2018 Conference on Information Communications Technology and Society (ICTAS)

Towards an Electronic retail cybersecurity framework

Paul Jideani
Cape Peninsula
University of Technology
Cape Town, South Africa
pcijideani@gmail.com

Dr Louise Leenen
Council for Scientist and
Industrial Research
Cape Town, South Africa
lleenen@csir.co.za

Prof Bennet Alexander
Cape Peninsula
University of Technology
Cape Town, South Africa
alexanderb@cput.ac.za

Jay Barnes
Cape Peninsula
University of Technology
Cape Town, South Africa
barnesb@cput.ac.za

***Abstract*— Cybersecurity is one of the five key technologies that will spell the difference between company success and failure. This study seeks to understand cybersecurity environment of e-retail in South Africa. The focus is intended to offer and/or inform the creation of policy for cyber-securing e-Retail organisations in South Africa, and to set parameters through which current legislation on cybersecurity can be made relevant to e-Retailers in terms of compliance, technology and security. It looks into the basis for further research into the security of e-Retailers and how it can be used to support the national cybersecurity plan of South Africa in its entirety. Data on parameters through which current legislation on cybersecurity can be made relevant to e-Retailers in South Africa is needed coupled with qualitative content analysis to analyze data on cybersecurity. Several data collection methods using purposive sampling are highlighted (but not presented in this paper) including: (i) direct and in-depth interviews with retail company managers and e-Retail employees - directly linked to the use and security of critical infrastructure such as technology. (ii) document analysis on cybersecurity policy frameworks currently in use as well as other relevant government documents on e-Retail in South Africa.**

Keywords— Cybersecurity; Cyber-space; Policy framework; e-Retail; Cybersecurity Policy; Cyber-crime

I. INTRODUCTION

The evolution of the web/internet has transformed the face of e-commerce over the years, and has brought about a need for security in e-Retailing due to persistent malicious threats and attacks [1]. With the evolution of the internet, cybercrime has become prevalent with small companies increasingly becoming major targets. Amongst many factors, small-to-medium companies often lack adequate knowledge on how to deal with cyber-crimes [2]. According to [3], there has been a concern over the need for a more secure cyber-space in the form of cybersecurity to prevent cyber-crime. Cybersecurity involves the protection of cyber-space, those that function in the cyberspace and any assets that can be reached via the cyber-space. According the South African National Cybersecurity Policy Framework [1], the cyber-space is any physical and non-physical terrain created by and/or composed of some or all of the following: computers, computers systems, networks, data, traffic data and users. Cybersecurity is required in all areas that involve the internet and the cyber-space. E-Retail, like any other electronic commerce activity, is also one of the areas that involve the internet and the cyber-space. E-Retailing is a form of electronic commerce in which goods and services are obtained over cyber-space [4]. According to [5], addressing cybersecurity in the retail sector has been a great challenge that many businesses and government bodies have been struggling with over the years; as a result, e-retail organizations especially small to medium organizations have increasingly become vulnerable targets of cybercrime. Von Solms [2] suggests that amongst other factors, a lack of cybersecurity expertise and knowledge makes companies vulnerable. Hence, there is a need for cybersecurity frameworks that are tailored to the operational peculiarities of the industrial sector. Without an appropriate cybersecurity framework tailored to cater for organizational threats and vulnerabilities, business organizations will remain victims of these cybercrimes and other related activities. The consequence of cybercrime and attacks would ultimately result in unforeseen operational, financial, strategic and other challenges to the organization and the country at large [6]. Little to no evidence of frameworks customized for e-retail exists and literature suggests a number of these frameworks do not appropriately address cybersecurity concerns within the e-Retail context [7].

As a result of continuous cyber-crimes, organizations, governments and countries have placed importance on implementing cybersecurity policies, legislations and frameworks in order to prevent or minimize the occurrence of cybercrimes [8]. According to PricewaterhouseCoopers [9], South African organizations experience a high rate of cyber-crime; with evolution of internet technology, cyber-crime has become more prominent being the 4th most reported type of economic crime. Amongst a number of cybersecurity frameworks currently available, there exists a South African National Cybersecurity Policy Framework which was published in Dec 2015 and addresses a broad perspective of national cybersecurity guidelines [2]. This framework will be addressed in the later section of this paper, (section VII).

