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

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0
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 it 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**

![Trends in impact type](image)

**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

<table>
<thead>
<tr>
<th>Victim type</th>
<th>Data exposure</th>
<th>Denial of service</th>
<th>Financial</th>
<th>Defacement</th>
<th>Data corruption</th>
<th>System penetration</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental/misconfiguration</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Criminal</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td>17</td>
</tr>
<tr>
<td>Insider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Malware</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Nation-state espionage</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Individual hacker</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Totals</td>
<td>22</td>
<td>9</td>
<td>12</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>54</td>
</tr>
</tbody>
</table>

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 illustrates 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 attacks 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 between 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

<table>
<thead>
<tr>
<th>Impacts</th>
<th>Data exposure</th>
<th>Denial of service</th>
<th>Financial</th>
<th>Defacement</th>
<th>Data corruption</th>
<th>System penetration</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>12</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>State/political</td>
<td>10</td>
<td>4</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>29</td>
</tr>
<tr>
<td>Total</td>
<td>22</td>
<td>9</td>
<td>12</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>54</td>
</tr>
</tbody>
</table>

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

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

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


