An Analysis of Cyber-Incidents in South Africa

Brett van Niekerk
Honorary Research Fellow, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Abstract
Cybersecurity concerns are present in all nations, but the exact nature of the threats differs depending on the country and/or region. Therefore there is a need to assess the threats and impacts for specific countries. This article presents a high-level analysis of "newsworthy" cyber-incidents that affected South Africa. The 54 incidents that are considered are categorised according to impact type, perpetrator type, and victim type, and the trends are assessed. It was found that the most common impact type was data exposure, which was also one that had increased noticeably in recent years. The most prevalent perpetrator type was found to be hacktivists, which had also exhibited a recent increase in activity. A particularly concerning trend was the recent high number of incidents of data exposure caused by error, a trend running contrary to the drive to improve cybersecurity. It was also found that of the incidents considered, 54% targeted state-owned or political entities as victims. In general, the results appeared consistent with global reported trends.

Keywords
advanced persistent threat, data breach, defacement, distributed denial of service, financial theft, system penetration

DOI: https://doi.org/10.23962/10539/23573

Recommended citation
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

1. Introduction

Concerns over cybersecurity are growing globally, fuelled by reports of ever-larger data breaches and a lack of skilled cyber-security professionals (Fearn, 2017). However, most organisations and nations seem to be at a loss of how to effectively respond. For instance, even though UK organisations have been found to generally consider cyber-security important, only 44% have implemented a cyber-security strategy (Ashford, 2017). Slay, quoted in Tate (2017), indicates that Australia has a lack of experienced cyber-security professionals. Reports from Kenya indicate that cyber-security is lagging, despite increased uptake of Internet services (Matinde, 2017). Similarly, reports in South Africa suggest that cyber-security is "reaching a critical point" in the country (*SABC News*, 2017).

Whilst the concerns of security are common across all regions, the exact nature of the threat types and motivations vary geographically as illustrated in Brown and Rudis (2017). Therefore it is necessary to assess the relevant trends in one's region to ensure the security measures and strategies are aligned to the threat activity. This article presents a high-level analysis of "newsworthy" cyber-incidents that targeted South Africa. The next section scans relevant literature, followed by a description of the methodology used. Summaries of the incidents are provided, after which the analysis is presented. The results are discussed with reference to the literature, and the article is then concluded.

2. Literature

There are different types of cyber-attacks, and some receive more hype than others. Receiving significant attention are instances of nation-state cyber-espionage, which are closely linked to advanced persistent threats (APTs). These have been found to be constantly present in the global cyber-threat environment, but the number of organisations affected by these is low unless they are in the specific target group for the attackers (Brown & Rudis, 2017). Ransomware is another threat operated by cyber-criminals that is receiving much attention. The number of ransomware payloads increased internationally from 18% of detections in January 2016 to 66% in November 2016. Only 1% of ransomware detections occur in Africa meaning that all the other populated continents, however, are much more heavily affected (Malwarebytes Labs, 2017).

In addition to the state-sponsored persistent attacks and criminal ransomware attacks mentioned above, the major threat types include: insider threats, either malicious or accidental, resulting in security incidents; attacks by hacktivists who are politically or ideologically motivated; and attacks by individual hackers who are trying to learn or show off, such as the "script kiddies" who make use of existing tools (Andress & Winterfield, 2014).

It has been reported that South Africa lost approximately ZAR50 billion in 2014 due to cyber-incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (*SABC News*, 2017). Estimates in 2011 put the financial losses from cyber-attacks at ZAR 3.7 billion in direct losses and ZAR6.5 billion in indirect costs (Norton South Africa, 2012). The threat will become more widespread going forward as the number of South African Internet users increases, aided by the African continent's increasing undersea capacity (Song, 2017).

The South African legislative context relating to online privacy and security is expanding. The foundational act from which the other acts derive is the Electronic Communications and Transactions Act (ECT) of 2002 (RSA, 2002). The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) was also promulgated in 2002 (RSA, 2002). The Protection of Personal Information (POPI) Bill was released in 2009, and enacted in 2013 (RSA, 2009; RSA, 2013), but has yet to come into full effect. The National Cybersecurity Policy Framework was released at the end of 2015 (SSA, 2015), followed by drafts of the Cybercrimes and Cybersecurity Bill (Department of Justice and Correctional Services, 2017).

Patrick (2015) has illustrated a lack of information flow regarding cyber-security in government departments, and the need for response teams. Chandarman (2016) has found that South African students sometimes over-estimate their knowledge regarding security threats and techniques, possibly putting them at risk. Dlamini and Modise (2012) interrogated awareness initiatives in the country up to 2012 and found that the focus of the initiatives appeared to be on tertiary institutions and schools. It thus seems clear that the cyber-security landscape in South Africa has room to improve.

3. Methodology

The research for this article analysed a number of documented cyber-incidents related to South Africa. The data were identified through scrutiny of published reports, news items, postings to email mailing lists, cross-referencing via document reference lists, and targeted online searches for additional information on documented incidents. A total of 54 incidents spanning 23 years, from April 1994 to end-2016, were identified. These were classified in a manner similar to that used in the work of Miller and Rowe (2012) and Van Niekerk (2017). Miller and Rowe (2012) analysed security incidents related to industrial control systems (ICS), categorising them by impact type and attack vector. In Van Niekerk (2017), security incidents affecting the transportation sector were considered, categorised by threat type and impact.

Impact categories

For this study, the impacts were categorised as follows:

- data exposure, where records have been released;
- financial, where there was an attempt (successful or otherwise) to steal money;
- denial of service, where operations or services were affected;
- defacement, where webpages were altered;
- data corruption, where data was modified; and
- system penetration, where illegitimate access to networks or systems was achieved, but no other activity was apparent.