II. CYBERSECURITY

Cybersecurity involves the protection of cyberspace, those that function in the cyberspace and any assets that can

be reached via the cyberspace [10]. As with many other definitions, scholars have argued and proposed similar or conflicting notions on what cybersecurity is. The National Cybersecurity Policy Framework describes cybersecurity as the "practice of making networks that constitute cyber-space secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them" [11]. The Information Systems Audit and Control Association previously known as (ISACA), took a more methodical approach in its definition by suggesting that to understand cybersecurity, cyber-risk must be understood first. Cyber-risk, (which may vary in technology, means, attack vector etc.) is a group of risks that have a potential of great impact and once considered improbable. The International Telecommunications Union (ITU) in [12], also defined cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets" against cyber-crime.

III. CYBER CRIME

There has been varying descriptions and definitions given to cybercrime, differing based on the perception of the observer and investigation at hand. According to [3], cyber-crime is "any crime that is facilitated or committed using a computer, network or hardware device". Similar to that is any criminal offence committed via the internet, computer network. From the aforementioned definitions, the European commission on EU law issued a publication and proposed to define cybercrime in 3 aspects:

1. Traditional crimes committed through electronic communication networks and information systems,
2. Any distribution of illegal content over electronic media and finally,
3. Crimes unique to electronic networks [4].

Taking a closer look at the definitions above a few aspects can be deduced: (i) in the case of cybercrimes, the computer or electronic device could be the agent of the crime and (ii) the facilitator of the crime or the target of the crime.

In summary, cyber-crime takes place using or targeting computer networks and devices. This review proposes to follow the definition: "any crime that is facilitated or committed using a computer, network or hardware device" suggested by [3] as it satisfies the dual nature that the computer, network or hardware device could be the means to commit or the target entity. Due to the global nature of the internet, illegal activities are perpetuated by criminals all over the world. More so, the internet knows no boundaries making it a challenge to contain illegal activity over the internet, networks and hardware. Therefore, it is essential countries make cybersecurity a priority [5].

IV. THE NEED FOR CYBERSECURITY IN E-RETAIL

Cybersecurity is not optional; it is a necessity as the world transition from traditional marketing to selling and buying of goods and services over the cyber-space is rapidly increasing with time [16], [17]. Thus, protecting technological infrastructure commonly known as critical infrastructure (technology, application, hardware, network and data) requires security as these are the fundamental building blocks for an ICT driven society. Several reasons justify the need for cybersecurity in e-retail as a priority. Among these reasons include the need to encourage wide range of acceptability of e-commerce [18].

Statistics reveal that cybercrime is growing faster in Africa than in any other continent, as 80 per cent of PCs on the continent are reported to be infected with malicious software [19]. In many developing countries, there seems to be a reluctance by individuals to perform e-retail or online purchase. As is the case in many African countries this fear is not unfounded given that Kenya loses about 2 billion annually on cybercrime [20], [21]. This discourages the growth of e-retail due to dissatisfaction with the security of transactions. As internet penetration expands, so also is the rate of cybercrime. Some authors have suggested that cybercrime is internet penetration driven [22]. Cybersecurity is an old new plague affecting organizations, industrial sectors and countries. Cybersecurity will instill trust in e-Retail; trust will stimulate customers' expectation of a secure transaction as well as eliminate uncertainty and perceived risk. When adequate security is put in place there will be no reluctance from customers to adopt e-retail [23], [24].

The intricacy and sophistication of cyber-attacks calls for the need for proactive cyber-defense measures. Also, the cybercriminals carrying out the small or wide scale attacks are becoming more skilled and adapt to circumvent protection that have been placed [25], [26]. Small and medium-sized businesses face challenges due to limited resources such as: expertise, information, finance. Thus, need cybersecurity to protect their cyberspace containing intellectual property, trade secrets are sensitive information [2]. There are multiple reasons for conducting cyber-attacks against the e-commerce sector. Due to the reliance of trade on the sector, an attack could be used to affect trade in general, or even target a specific commodity. Due to the interdependence of the various commerce infrastructures, there are a variety of targets to impact on the trade: service providers could be targeted to prevent transaction from going through. Customer information could be stolen to commit phishing and impersonation [2].

V. CONCEPTUALISATION OF THE E-RETAIL ENVIRONMENT

E-Retail is the sale of goods and services via the internet or electronic channels. It involves transactions taking place from Business to Customer [6]. E-Retail is a type of activity that falls under e-Commerce which involves strategic use of computer mediated tools and information technologies to meet business objectives [7]. Cybercrime within e-Commerce is real in South Africa, with 31% of all attacks

targeting small businesses because they are less prepared to handle cyber risks [8]. South Africa is lagging behind on e-Retail development and remains at a nascent stage, calling for future developments in this sector ranging from infrastructure, legal compliance to security. The [8] also highlights broad issues that need to be addressed in South Africa such as international cybersecurity strategies that focus on technical, procedural and institutional measures. Through a deep examination of e-retail below is a conceptualisation of the ecosystem of e-retail in South Africa.

