Contextualising Cybersecurity Readiness in South Africa

Namosha Veerasamy [1], Thulani Mashiane [2] and Kiru Pillay,
[1, 2] Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
LINK Centre, South Africa
nveerasamy@csir.co.za
tmashiane@csir.co.za
kiru2010@gmail.com

Abstract: The expansion of the information society has brought with it a revolution in the use of Information Communication Technology (ICT). In South Africa, the adoption of various digital devices and technologies has introduced conveniences but at the same time it also opens up the door for various cybercrime attackers. This digital paradox demonstrates that ICT has tremendous capabilities for the rapid provision of services but at the same time can be exploited by malicious cybercriminals.

It is vital that organisations and individuals not overlook the strong imperative for cybersecurity. In an interconnected world, cybersecurity and cybercrime go hand in hand. With cyber-attacks and data breaches are on the rise organisations need to be constantly adapting their security measures and preparing for cyber threats.

At the end of 2017, a survey was carried out on the state of cyber readiness levels across various sectors in South Africa. The aim of the survey was to identify the current security posture in organisations and ascertain where the gaps were in order to respond to developing cyber threats. Cybersecurity needs to be viewed from various dimensions and thus the survey focused on the status of cybersecurity plans, strategies, governance, standards, Computer Security Incident Response Team (CSIRT) membership, awareness programs, vulnerability and risk assessments as well as incident management capabilities.

This paper presents the results of the survey which are further analysed in order to contextualise critical findings and recommendations. The survey provided important insights into cyber readiness in South Africa. In this paper the results are placed in context of global trends in order to determine key areas that require attention. It is important to identify how organisations in South Africa should be dealing with disaster recovery planning and how to remain operational when faced with system interruptions and interferences. Contextualising the cyber readiness levels helps asses the latest threat landscape, as well as develop strategies to mitigate these cyber risks.

Keywords: cyberattack, cyber awareness, cybersecurity readiness, data breach, threat intelligence

1. Introduction

South Africa has experienced a number of high-profile data breaches in recent years. In October 2017 over 60 million South African citizens' personal data - ranging from ID number to company directorships - were leaked (Fraser, 2017). Soon after approximately one million personal records was posted publicly by one of the companies responsible for online payments of traffic fines in South Africa (Business Tech, 2018). In the middle of 2018 Liberty Holdings informed clients that its email repository has been breached by a third party demanding a "ransom" in exchange for the data (Niselow, 2018).

These breaches have placed a spotlight on how the South African government and relevant government agencies and institutions respond. The country's Protection of Personal Information Act (POPIA) was intended to help establish stronger controls. However execution of the Act has been challenging, with only certain provisions of the Act currently being implemented. The establishment of cyber measures and the building of cyber resilience by organisations can assist in preventing data breaches and other system exploits.

Very little information is available about the state of cyber readiness in South Africa. Thus, in 2016 the Department of Telecommunications and Postal Services, as the Department with the mandate for the establishment and operationalising of the national CSIRT known as the Cybersecurity Hub, together with its research partner the Council of Scientific and Industrial Research (CSIR) undertook a baseline study on the state of cyber readiness in South African organisations.

This paper reveals key findings about how organisations view their cyber readiness levels. It further describes local trends within the context of global patterns, which identifies how South Africa organisations compare with regards to the global threat landscape. This is important as South Africa has a leading role in the African continent.

The sample size of the survey was 83, with the majority of the respondents employed in the security management field. The respondent organisations were representative of the following sectors: finance (28.92%), government and defence (31.33%), higher education (19.28%), research, information technology (IT) and telecommunications (20.48%) sectors.

Organisation size represented in the survey was largely in favour of very small organisations, with 55% having 1-999 employees. Just over 17% of the respondents worked in a large organisation that had more than 5000 employees; 11% were from medium-size organisations that have 2000-3999 employees; with 17% working for small organisation that have between 1000-1999 employees.

In the next section, the key outcomes of the survey results are discussed and placed in context of global patterns and findings. Thereafter, implications of the survey findings, as well recommendations for the improvement of cyber resilience are covered.

2. Key Outcomes

This section focuses on some of the key outcomes that are in line with global trends. One of the most significant findings relate to the threats facing organisations.

