *ITWeb.* https://www.itweb.co.za/content/JBwErvnBK4av6Db2

MyBroadband. (2012, December 9). South African websites hacked. https://mybroadband.co.za/news/security/66474-south-african-websites-hacked.html

MyBroadband. (2014, September 21). Mass hacking of South African websites. https://mybroadband.co.za/news/security/110316-mass-hacking-of-south-african-websites.html

MyBroadband. (2016, May 30). MTN exposing subscribers' personal details online. https://mybroadband.co.za/news/cellular/166734-mtn-exposing-subscribers-personal-details-online.html

MyBroadband. (2017, May 21). Telkom systems crippled by WannaCry ransomware. https://mybroadband.co.za/news/security/211576-telkom-systems-crippled-by-wannacry-ransomware.html

MyBroadband. (2018, July 7). South African presidency website hacked. https://mybroadband.co.za/news/security/267491-south-african-presidency-website-hacked.html

Mzekandaba, S. (2019, July 23). SASSA web site remains down after hack. *ITWeb*. https://www.itweb.co.za/content/rxP3jqBpVJ27A2ye

Ngqakamba, S. (2021, September 9). Justice department's IT system brought down in ransomware attack. *News24*. https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909

Rawlins, L. K. (2017, June 28). Hackers again prove their global power. *ITWeb*. https://www.itweb.co.za/content/nLPp6VMrdbzvDKQz

Republic of South Africa (RSA). (2013). Protection of Personal Information Act (POPIA) 4 of 2013.

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176.

Slabbert, A., & Peyper, L. (2021, August 1). Transnet attack is cyber warfare. *City Press*. https://www.news24.com/citypress/business/transnet-attack-is-cyber-warfare-20210801

Trautman, L. J., & Ormerod, P. (2019). Wannacry, ransomware, and the emerging threat to corporations. *Tennessee Law Review*, *86*(503), 504–556. https://doi.org/10.2139/ssrn.3238293

Trend Micro. (2017). *Ransomware: Past, present, and future*. https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

Van Heerden, R. P., Irwin, B., Burke, I. D., & Leenen, L. (2012). A computer network attack taxonomy and ontology. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *2*(3), 12–25. https://doi.org/10.4018/ijcwt.2012070102

Van Heerden, R. P., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. In IEEE (Ed.), *2016 IST-Africa Week Conference* (pp. 1–16). https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Vermeulen, J. (2016, February 12). Massive number of South African websites hacked by Anonymous. *MyBroadband*. https://mybroadband.co.za/news/security/155040-massive-number-of-south-african-websites-hacked-by-anonymous.html

Vermeulen, J. (2019, November 25). Massive DDoS attacks – South African internet providers crippled. *MyBroadband*. https://mybroadband.co.za/news/internet/329539-massive-ddos-attacks-south-african-internet-providers-crippled.html

Vermeulen, J. (2020a, May 27). Data leak on UIF COVID-19 relief scheme website. *MyBroadband*. https://mybroadband.co.za/news/cloud-hosting/353473-data-leak-on-uif-covid-19-relief-scheme-website.html

Vermeulen, J. (2020b, October 1). Ransomware group claims hack on Office of the Chief Justice. *MyBroadband*. https://mybroadband.co.za/news/security/369503-ransomware-group-claims-hack-on-office-of-the-chief-justice.html

Vermeulen, J. (2020c, November 7). Ransomware group releases data after attack on Office of the Chief Justice. *MyBroadband*. https://mybroadband.co.za/news/security/374310-ransomware-group-releases-data-after-attack-on-office-of-the-chief-justice.html

Willett, M. (2021). Lessons of the SolarWinds hack. *Survival*, *63*(2), 7–26. https://doi.org/10.1080/00396338.2021.1906001

Wyatt, M. (2021, March 16). Responding to the Microsoft Exchange Hack. Wall Street Journal Pro Cybersecurity Research.