Perpetrator categories

The categorisation of the perpetrators (or key perpetuating factors) was as follows:

- hacktivist, where the perpetrator was affiliated to online activist groups making political statements;
- criminal, where the perpetrator was affiliated to criminal groups usually seeking financial gain;
- accidental/misconfiguration, where the incident was as a result of misconfigured systems;
- individual hacker, where the incident appeared to be to prove or develop individual skills;
- nation-state espionage, where the incident relates to state-sponsored threats;
- malware, where malware was discovered but no perpetrator or motivation can be established; and
- insider, where the perpetrator had legitimate access but acted maliciously for personal gain or reasons.

The incidents were analysed according to perpetrators and impacts, in terms of overall prevalence and trends over time. A pivot table is used to determine the prevalent threat-impact pairs.

Victim categories

In order to determine if there is a noticeable relationship between the threat types and impacts associated with public organisations, the victims were categorised as:

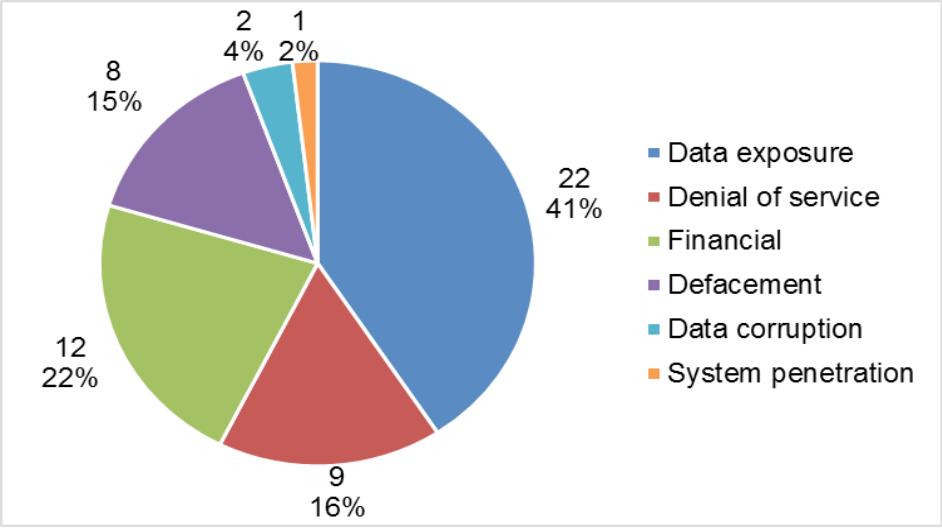
- state/political organisations; or
- other.

4. Findings and analysis

Impact type

Figure 1 below shows the percentage distribution of the 54 incidents across the six impact types. As is evident, data exposure is the most prominent impact type. Financial, denial of service. and defacement are also noticeable.

Figure 1: Impact type



The findings are detailed according to their impact categories, moving from the most common impact category (data exposure) to the two least-common categories (data corruption, system penetration).

Data exposure

Data exposure was found to be the most common impact category. In 2008, the whistleblower site Wikileaks posted an unredacted version of a Competition Commission report about possible unethical practices by South African banks after removing the redaction (HomeGrownHoney, 2009). In 2010, a state hospital in the Western Cape was found to have an insecure site, and thousands of patient records could be accessed (Stone, 2010).

Advanced persistent threat (APTs) infections were also documented. An organisation in South Africa fell victim to the APT1 espionage group attributed to Chinese hackers, with the first major report occurring in 2010 (Mandiant, 2013). In 2012 the

Red October cyber-espionage campaign (attributed to Russian hackers) was detected, after having possibly operating for five years undetected, with various targets in a number of countries affected, including infecting a diplomatic organisation in South Africa (Limer, 2013; Paganini, 2013).

Servers hosting the espionage tool FinFisher, usually employed by governments to track dissent, were detected in South Africa in 2013. The South African government denied using this tool (Vermeulen, 2013). Also in 2013, the Sednit/APT28 cyber-espionage campaign, attributed to Russian hackers, targeted South African embassies via an infected document sent to the embassies purporting to be from the Department of International Relations and Cooperation (ESET, 2016; FireEye, 2014).

The South African Police Service suffered a hack in 2013 that resulted in the release of approximately 16,000 details of whistleblowers and victims. The attack appeared to be by the group Anonymous in response to the police killings of striking mineworkers at the Marikana mine (Roane, 2013; Tubbs, 2013). Also in 2013, a fast-food outlet's point-of-sale system was infected with the Dexter malware designed to steal customers' credit card information (*MyBroadband*, 2013b). (Though this breach resulted in financial loss to the banks, the attack listed here only compromised the credit card information, and will therefore was classed as data exposure.)

Accidental data exposure incidents also occurred in 2013. A flaw in mobile operator Vodacom's portal allowed any subscriber to access high level account summary information linked to any phone number (Muller, 2013). The City of Johannesburg's invoicing portal was found to have vulnerabilities that could expose personal information, and the website was taken offline by the City – but then appeared to be operational a few days later with the vulnerability still present (*MyBroadband*, 2013a).

The year 2014 also saw both accidental and malicious data exposures. A flaw was discovered in mobile operator Cell C's portal, allowing access to a number of customer records (*MyBroadband*, 2014). Altech Autopage suffered an accidental release of records (Patrick, 2015; Safenet, 2014). The South African National Roads Agency Limited (Sanral) E-Toll website was hacked, making the site vulnerable to release of personal details (Vermeulen, 2014). WooThemes was compromised, giving hackers access to financial information (Patrick, 2015; Safenet, 2014).