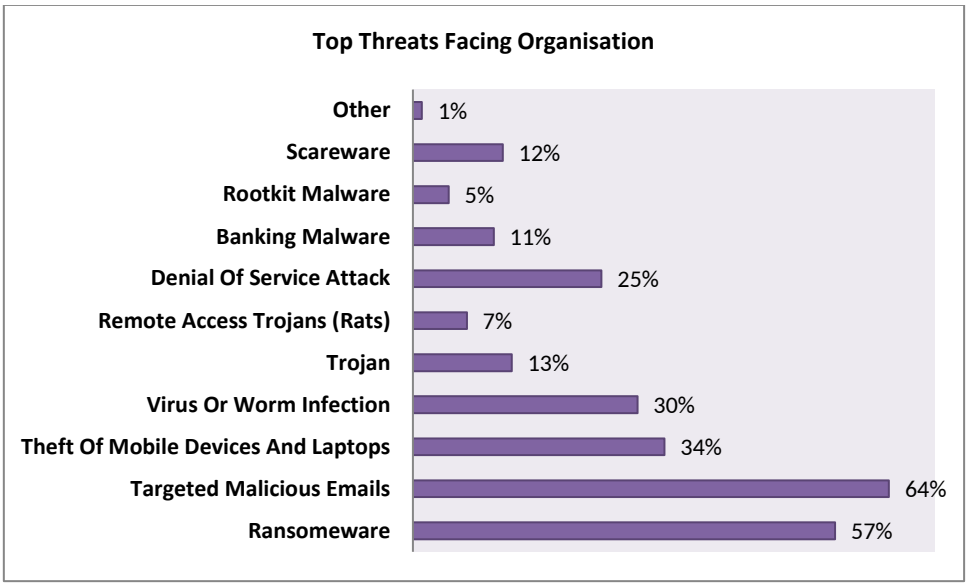

Figure 1 : Top Threats Facing Organisations

The top three threats facing organisations (see Fig1) were targeted malicious emails (64%), ransomware (57%) and theft of mobile devices and laptops (34%). Targeted malicious emails are low volume socially engineered emails aimed at soliciting sensitive information or clicking on malicious links. The Symantec Internet Threat Report- Email Threats 2017 discusses the various forms of email threats that have evolved over the years. The threat of business email compromise (BEC) scams continues to grow, as does the financial impact (Nahorney, 2017). Targeted malicious emails can take the form of a spoofed email from an executive asking for an urgent money transfer or a supplier that needs to be paid for outstanding goods.

Other forms of the attack may try to convince employees to disclose sensitive files or even click on a malicious link in the email in order to compromise critical systems in the organisation. Without knowledge about potential signs of these malicious emails, the intended recipients of these emails could fall victim to a serious ploy. The prevailing theme of these messages is the requirement to act quickly and the sense of urgency created. Phishing schemes have evolved into spear-phishing (specific targets instead of bulk unsolicited emailing) and whaling (high-profile targets like executives in an organisation).

Email is the most frequently used delivery mechanism of malware (Nahorney, 2017). Many malicious emails try to entice users into opening a malicious attachment with subject lines like bill, invoice, package delivery, scanned documents as they appear to be standard emails. When users are faced with threat of an account being locked out, they may also be keen to click on email links and attachments. Such emails that appear legitimate to users are a constant danger. Phishing schemes continue to persist and evolve as attackers find innovative ways of tricking users and convincing them to respond to fake emails.

Furthermore, malware in the form of ransomware continues to be a prevailing threat. This draws a parallel to global trends whereby ransomware has continued to grow with immense financial effects on consumers and businesses.

Cybersecurity Ventures predicts ransomware will globally cost $6 trillion annually by 2021 (Morgan, 2017). Ransomware has also advanced as cybercriminals adapt with more complex ways of encrypting data and extorting organisations. According to a Kapersky Lab survey, 34% of businesses hit with malware took over a week or more to

recover full access to their data (Cook, 2018). This highlights the need for proper disaster recovery planning, as well as backup procedures in order to get system operational once more.

The concern over ransomware was a valid one as 2017 saw the outbreak of WannaCry- the cyber attack that targeted over 200 000 systems on its first day and affected companies and individuals in more than 150 countries, including government agencies (Langde, 2017). A month later in June 2017, the Petya ransomware swept across systems and once more affected various companies including banks, airlines and hospitals. Data is being used as a powerful weapon as attackers target it as a commodity for which they can extort money. In order to adapt to this growing trend, organisations need to become better equipped to dealing with such attacks. Cyber resilience, planning and training is necessary in order to build stronger defences.

The third most dominant threat found in the survey was theft of mobile devices and laptops. Kensington estimates that a laptop is stolen every 53 seconds; 70 million smartphones are lost each year with 80% of the cost of the lost laptop stemming from the data breach. (Hom, 2017). A stolen laptop does not only entail the costs of replacing the device, but other factors like loss productivity, lost intellectual property, data breaches, support and managerial administration also play a dominant role. Users need to take additional steps in securing their data like encryption, authentication, physical security and never leaving applications logged in. Users also need to cautious when utilising open Wi-Fi as these networks are often not secured and information can be easily disclosed without the permission of users. Nearly 41% of all data breach events from 2005 through 2015 were caused by lost devices such as laptops, tablets and smartphones (Olenski, 2017). Theft still prevails as a prominent problem in recent years but organisations need to implement measures in order to reduce exposure of data. Businesses cannot afford to take chances with sensitive data.