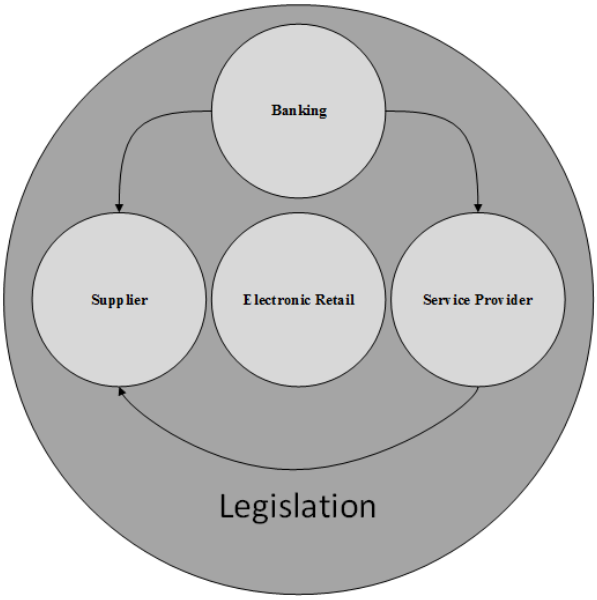

Figure 1. Interaction of niches in the e-retail environment

The e-retail organization at the core, secondly, physical connected environment at the next orbital level: these are considered as the actors or areas which service the e-retail organization. The actors include: Banking which facilitates payments and financial transactions. Service providers: these are agencies that provide resources to the e-retailer these include web development houses, data storage facilities or any other form of third-party amenity. Supplier: these provide products to the e-retail, there exists situations where the supplier is fully integrated into the system of the e-retail organization where a dedicated system is given to the supplier to manage. This is a very important aspect which should be noted and secured however, in some cases the supplier is a separate entity, not having any rights to systems. For the purpose of the research, the delivery service was intentionally omitted as it does not directly influence ecosystem. The legislative framework at the outer orbital which should govern the operations of the e-retailer. The legislative framework recognizes salient global, regional and national legal imperatives that support cybersecurity for e-commerce. The legislative framework will evolve using desktop research.

VI. SOUTH AFRICAN LEGISLATION AND POLICIES

South African legislative polices that should address cybersecurity and how these polices affect organizations are important if the country is ready to join the global competitiveness as well as to position itself in the next (fourth) industrial revolution. These policies cut across various information technology practices of which e-Retail falls under. Table 1 shows bills and acts with bearing to electronic retailing.

Legislation	Date of publication	Reason(s) for enacting
National Cybersecurity Policy Framework	December 2015	To facilitate protection of critical infrastructure. A strategy to guide cybersecurity in South Africa.
Protection of personal information act	November 2013	To safeguard personal identifiable information used by companies for business purposes. In addition, to regulate the manner in which personal information is processed.
Electronic communication and transaction act	August 2002	To facilitate and regulate electronic communications and transactions
Cybercrimes and cybersecurity bill	In the pipeline	To impose penalties which have a bearing on cybercrime. To criminalise acts related to cybercrime.

Table 1. Shows bills and acts with bearing to electronic retailing.

1) National Cybersecurity Policy Framework

The first draft of the National Cybersecurity Policy Framework (NCPF) was written in in 2010, approved by Government in 2012 and published in December 2015 [9]. The purpose of NCPF is to create a secure cyber environment that facilitates protection of critical information infrastructure. The NCPF is a high level document used as a single comprehensive strategy that guides the cybersecurity within South Africa [10]. However, writers such as [9], [2] have critiqued and criticised the framework as being too vague and general with no specific implementation strategies in place. It is important to note that the NCPF is not a practical guideline like the NIST Cybersecurity framework or ISO frameworks but a policy to guide cybersecurity; therefore, it requires room for contextualization depending on where it is to be applied [9], [2].

2) Protection of Personal Information Act

The Protection of Personal Information (POPI) is an information technology law passed into law in 2013 to govern the use of personal information [11]. The POPI Act was created to safeguard personal identifiable information used by companies for business purposes. Secondly, it is intended to regulate the manner in which personal information is processed [12]. However, there have been concerns raised that the POPI Act is not being enforced, and also that enforcement of the POPI Act will require South African SMEs to change current strategies used to gather, save and distribute personal information [13]. Failure to comply with the POPI act could be result in payment of significant monetary amounts, jail time, closure of company etc. Lack of awareness is highlighted as one of the reasons for non-compliance as SMEs are unaware of the legal obligations imposed by the POPI act. In a survey conducted, 16% of SME's were not compliant with the POPI act, 56% were not aware of the conditions set out by the act, while 12% indicated as being in the process of complying [13]. According to an article by KPMG, most companies have some internal security strategies in place but has encouraged companies to embark on a gap analysis in terms of their readiness to the POPI act [12], [13].