In 2016, Anonymous launched #OpAfrica, and its first South African target was an online job portal, V-Report, compromising 33,000 records (Vermeulen, 2016a). The state's Government Communication and Information System (GCIS) was compromised shortly after V-Report, exposing the data of 1,500 government employees (Fripp, 2016; Vermeulen, 2016a). A number of web pages hosted by an

unnamed service provider were the next target for #OpAfrica, with 2,500 websites claimed to have been compromised (Fripp, 2016). Hackers affiliated with #OpAfrica compromised the state-owned arms procurement agency Armscor's invoicing portal, releasing a number of purchasing information records (Van Zyl, 2016c). Cinema chain Ster Kinekor was hacked, with a release of approximately 6 million records in 2016 (Cave, 2017). The Chinese-linked group known as APT10 were involved in the Cloud Hopper espionage campaign in late 2016, or which there were South African victims (PwC and BAE Systems, 2017). As the majority of infections were late 2016, it is assumed this is the compromise date for the South African victims.

Accidental exposure again featured in 2016. The eThekwini Municipality (Durban) e-services portal was found to release customer information when the URL was edited, and the website was taken down to correct the error (Venktess, 2016). The e-billing portal of mobile operator MTN was found to be providing users with access to bills of other customers, and the website was taken offline to correct the error (*MyBroadband*, 2016).

Financial

The first instance of financial impact identified in the documents occurred in 2003, when Absa bank lost approximately ZAR500,000 due to a hack (Thiel, 2004). Hackers targeted three South African banks in 2006, managing to transfer cash from bank accounts into prepaid accounts held with mobile operators. It appeared that information gained from key loggers (devices or software to record a user's keystrokes) and phishing were used to conduct the hacks (Oiaga, 2006).

In July 2009, a criminal group acquired, via threats to an engineer at Vodacom, duplicate SIM cards that allowed for interception of online banking one-time PIN codes (OTPs) for bank accounts they had compromised via phishing. The group managed to steal in excess of ZAR7 million from the compromised accounts (Dingle, 2009; Van Rooyen, 2009). The Land Bank initially lost ZAR8 million stolen through fraudulent transfers in December 2010 after hackers compromised the bank's IT security possibly with inside help, but managed to recover most of money (Potgieter, 2011).

A credit card payment provider, PayGate, was compromised in August 2012, affecting four of the major banks and compromising "hundreds of thousands" of credit card details (Arde, 2012, p. 18). Though no details of financial losses were released, it is assumed that the banks suffered financial losses (Ajam, 2012; Arde, 2012). Compromised passwords resulted in the National Department of Water Affairs losing ZAR2.84 million in 2011 (Patrick, 2015; Rasool, 2012). Postbank, the South African Post Office's financial institution, had ZAR42 million stolen in January 2012 after hackers accessed servers via an employee's workstation (Patrick,

2015; Rasool, 2012; Swart & Afrika, 2012). In 2013, over ZAR15 million was lost by the Department of Minerals and Energy after login credentials were stolen by criminals using a keystroke logging device (Patrick, 2015; Tengimfene, 2013).

In 2014, state-owned electricity provider Eskom's payroll system was hacked by employees, but the employees were prevented from making transfers by Eskom's anti-corruption units (Patrick, 2015; Speckman, 2015). In the same year, the Gautrain Management Agency's bank account nearly lost ZAR800 million to a hack (Patrick, 2015; Speckman, 2015). In 2015, the Road Traffic Management Corporation lost ZAR8.5 million to a series of illegal transfer by hackers (Mkhwanazi, 2015; Patrick, 2015). In 2016, Standard Bank was targeted by hackers, who managed to steal approximately ZAR300,000 via thousands of ATMs in Japan (Van Zyl, 2016b).

Denial of service

A South African petrochemical company's supervisory, control and data acquisition system was infected by the PE Sality virus in 2009, denying the operator's visibility of operations for eight hours until the infected servers were recovered (Cusimano, 2010; Pretorius, 2016). The aforementioned Sanral E-Toll website came under a denial-of-service attack in 2012, but the attack was not successful (*SANews*, 2012). It is assumed this attacker was conducted by hacktivists, given the ongoing controversy over the e-toll project.

In 2013, the website of the national ruling party, the African National Congress (ANC), was made inaccessible due to a distributed denial of service (DDoS) attack by Anonymous Africa (different from Anonymous #OpAfrica) (Vermeulen, 2016b). Also in 2013, the Independent Online news website was targeted and access disrupted (Vermeulen, 2016b), and mobile operator MTN and affiliated service providers suffered a service outage due to a DDoS attack (ITNewsAfrica, 2013). MTN again suffered performance degradation in 2015 due to a DDoS attack (TelecomSpeak, 2015).

Anonymous Africa returned in 2016 by targeting the South African Broadcasting Corporation (SABC), whose website was unavailable due to the DDoS attack, with the hackers stating that the attack was in protest against corruption and the recent censoring of protests (Vermeulen, 2016b). Also in 2016, the websites of the news channel ANN7, *The New Age* newspaper, and computing company Sahara were targeted with DDoS attacks, in protest against perceived corruption by their owners and the South African government (Van Zyl, 2016a). A series of denial-of-service attacks was conducted against the Economic Freedom Fighters political party (Gorton, 2016).

Defacement

The websites of five major universities (University of Stellenbosch, Natal University,

Rhodes University and the University of the Witwatersrand and University of Cape Town) were defaced by hackers in 2003. Each website appeared to be attacked by a different hacker, and international hackers were suspected (Porter, 2003). In 2004, 45 company websites in Cape Town and Stellenbosch were defaced by a group known as Spykids, who appeared to be motivated by a desire for recognition (Thiel, 2004). In January 2005, hackers from Morocco, known as Team Evil, defaced approximately 260 South African websites, replacing the legitimate websites with anti-US messages (Mbongwa & Makua, 2005).

In 2008, the Democratic Alliance political party's website was compromised and was offline for over a week; a spokesperson stated that it appeared to be common hacking, implying that is was not a targeted or political attack (*Mail & Guardian*, 2008). The ANC Youth League website was defaced, with a fake message supposedly from the then Youth League president Julius Malema stating he was stepping down (Redelinghuis, 2011).