Though not featured in the survey at the time, an associated threat that has emerged is the exploitation of digital currencies and the various attempts designed to mine cryptocurrency. The theft of cryptocurrency, as well as the theft of computer processing power to mine cryptocurrency is listed as one top emerging threats (Giles, 2018). The rise of crypto-mining requires intensive computational processors. This has led hackers to breach more computer networks in order to access more computational power in order to solve complex mathematical problems. In 2017, Kapersky Labs found cryptocurrency mining tools on 1.65million of its client's computers which was far above the previous years (Orcutt, 2017). Hackers may also be keen to prey on easier-to-mine currencies and try to make use of computing power.

Threats may stem different type of actors. In the next section, the results of the top threat actors are elaborated on.

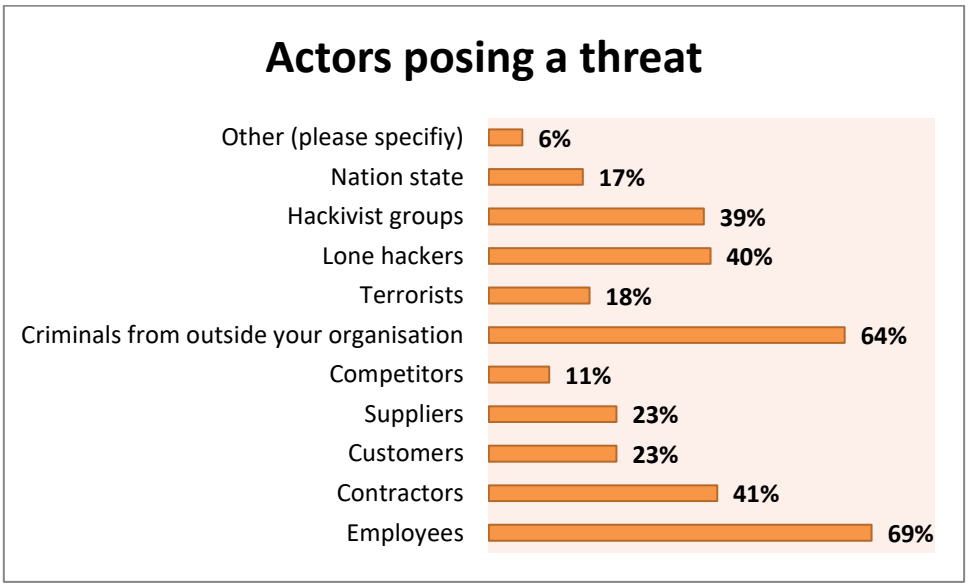

Figure 2 : Actors posing a threat to organisations

The threat actors posing the biggest threat to organisations were identifed as employees (69%) and external criminals (64%) as illustrated in Figure 2.

Ablon (2018) explains that cyber criminals are typically motivated by financial gain and seek to access data (persona, financial or health) in order to monetize them, typically on the black markets.

The insider threat stems from attackers within an organisation that may be disgruntled or looking for revenge or some other financial gain. Employees could also be infiltatred through bribery by an organised criminal group or sponsored hacker in order to carry out an attack on organisatonal systems.

In some cases, employees may inadvertently infect an organisation or unleash a virus. This links up to the top threats facing organisations as spear phishing attacks (targeted malicious emails) can disclose sensitive information or result in a ransomware infection.

Hacktivists threat actors, which were chosen by 39% of respondents (see Figure 2), seek to create awareness or protest about a specifc issue and may be involved in cybervandalism. For many organisations, hacktivists are of great concern as they carry out web defacement or publicize a breach in order to emphasise the vulnerability of organisaitons.

In order to overcome the exploitation of unsuspecting users, a strong cyber culture needs to be developed. This requires an investment in time, resources and training and can help instil cyber safe practices and creating more awareness of emerging threats and trends. Furthermore, an important aspect of cyber resilience and building cyber readiness is the development of threat intelligence. 25% of organisations surveyed had established a threat intelligence capability while 20% were in the process (refer to Figure 3).