3) Electronic Communication Act

The Electronic communication and Transaction Act is another information technology law passed in 2002 with a purpose set out to facilitate and regulate electronic communications and transactions, develop national e-strategy, promote universal access to electronic communication and transactions and the use of electronic transaction by SMMEs [14].

4) Cybercrimes and Cybersecurity Bill

This is the latest information technology bill published for review and public comment with an aim set out to describe types of cybercrime and offences, creation of a government and private sector CSIRTs, cybersecurity structures, and identification, regulation and compliance of national Information Infrastructure [9], [15].

B. Existing International Framework

1) National Institute of Standards & Technology (NIST)

The National Institute of Standards and Technology (NIST) is a division of the U.S Department of Commerce to apply technology, measurements & standards with the purpose of promoting innovation & industrial competitiveness [16]. The NIST wrote a cybersecurity framework which seeks to promote the wide adoption of practices to increase cybersecurity across all sectors and industrial types [17]. It contains practical guidelines on how to secure critical infrastructure called framework cores and provides a set of activities to achieve specific cybersecurity outcomes which include key functions such identify, protect, detect, respond and recover. Core activities can be used to align an organisations cybersecurity activities or initiatives with business requirements [18]. The United Nations Economic Commission for Africa [19] suggests the NIST framework provides a common language platform on how organisations can keep and secure online information. Further [20] that the NIST cybersecurity framework in conjunction with the NIST Risk management framework provide model approaches for assessing cyber risks and determining a budget for protecting IT systems and data which can be used as tools for

development of further suitable frameworks for organizational specifics.

VII. METHOD

Figure 1. Shows how the research will be conducted leading to the development of an e-retail framework.

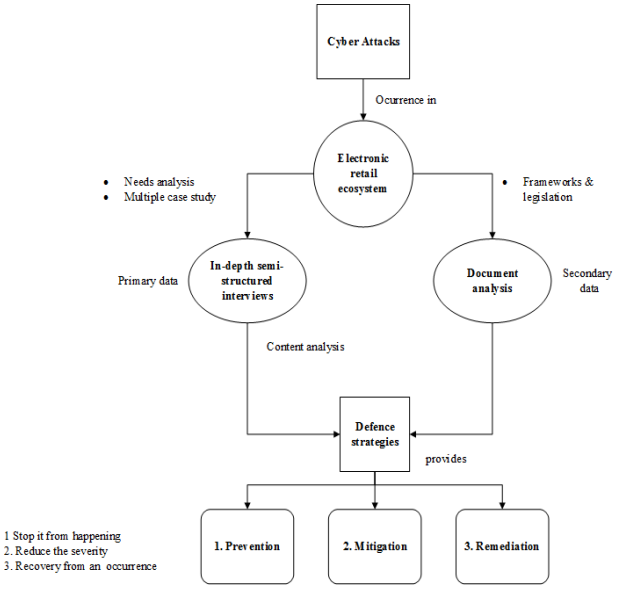

Figure 1: Steps through development of framework

Since this study seeks to understand the cybersecurity environment of e-retail in South Africawithin the retail sector, Figure 1 above is an indication of how the data will be collected leading to the development of a framework. By looking at the cyber-attacks currently happening in the e-retail sector; the research seeks to find out how these attacks can be stopped by looking at the current e-retail ecosystem**.** The empirical dataset consists of e-Retail store databases from any retail stores in South Africa. For this particular study, more than fifteen e-retail information security personnel from e-retail organizations across South Africa will be purposefully selected. These e-retail managers and database controllers will then be interviewed in the form of in-depth semi-structured interviews over a period of six months at any retail stores. Secondary data in the form of document analysis will be performed on local and international legislation using the NCPF as a theoretical lens. The sampling criteria used to select the participants will be purposive; which implies that participants will be hand-picked on the basis of their typicality and richness of information, with the intention that they would provide the necessary information to help guide this study. All, e-retail managers and database controllers will be asked to respond to an interview invitation. It is hoped that all e-retail managers and database controllers that will be purposefully selected will agree to the request to participate in the study. See Table 2 above. Using the NCPF to establish an e-retail framework that brings together findings from Laws, bills, acts and e-retail needs analysis. After findings from Laws, bills, acts and e-retail needs analysis have been established, the study seeks to develop an e-retail framework that will provide defense strategies against cyber-attacks to small scale e-retail organizations in South Africa. The framework aims to provide this defensive mechanism in the form of three strategies:

- Prevention: this will entail the necessary safe guards that e-retail organization should have in place to prevent the occurrence of cyberattacks as shown in the ecosystem above.
- Mitigation: in the event an e-retail organization has become a victim of any of the attacks above, what should be done to minimize the crippling effects of cyberattacks on the business. In other words, what is required to reduce the severity of such an attack.
- Remediation: how does an e-retail organization recover from the cyberattack. This will deal with recovery process.