Three government websites were defaced by Moroccan hackers in 2012, protesting the official South Africa position on Western Sahara (Saville, 2012). The Administrative Adjudication of Road Traffic Offences website was defaced by a Bangladeshi hacker in 2013, who posted a message notifying the website owner to secure the website (*ITWeb,* 2013). Approximately 20 websites, including Sasol, were defaced by a Moroccan hacktivist in 2014, again protesting the South African position on Western Sahara (Ackroyd, 2014).

Data corruption, system penetration

These two categories are the smallest, and are therefore presented together. They also represent the earliest three attacks reported. It is reported that in 1994 a right-wing hacker attempted to disrupt the first democratic elections in South Africa, but was detected after moving votes from the ANC to three right wing parties (Plaut, 2010). Stats SA's website was targeted by hackers in 1999, who replaced data with negative comments about Telkom (*BBC News*, 1999). A teenage hacker managed to penetrate through Telkom (the state telephony operator) in 1998, however no damage was done. The teenager was arrested (Reuters, 1998).

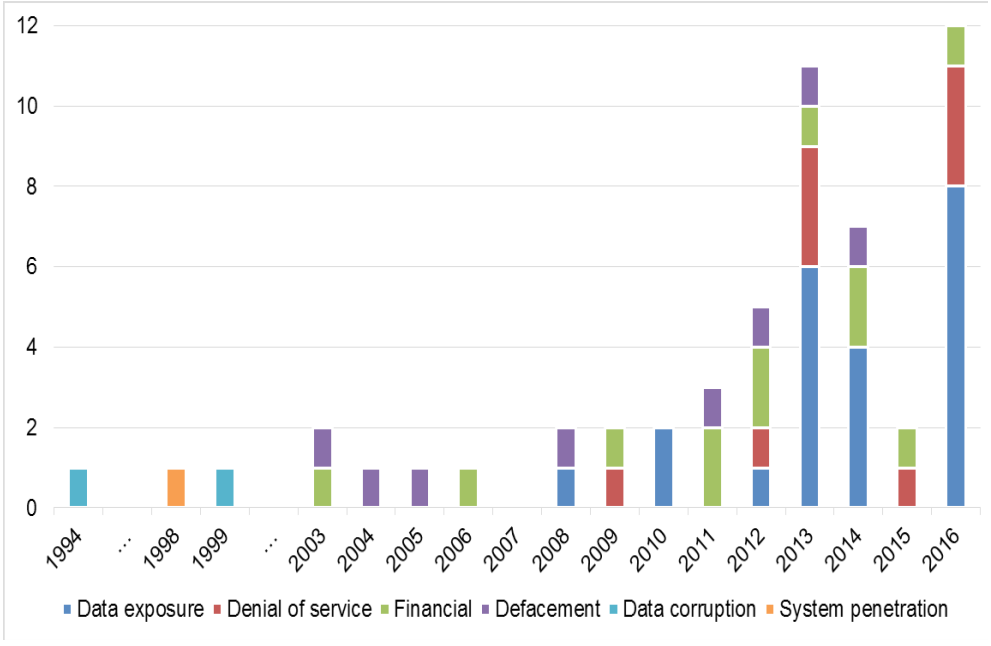
Trends in impact type

Figure 2 below illustrates the trends for each of the six impact types between April 1994 and end-2016. As can be seen, there were significant spikes in data exposure attacks in 2013, 2014 and 2016, and of denial of service attacks in 2013 and 2016. The number of financial-impact attacks, the third-most-common kind, remained largely stable from 2011 to 2016; and defacements, the fourth-most-frequent mode of attack, remained at a consistent level between 2011 and 2014 but were not found to be present in 2015 or 2016.

Thus, the financial-crime motivation for hacking appears to be remaining somewhat constant, whereas the data exposure and denial of service motivations, often indicators of hacktivism and protest – i.e., they commonly used to discredit or exact revenge -- appear to be on the rise in the South African context.

Finally, it is interesting to note that after reaching a total of 11 instances in 2013, there were declines in 2014 (7 instances) and 2015 (2 instances), before a spike to 12 instances in 2016, the largest number recorded for any of the years studied – an apparent indication that cybersecurity measure are still not being effectively applied in South Africa, and/or that attempts at perpetration are becoming increasing complex and skilful.

Figure 2: Trends in impact type



Perpetrator type

Figure 3 presents the percentage distribution of the perpetration types. Hacktivist perpetrators – i.e., perpetrators affiliated to online activist groups making political statements – were found to be the most common, followed by criminals, then individual hackers, and then instances of accidental/misconfiguration due to non-malicious insiders.

Figure 3: Perpetrator type

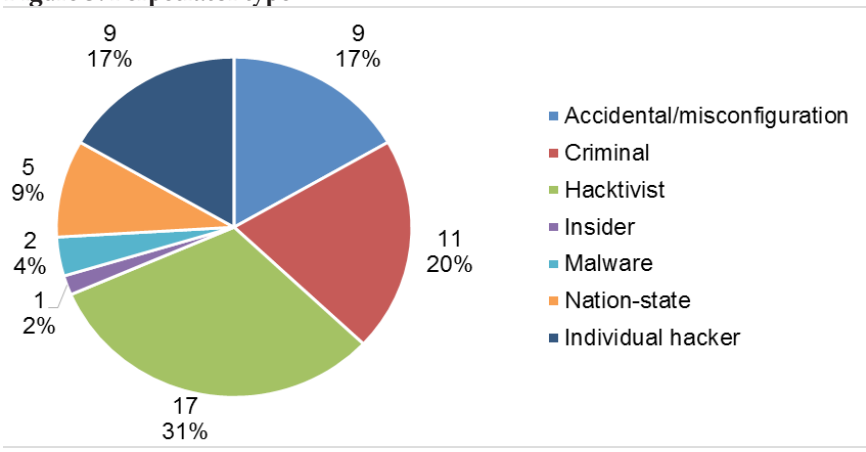


Figure 4 illustrates the trends in perpetrator type. Hacktivist perpetration has been present, off and on, since 1999, with slight increases in 2012 and 2012, and a sharp spike in 2016, indicating a growing protest and revenge dimension in South Africa's cybersecurity risk profile. Another concerning trend is the increasing prevalence of cases of accidental/misconfiguration due to non-malicious insiders, non-existent before 2010 but representing three cases in each of 2014 and 2016. It was found that nation-state cyber-espionage perpetrators have only been active in South African cyberattacks since 2010, whereas individual hackers have had an intermittent presence throughout.