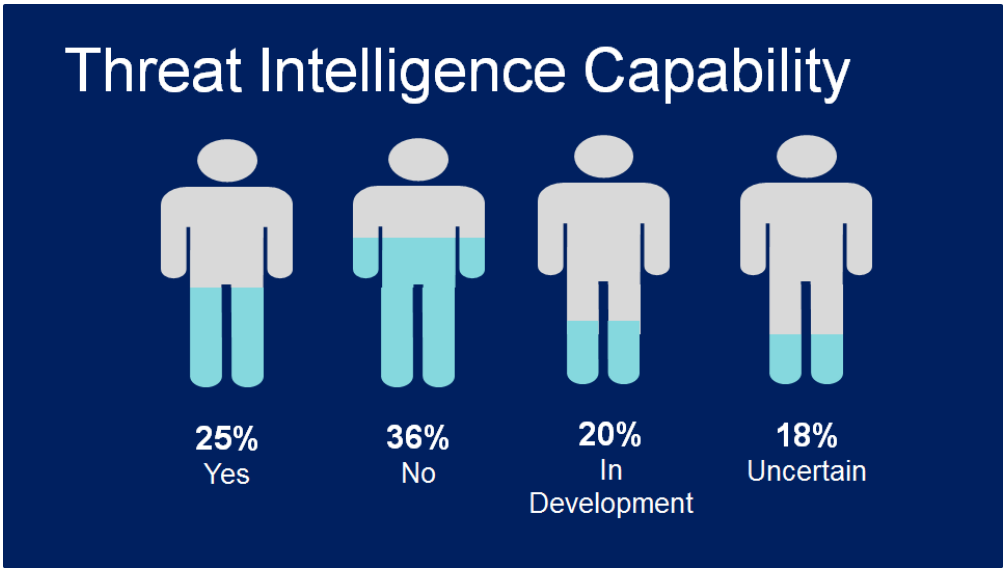

Figure 3 : Cyber Threat Intelligence Capability

Cyber threat intelligence (CTI) recognizes indicators of attacks as they progress and essentially put these pieces together with shared knowledge about attack methods and processes (Shackleford, 2015). A cyber threat intelligence capability allows organisation to merge and analyse multiple data feeds so as to gain deeper insights into system weaknesses and the spread of attacks. Collated data from cyber threat intelligence provides the context of complex threats, as well as can help develop more proactive and defensive mechanisms. Through cyber threat intelligence, the sharing and exchange of critical attack data can be facilitated.

With regards to the handling of cyber incidents and intelligence, membership to a Computer Security Incident Response Team (CSIRT) can be beneficial. 45% of the organisations surveyed belonged to a CSIRT and 22% obliged to report incidents to their respective CSIRTs (Refer to Figure 4). In South Africa the emerging legislative framework and specifically the National Cybersecurity Policy Framework (NCPF), which was passed in 2012, mandates the establishment of various national CSIRTs. The policy framework also mandates the establishment of sector-based CSIRTs which are meant to cultivate a collective capability for cybersecurity within specific sectors. The banking sector for example has collectively established the South African Banking Risk Information Centre (SABRIC), whose stated aim is to be "Africa's trusted financial crime risk information centre leveraging on strategic partnerships (South African Banking Risk Information Centre, 2018). Various other sector-CSIRTs have been established or are in the process of being established.

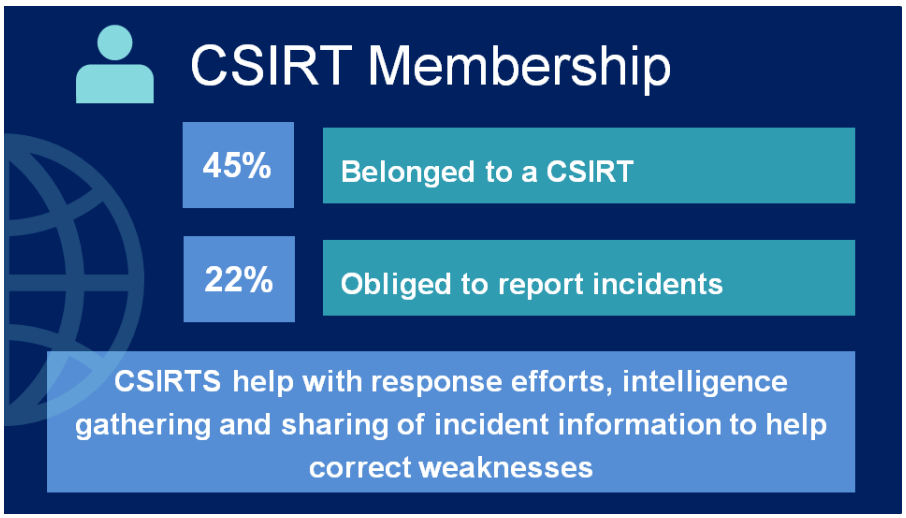

Figure 4 : CSIRT Membership of Organisations

Overall, when striving to meet cyber readiness is it important to understand both the adversaries, as well as the threats. Strong cyber capabilities will entail proactive measures in order to try and stay ahead of the attack vectors and perpetrators. Improvement of policies, technologies and processes all aim to identify, track and repel attacks. In this section, vital details about attack trends were discussed. In the next section, further findings related to proactive measures are discussed.

3. Implications from Findings

The survey posed various questions regarding the state of the organisations' security measures. From the findings, the following implications and critical findings are summarised next. It is imperative for the building of cyber readiness that organisations address the following core issues:

- Implement a cyber security plan
- Increase cyber security awareness and training
- Train and upscale cybersecurity experts
- Execute risk assessments
- Improve Business Continuity/Disaster Recovery Planning

A discussion follows on the survey results that inferred these critical implications that organisation should address. .