Figure 4: Trends in perpetrator type

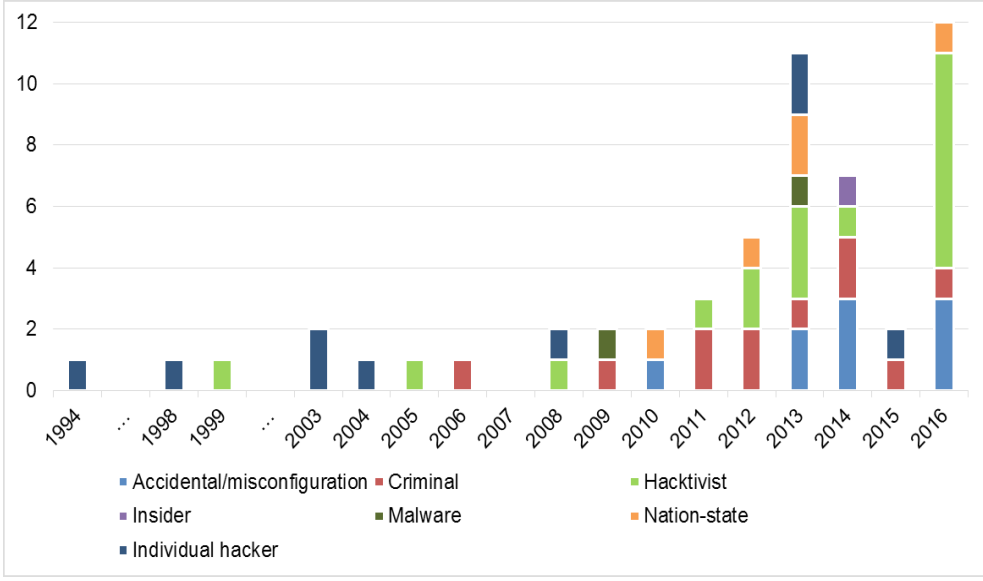


Table 1 is a pivot table associating the perpetrator types to the impact types. The strongest association is between criminal hackers and a financial attacks (10 instances), followed by accidental/misconfiguration due to non-malicious insiders resulting in data exposure (9 instances). These are followed by hacktivists exposing data (6 instances) and hacktivists denying service (6 instances), and then nation-state espionage perpetration seeking to expose (and presumably gain) data.

Whilst the prevalence of criminal activity is almost a given, data exposure due to error (accidental/misconfiguration) is presumably much more easily prevented than criminal activity should be of particular concern to South African institutions.

Table 1: Impacts by perpetrator type

	Impacts						
	Data exposure	Denial of service	Financial	Deface-ment	Data corruption	System penetration	Totals
Accidental/ miscon-figuration	9						**9**
Criminal	1		10				**11**
Hacktivist	6	6		4	1		**17**
Insider			1				**1**
Malware	1	1					**2**
Nation-state espionage	5						**5**
Individual hacker		2	1	4	1	1	**9**
Totals	22	9	12	8	2	1	54

Victim type

Figure 5 presents the distribution of victims in terms of state/political entities and other entities. As can be seen, it was found that attacks targeting the state/political entities represented more than half of the 54 attacks documented.

Figure 5: Victim type

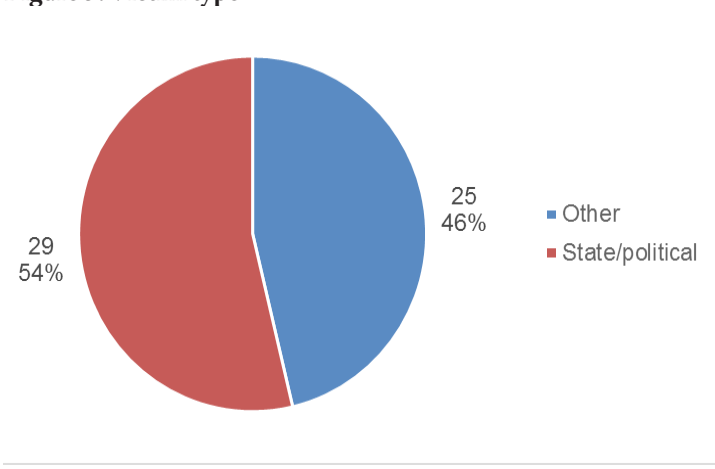


Figure 6 below llustrates the trends over time for the two victim categories. While the first attack on a state/political entity was detected in the first year of study, 1994, the first attack on a non-state/political entity was only documented in 2003. However, in two of the most recent years studied, 2014 and 2016, attacks on non-state/political entities outnumbered state/political breaches.

Figure 6: Trends in victim type

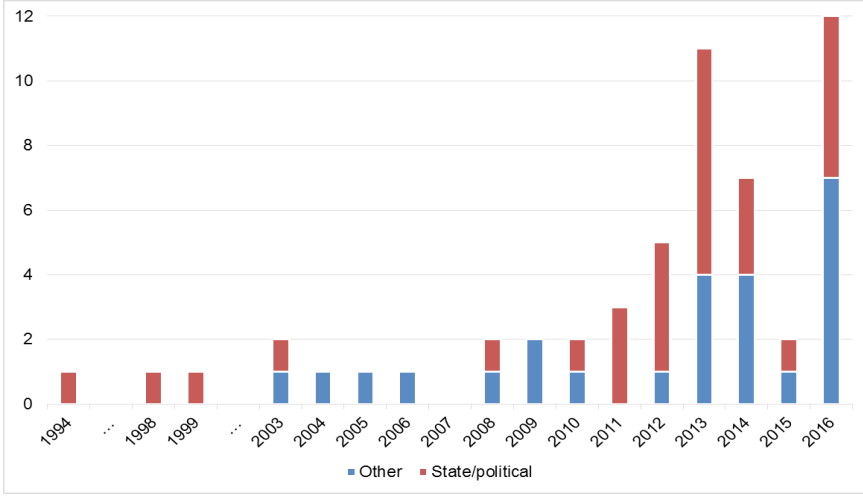


Table 2 below is a pivot table illustrating associations been impacts and victim types. There does not appear to be any significant difference between the distribution of impact types for the two victim types

Table 2: Impacts by victim type

	Impacts						
	Data exposure	Denial of service	Financial	Defacement	Data corruption	System penetration	Totals
Other	12	5	5	3			**25**
State/ political	10	4	7	5	2	1	**29**
Total	22	9	12	8	2	1	54

Table 3 below presents the perpetrator types associated with each of the two victim types. As before, nothing significant can be determined from these figures. The fact that hacktivists and nation-state perpetrators targeted state and political victims more than other organisations is logical. The state or political may have more impact from most perpetrators due to a lack of information security capability at those organisations.

Table 3: Perpetrator by victim type

	Perpetrator							
	Accidental/ misconfiguration	Criminal	Hacktivist	Individual hacker	Insider	Malware	Nation-state espionage	Total
Other	5	5	7	4		2	2	25
State/ political	4	6	10	5	1		3	29
Total	9	11	17	9	1	2	5	54

5. Conclusions

This research has shown that in South Africa, the leading perpetrators of cyber-attacks are hacktivists and criminals. The top two cyber-attack impacts are data exposure and financial theft. The top two perpetration-impact combinations are criminals resulting in financial impact, and accidental/misconfiguration resulting in data exposure.

Given the prevalence of cyber-crime globally, the criminal appearance as a top perpetrator, linked to a top impact, is unsurprising. As Internet connectivity in Africa increases and a greater percentage of the population has Internet access, we can expect the rate of cyber-crime to increase, targeting, among others, new entrants who are not yet fully aware of the security risks. Due the increasing financial impact of cyber-incidents, it is imperative that the legislative environment is enabled to afford corporations protection and support law-enforcement in combatting cyber-attacks.

The increase in hacktivism in South Africa, notable in the data for 2016, can be linked to increased political tensions in the country (Vermeulen, 2016b). Even some of the non-state/non-political organisations targeted were linked to perceived government corruption (Van Zyl, 2016a). None of the organisations targeted, nor the way they were targeted, appeared to have any major direct impact on national stability or the national economy. However, there are at present certain large state-owned enterprises in South Africa, also linked to the political scandals, which have not yet been targeted. Should, for instance, the major electricity provider, Eskom, be attacked and for some reason operations hindered, there could be significant socioeconomic ramifications.

The numerous instances of cybersecurity threats caused by accidental/misconfiguration perpetration is concerning, as they have all occurred since the POPI Bill of 2009. It is possible that the Bill resulted in increased awareness and, in turn, an increase in exposures being reported. However, it still suggests that organisations, both state/political and other neglecting their responsibility to ensure that the systems are configured correctly. A possible solution will be to focus cyber-security awareness training on IT professionals in the country, in order to assist in creating a secure culture and an improvement of security in system development. Moreover, once the POPI Act is fully enforced and organisations are held fully accountable for such breaches, more effort may be given to discovering flaws, thereby reducing the accidental exposure.

Nation-state espionage is relatively low, and this is consistent with the findings of the report by Brown and Rudis (2017). At the same time, it is interesting to note that two of the nations most commonly associated with cyber-espionage campaigns – Russia and China – belong to a club of countries, the BRICS, of which South Africa is also a member along with Brazil and India. As can be seen from the revelations of the United States and Western European nations spying on each other, even allied countries conduct espionage operations against each other. Therefore as global tensions rise, South Africa should not be surprised if economic friendly countries increase espionage activities to monitor its politics and foreign policy. This concept, known as the "cyber-security dilemma", is discussed by Buchanan (2017). This in turn may also instigate an increase of international hacktivist activity.

Overall, the prevalence of perpetration factors and actors, and the impacts, that this study found in South Africa are consistent with reported international cyber-incident trends. A limitation of this study is that the data available were limited to what is reported publicly. Until it is mandatory for South African organisations to report cyber-incidents, it will be difficult to conduct in-depth assessments of the composition of threat activities and their impacts.

References

Ackroyd, B. (2014, December 4). Cyber hacktivist strikes SA sites again. *ENCA*. Retrieved from http://www.enca.com/technology/cyber-hactivist-strikes-sa-sites-again

Ajam, K. (2012, November 10). Alarm over credit card breach. *The Independent on Saturday*.

Andress, J., & Winterfield, S. (2014). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed). Waltham, MA: Elsevier.

Arde, A. (2012, November 17). Hack attack a costly lesson for banks, *The Independent on Saturday*.