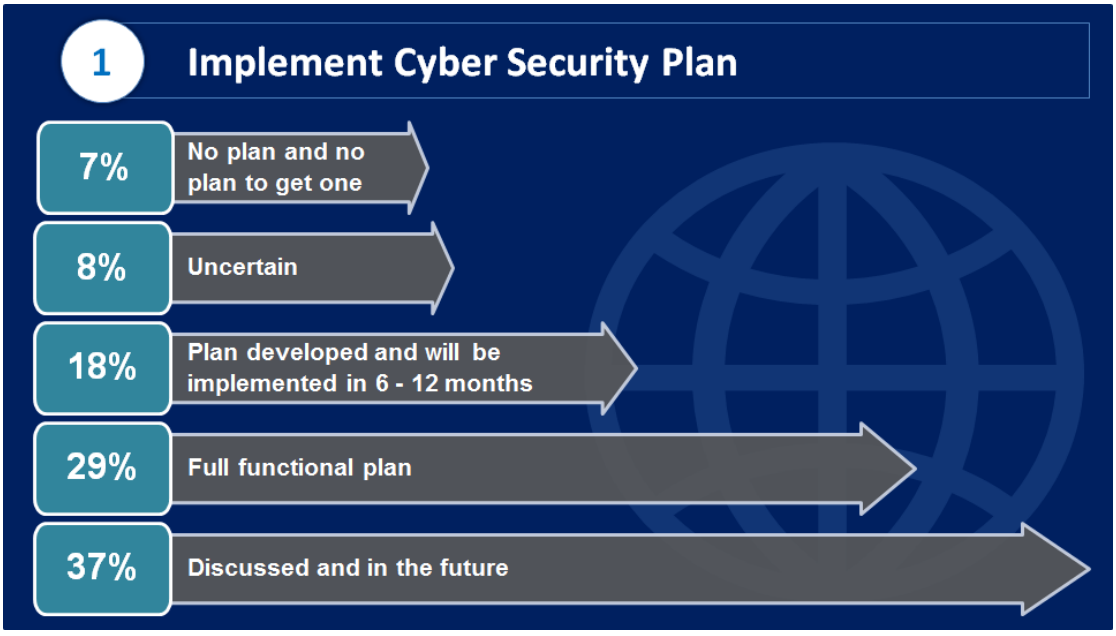

Figure 5 : Cyber Plan Status in Organisations

From the organisations that participated in the survey, 29% had a fully functional plan and 37% had discussed and planned to implement sometime in the future (See Figure 5). 18% planned to develop and implement a cyber security

plan within a year. A proper security plan would outline an organisation's strategy and operational approach in implementing cyber security. It would address the various aspects dealing with the people, processes and technology required to manage cyber security. Without a suitable plan an organisation may tackle aspects of cybersecurity on an ad hoc basis. This could result in an organisation having its security seriously compromised as there is no directorial governance or guidance as to how cyber security is handled in the organisation. A key part of a cyber security plan is how an awareness program will be carried out in an organisation. This is discussed next.