BBC News. (1999, September 13). Hackers deface SA stats site. Retrieved from http://news.bbc.co.uk/2/hi/africa/446392.stm

Brown, R., & Rudis, B. (2017). *Rapid7 threat report 2017 Q1*. Retrieved from https://www.rapid7.com/globalassets/_pdfs/research/rapid7-threat-report-2017-q1.pdf

Buchanan, B. (2017). *The cybersecurity dilemma*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

Cave, K. (2017, March 24). Cinema chain hack sees data security take centre stage in South Africa. *IDG Connect*. Retrieved from http://www.idgconnect.com/blog-abstract/25679/cinema-chain-hack-security-centre-stage-south-africa

Chandarman, R. (2016). *Cybersecurity awareness of students at a private higher education institute in South Africa*. Master's dissertation, University of KwaZulu-Natal, Westville, Durban.

Cusimano, J. (2010). DCS virus infection, investigation and response: A case study. Presentation to Industrial Control Systems Joint Working Group (ICSJWG) Fall Conference, 25-28 October, Seattle.

Department of Justice and Correctional Services. (2017). *Cybercrimes and Cybersecurity Bill*. Pretoria.

Dingle, S. (2009, July 15). Anatomy of an SMS banking scam. *FIN24.com*. Retrieved from http://www.fin24.com/articles/default/display_article.aspx?ArticleId=2638902

Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: A synergy approach. In V. Lysenko (Ed.), *7th International Conference on Information Warfare and Security* (pp. 98-107). Seattle: University of Washington.

ESET. (2016, October). *En route with Sednit: Part I: Approaching the target*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

Fearn, N. (2017, March 29). Critical lack of skills could be the biggest security challenge. *IDG Connect*. Retrieved from http://www.idgconnect.com/abstract/25505/critical-lack-skills-biggest-security-challenge

FireEye. (2014). APT28: A window into Russia's cyber espionage operations? Retrieved from https://www2.fireeye.com/apt28.html

Fripp, C. (2016, February 12). Anonymous begins #OpAfrica: Claims thousands of SA sites compromised. *htxt.africa*. Retrieved from http://www.htxt.co.za/2016/02/12/anonymous-makes-good-on-promise-goes-after-sa-government-websites/

Gorton, B. (2016, June 14). Anonymous Africa goes after "racist" EFF and their "Godfathers" Zanu PF. *Sowetan Live*. Retrieved from http://www.sowetanlive.co.za/news/article16983627.ece

HomeGrownHoney. (2009, January 7). Hackers expose South African banks. *ITWeb*. Retrieved from http://mydl.itweb.co.za/index.php?option=com_myblog&show=hackers-expose-south-african-bankshtml&Itemid=

ITNewsAfrica. (2013, August 30). MTN victim of cyber attack. Retrieved from http://www.itnewsafrica.com/2013/08/mtn-victim-of-cyber-attack/

ITWeb. (2013, May 6). No damage during Aarto hacking. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=63798

Limer, E, (2013). Meet Red October: The global cyber-espionage ring that spent 5 years in the shadows. *Gizmodo*. Retrieved from http://gizmodo.com/5975793/meet-red-october-the-global-cyber+espionage-ring-that-spent-5-years-in-the-shadows

Mail & Guardian. (2008, August 15). Hacker compromises DA website. Retrieved from https://mg.co.za/article/2008-08-15-hacker-compromises-da-website

Malwarebytes Labs. (2017). *State of malware report 2017*. Retrieved from https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf

Mandiant. (2013, February 19). *APT1: Exposing one of China's cyber espionage units*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Matinde, V. (2017, March 10). Cybersecurity must play catch up as more Kenyans move online. *IDG Connect*. Retrieved from http://www.idgconnect.com/abstract/25318/cybersecurity-play-catch-kenyans-online

Mbongwa, L., & Makua, J. (2005, January 13). Moroccan hackers blamed for website blitz. *Independent Online*. Retrieved from http://www.iol.co.za/news/south-africa/moroccan-hackers-blamed-for-website-blitz-231419

Miller, B., & Rowe, D. C. (2012). A survey of SCADA and critical infrastructure incidents. In RIIT '12 (Ed.), *Proceedings of the 1st Annual Conference on Research in Information Technology* [RIIT '12], (pp 51-56), New York: ACM. https://doi.org/10.1145/2380790.2380805

Mkhwanazi, S. (2015, October 12). Roads agency account hacked for R8.5m. *Independent Online*. Retrieved from http://www.iol.co.za/capetimes/roads-agency-account-hacked-for-r8-5m-1.1928834

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

MyBroadband. (2013a, August 21). City of Joburg exposes private information again. Retrieved from https://mybroadband.co.za/news/security/84929-city-of-joburg-exposes-private-information-again.html

MyBroadband. (2013b, October 15). Mass security breach of fast food payment systems in SA. Retrieved from http://mybroadband.co.za/news/security/88985-mass-security-breach-of-fast-food-payment-systems-in-sa.html

MyBroadband. (2014, January 5). Big Cell C security flaw uncovered. Retrieved from https://mybroadband.co.za/news/security/94332-big-cell-c-security-flaw-uncovered.html

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

Norton South Africa (2012) *Norton cybercrime report 2012*. Retrieved from http://za.norton.com/cybercrimereport/promo?inid=uk_hho_downloads_home_link_cybercrimereport

Oiaga, M. (2006, July 4). Three South African banks hit by hackers. *Softpedia*. Retrieved from http://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml

Paganini, P. (2013, January 17). Red October, RBN and too many questions still unresolved. Security Affairs blog. Retrieved from http://securityaffairs.co/wordpress/11779/cyber-crime/red-october-rbn-and-too-many-questions-still-unresolved.html

Patrick, H. (2015). *Security information flow in the public sector: KZN health and education*. PhD thesis. University of KwaZulu-Natal, Durban.

Plaut, M. (2010, October 26). Book says hacker tried to stop Mandela coming to power. *BBC News*. Retrieved from http://www.bbc.com/news/world-africa-11630092

Porter, B. (2003, August 8). Hackers target SA universities. *News24*. Retrieved from http://www.news24.com/SciTech/News/Hackers-target-SA-universities-20030808

Potgieter, D. (2011, January 8) Absa intercepts land bank swindle. *Saturday Star*. Retrieved from http://www.iol.co.za/business/companies/absa-intercepts-land-bank-swindle-1.1009423

Pretorius, B. H. (2016). *Cyber-security and governance for industrial control systems (ICS) in South Africa*. Master's dissertation, University of KwaZulu-Natal, Durban.

PricewaterhouseCoopers (PwC), & BAE Systems. (2017). Operation Cloud Hopper. Retrieved from https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

Rasool, F. 2012. Postbank heist signals policy gap, *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=50818

Redelinghuis, K. (2011, March 30). ANC Youth League website hacked by "Warbird". *Memeburn*. Retrieved from http://memeburn.com/2011/03/anc-youth-league-website-hacked/

Republic of South Africa (RSA). (2002a). Electronic Communications and Transactions Act 25 of 2002.

RSA. (2002b). Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002.

RSA. (2009). Protection of Personal Information (POPI) Bill 9 of 2009.

RSA. (2013). Protection of Personal Information (POPI) Act 4 of 2013.

Reuters. (1998, June 11). South Africa police arrest teen hacker. Retrieved from http://lists.jammed.com/ISN/1998/11/0032.html

Roane, B. (2013, May 22). SAPS website hacked. *The Star*. Retrieved from http://www.iol.co.za/news/crime-courts/saps-website-hacked-1.1520042

SABC News. (2017, April 19). Cyber-attacks reaching a critical point in SA. Retrieved from http://www.timenews.co.za/timenews-sabc-news-cyber-attacks-reaching-a-critical-point-in-sawednesday-19-april-2017

Safenet. (2014). Breach database: Top data breaches. Retrieved from http://www.breachlevelindex.com/#!breach-database

SANews. (2012, December 21). Attack on e-toll website foiled. Retrieved from http://www.sanews.gov.za/south-africa/attack-e-toll-website-foiled

Saville, M. (2012, December 9). Three SA government websites hacked. *Mail & Guardian*. Retrieved from https://mg.co.za/article/2012-12-09-three-government-websites-hacked

Song, S. (2017). African undersea cables – Interactive. Many Possibilities blog. Retrieved from https://manypossibilities.net/african-undersea-cables-interactive

Speckman, A. (2015). Cybercriminals are on the prowl. *BDLive*. Retrieved from http://www.bdlive.co.za/businesstimes/2015/02/01/cybercriminals-are-on-the-prowl

State Security Agency (SSA). (2015). *National cybersecurity policy framework*. Pretoria.

Stone, A. (2010, April 25). Patient records for all to see. *I-Net*. Retrieved from http://news.za.msn.com/local/article.aspx?cp-documentid=153155730

Swart, W., & wa Afrika, M. (2012, January 15). It was a happy New Year's Day for a gang who pulled off...R42m Postbank heist. *Times Live*. Retrieved from https://www.timeslive.co.za/news/south-africa/2012-01-15-it-was-a-happy-new-years-day-for-gang-who-pulled-offr42m-postbank-heist

Tate, S. (2017, April 19). Why Australia will lose a cyberwar. *Vice*. Retrieved from https://www.vice.com/en_au/article/why-australia-will-lose-a-cyberwar

TelecomSpeak. (2015, May 18). Cyber attack targets MTN Data Centre. Retrieved from http://www.telecomspeak.com/2015/05/18/cyber-attack-targets-mtn-data-centre

Tengimfene, N. (2013). Media statement on progress made by the Justice, Crime Prevention & Security cluster in the fight against corruption. Pretoria: Government Communication and Information System (GCIS).

Tubbs, B. (2013, May 22). SAPS hack spells negligence. *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=64268:SAPS-hack-spells-negligence&catid=265

Van Niekerk, B. (2017). Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (Ed.), *Threat mitigation and detection of cyber warfare and terrorism activities* (pp. 69-92), Hershey PA: IGI. https://doi.org/10.4018/978-1-5225-1938-6.ch004

Van Rooyen, K. (2009, July 18). Hidden price of a banking scam. *The Times*. Retrieved from http://www.thetimes.co.za/News/Article.aspx?id=1036132

Van Zyl, G. (2016a, June 15). Hack attack threat for Gupta sites, Oakbay and Sahara down. *Fin24*. Retrieved from https://www.fin24.com/Tech/Cyber-Security/anonymous-threatens-hack-attacks-on-gupta-websites-20160615

Van Zyl, G. (2016b, June 30). Standard Bank computer was hacked in R300m ATM fraud hit – report. *Fin24*. Retrieved from http://www.fin24.com/Tech/Cyber-Security/standard-bank-computer-was-hacked-in-r300m-atm-fraud-hit-report-20160630

Van Zyl, G. (2016c, July 12). Anonymous "hacks" Armscor website. *Fin24*. Retrieved from http://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712

Venktess, K. (2016, September 8). eThekwini municipality website leaks user data – Expert. *Fin24*. Retrieved from http://www.fin24.com/Tech/News/ethekwini-municipality-website-leaks-user-data-expert-20160908

Vermeulen, J. (2013, May 14). Spyware servers in South Africa: the plot thickens. *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/77110-government-spyware-servers-in-south-africa-telkom-govt-mum.html

Vermeulen, J. (2014, January 8). E-toll website flaw a cyber-attack: Sanral. *MyBroadband*. Retrieved from https://mybroadband.co.za/news/security/94554-e-toll-website-flaw-a-cyber-attack-sanral.html

Vermeulen, J. (2016a, February 12). Anonymous hacks SA government database, *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html

Vermeulen, J. (2016b, June 13). This is how I took down the SABC: Anonymous hacker. *MyBroadband*. Retrieved from http://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html