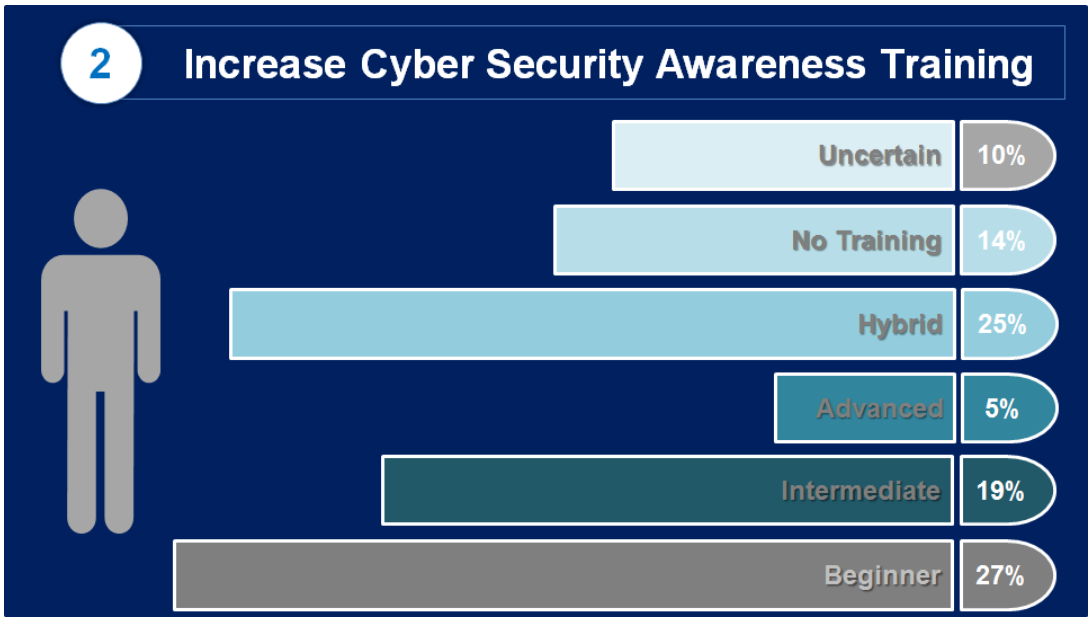

Figure 6 : Cyber Security Awareness Training Results

In terms of cyber security awareness training, 14% of the organisations indicated that the organisation has never rolled out a training program (Refer to Figure 6). This is problematic as cyber criminals such as social engineers rely on the lack of knowledge of employees in an organisation to carry out an attack. Of those organisation that have provided training, 25% of the training has been provided by a mixture of in-house, external service provider or by an affiliated organisation. The survey also probed the participants on the overall level of cyber security awareness of their organisations (see Figure 6), the results show that 27% of the participants indicated beginner, 19% indicated intermediate and 5% indicated advanced. These results should be an alert to South Africa to train employees in cyber security because cybercriminals are now targeting users to gain access to an organisation's systems (Nilsen, 2017).

Together with the lack of awareness, cyber security faces various challenges. The discussion on the various cyber security challenges follows next.

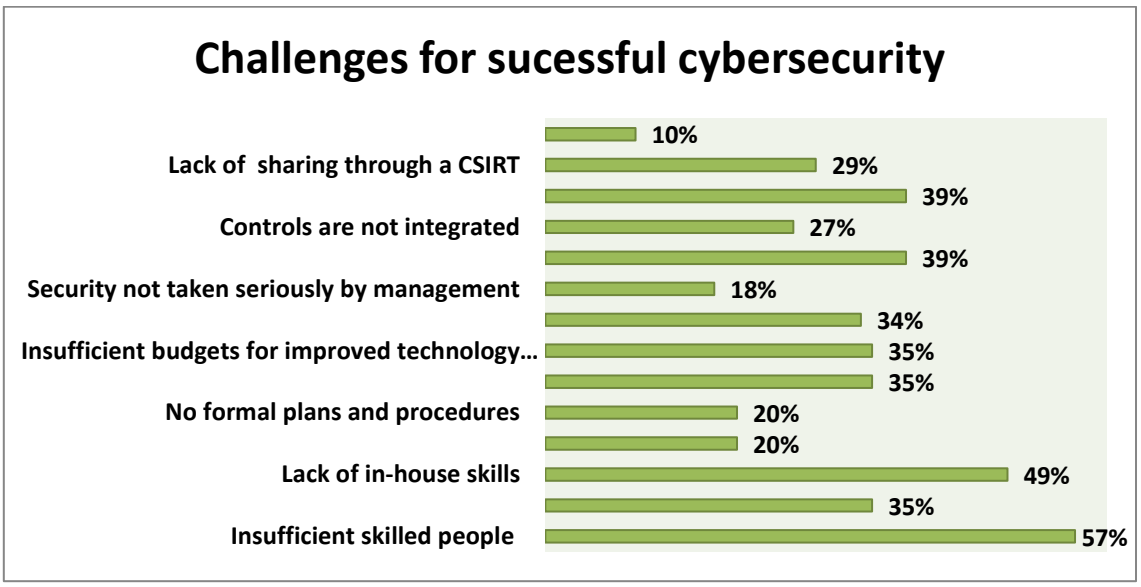

Figure 7 : Challenges for successful cybersecurity

The top challenges facing organisation for the implementation of successful cybersecurity were insufficient skilled people (57%), lack of in-house skills (49%), lack of awareness (39) and lack of threat intelligence (39%) (Refer to Figure 7).

Cyber security skills shortage has become a major challenge in industry and thus the requirement for training and upscaling cybersecurity specialists has increased. A common consensus is that at least 1.5 million cyber security jobs will be left vacant by 2019 and ISACA predicts there will be a global shortage of two million security professionals by 2019 (Silensec, 2017). Continued training is vital to retaining cybersecurity talent as well the development of critical technical skills, cultivation of a more diverse workforce and reformation of educational and training programs to include more hands on training (McAffee, 2016). Closing the skills gap will require various changes like training opportunities, workplace diversification, certifications, educational improvements and various concurrent efforts.

Furthermore, the findings highlight the need for awareness programs and threat intelligence (mentioned previously). Awareness programs helps to influence the adoption of secure behaviour whereas, threat intelligence can help identify emerging threats and patterns of attack. These core capabilities are necessary in the fight against cyberattacks. Another strategic positioning of an organisation in combatting threats is its risk assessment capability. This is discussed next.

Figure 8 : Risk Assessment Execution Frequency

With reference to Figure 8, it was found that 36% of organisations that participated in the survey, carried out a risk assessment annually, with 14 % either doing it periodically or unsure of the frequency of their risk assessment schedule (See Figure 8). 4% had no formal processes for risk assessment. The enterprise risk assessment methodology has become as established approach in identifying and managing systematic risk for an organisation (Schmittling, 2010).

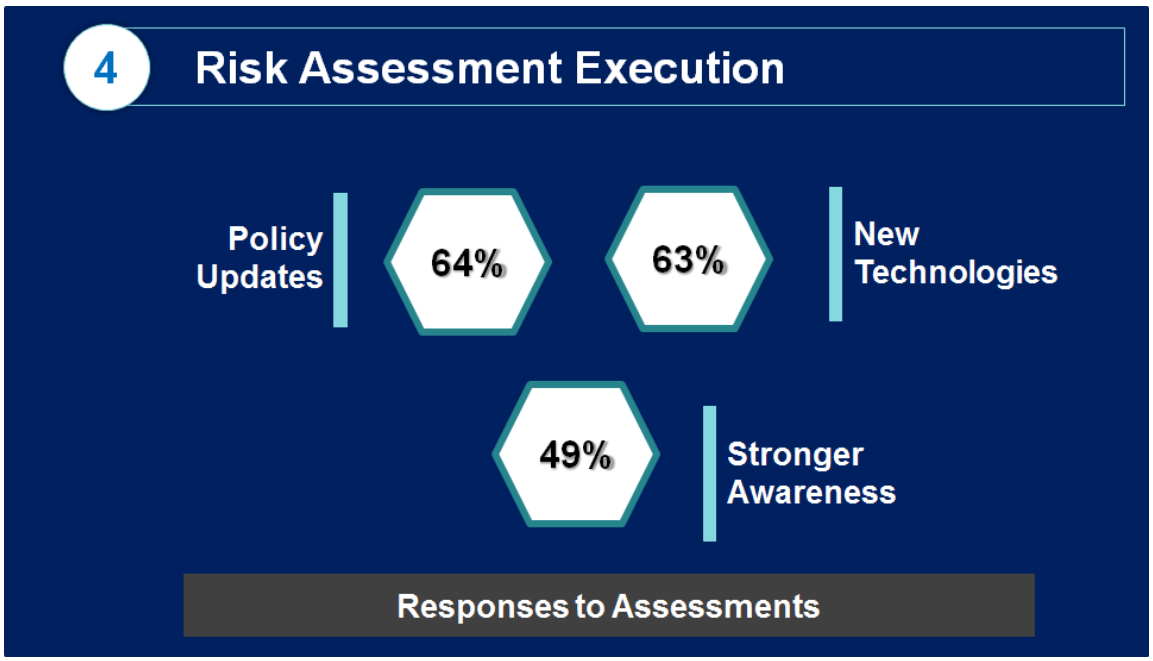

Figure 9 : Response to Risk Assessments

In response to risk assessments (see Figure 9), 64% of organisations carried out policy updates, 63% implemented new technologies and 49% rolled out stronger awareness campaigns. These three responses are aligned to the concepts that good security requires management of people, processes, and technology. These key response mechanisms aim to help to reduce human error, as well as system vulnerabilities. Another critical area of cyber readiness is the ability to respond after a disaster or incident. The findings in the survey relating to business continuity/disaster recover are discussed next.

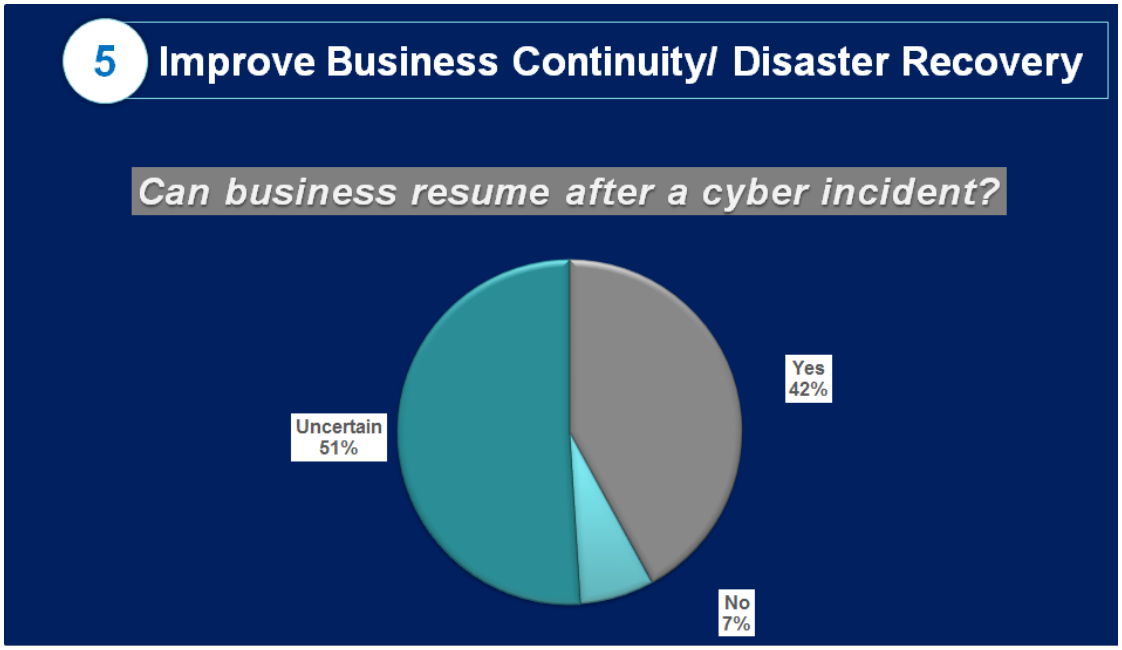

Figure 10 : Ability to resume business after an incident

A study by Ada (2017) focused on measuring cyber resilience of Africa's to 12 economies. The results of the study places South Africa in 6th position in terms of the cyber preparedness readiness index. This is despite the country being second in terms of GDP (Ada, 2017). In the present study (results shown in Figure 10), a large percentage (51%) of the participants indicted uncertainty of whether their organisation can survive a cyber-attack. This number is unsettling because technology does not only play a supportive role in business it is also strategic. This may result in organisations shutting down after a successful cyber-attack. Cyber security resilience is important for organisations because business continuation after an attack is essential to the economy as well.

4. Conclusion

The issue of cybersecurity is high on the agenda of many governments and organisations with many mindful of the shared public private responsibility for cybersecurity, and of the need to mobilise both public and private organisations within a multi-stakeholder model. A growing number of African countries have established - or are in the process of establishing - an enabling policy and legislative environment for cybersecurity.

While the trends in the survey point to a positive attitude towards cybersecurity it is incumbent on government and organisations remain vigilant to ensure that we build confidence in our citizens and institutions to transact and socialise in cyberspace.

1 Bibliography

Ablon, L., 2018. *The Motivations for Cyber Threat Actors and their use and Monetization of Stolen Data.* s.l.:RAND Corporation.

Ada, P. S., 2017. Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection,* Volume 17, pp. 49-59.

Business Tech, 2018. *South African exposed in another massive data breach.* [Online] Available at: https://businesstech.co.za/news/internet/246729/south-africans-exposed-in-another-massive-data-breach-report/

Cook, S., 2018. *2017-2018 Ransomware statistics and facts.* [Online] Available at: https://www.comparitech.com/antivirus/ransomware-statistics/#gref [Accessed 2 August 2018].

Fraser, A., 2017. *Biggest ever SA data breach : 60 million ID numbers leaked on real estate server.* s.l.:Global Citizen.

Giles, M., 2018. *Six Cyber Threats to Really Worry About in 2018.* [Online] Available at: https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/ [Accessed 21 August 2018].

Hom, E. J., 2017. *Mobile Device Security: Startling Statistics on Data Loss and Data Breaches.* [Online] Available at: http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches
[Accessed 21 August 2018].

Langde, R., 2017. *WannaCry Ransomware: A Detailed Analysis of the Attack.* [Online] Available at: https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/ [Accessed 21 08 2018].

McAffee, 2016. *Hacking the Skills Shortage,* California, United States: Centre for Strategic and International Studies.

Morgan, S., 2017. *Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017,* California: Cyber Security Ventures.

Nahorney, B., 2017. *Internet Security Threat Report: Email Threats 2017,* s.l.: Symantec.

Nilsen, R. Y. L. S. T. a. D. B., 2017. *A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users.* s.l., s.n.

Niselow, T., 2018. *Five massive data breaches affecting South Africans.* s.l.:Fin24.com.

Olenski, S., 2017. *Is the Data on Yours Business Digital Devices Safe?.* [Online] Available at: https://www.forbes.com/sites/steveolenski/2017/12/08/is-the-data-on-your-business-digital-devices-safe/#46ffaa8e4c6a
[Accessed 21 August 2018].

Orcutt, M., 2017. *Hijacking Computers to Mine Cryptocurrency is all the Rage.* [Online] Available at: https://www.technologyreview.com/s/609031/hijacking-computers-to-mine-cryptocurrency-is-all-the-rage/
[Accessed 21 August 2018].

Schmittling, R., 2010. Performing a Security Risk Assessment. *ISASA Journal,* Volume 1.

Shackleford, D., 2015. *Who's Using Cyberthreat Intelligence and How?.* [Online] Available at: 1 www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

Silensec, 2017. *Addressing the Cyber Security Skills Gap,* s.l.: s.n.

South African Banking Risk Information Centre, 2018. *SABRIC.* [Online]
Available at: https://www.sabric.co.za/who-we-are/
[Accessed 21 September 2018].