VIII. CONCLUSION

In conclusion, this review is intended to offer and/or inform the creation of policy for cyber-securing e-Retail organizations in South Africa and to provide the parameters through which current legislation on cybersecurity can be made relevant to e-Retailers in terms of compliance, technology and security. Little evidence of frameworks customized for e-retail exists and evidence suggests a number of these frameworks apparently do not appropriately address cybersecurity concerns within the small to medium enterprise e-Retail context. Unlike large businesses with dedicated IT resources, small to medium enterprise businesses often lack the skills, resources, and infrastructure to tackle cybercrime and even to conduct security assessment. Small to medium enterprise businesses frequently fail to deploy comprehensive and effective security policies. Because of ongoing challenges, cybercriminals increasingly target small instead of large businesses for identity theft, phishing, credit cards and bank account information. Therefore, there is a need for a cybersecurity guideline to enable small to medium enterprises mitigate against cyberattacks. Furthermore, it will serve as basis for further research into the security of e-Retailers and will support the National cybersecurity plan of South Africa in its entirety.

REFERENCES

[1] L. Smedley, Virtual Entrepreneurship creating & operating a Home-based online business, Academic e. 2014.

[2] B. Von Solms, “Improving South Africa’s Cyber Security by cyber securing its small companies,” 2015 IST-Africa Conf. IST-Africa 2015, pp. 1–8, 2015.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[4] M. Mohanraj and M. Sakthivel, Customer Perception about Online Shopping, 1st ed. EduPedia Publications, 2016.

[5] Deloitte, “Cyber risk in retail Protecting the retail business to secure tomorrow’s growth,” 2015.

[6] R. Taylor, E. Fritsch, and J. Liederbach, Digital Crime and Digital Terrorism, 3rd ed. New Jersey: Prentice Hall Press, 2014.

[7] PriceWatersHousecoopers, “Why you should adopt the NIST CYbersecurity Framework,” 2014.

[8] D. Bessette, J. LeClair, R. Sylvertooth, and S. Burton, “Communication, Technology, and Cyber Crime in Sub-Saharan Africa,” in New Threats and Countermeasures in Digital and Cyber Terrorism, D. Maurice, Ed. IGI Global, 2015.

[9] Price Waterhouse Coopers, “South African organisations report the highest rate of economic crime in the world,” 2016.

[10] South African Government Gazette, The National Cybersecurity Policy Framework, no. 39475. 2015, pp. 66–95.

[11] D. Craigen, N. Diakun-Thibault, and R. Purse, “Defining cybersecurity,” 2014.

[12] D. Korff, “Cyber Security Definitions – a selection (US) National Initiative for Cybersecurity Education (NICE):,” 2015.

[13] G. Sarah and R. Ford, “On the definition and classification of cybercrime,” J. Comput. Virol., vol. 2, no. 1, pp. 13–20, 2006.

[14] R. Anderson et al., “Measuring the Cost of Cybercrime,” Work. Econ. Inf. Secur., pp. 1–31, 2013.

[15] F. Parodi, “The Concept of Cybercrime and Online Threats Analysis,” Int. J. Inf. Secur., vol. 2, p. 59, 2013.

[16] R. Rust and K. Lemon, “E-Service and the Consumer,” Int. J. Electron. Commer., vol. 5, no. 3, pp. 85–101, 2014.

[17] K. Kim, I. J. Kim, and J. Lim, “National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment,” J. Supercomput., vol. 73, no. 3, pp. 1140–1151, 2017.

[18] V. Misra and K. Mishra, “ACCEPTABILITY OF E-COMMERCE AMONG INDIAN CONSUMERS,” Int. J. Entrep. Dev. Stud., vol. 2, no. 1, pp. 1–10, 2014.

[19] United Nations Economic Commission for Africa, “Tackling the challenges of cybersecurity in Africa,” Policy brief, no. 8, pp. 1–6, 2014.

[20] Mastercard, “Online Shopping Security in the Spotlight – MasterCard Survey,” 2014.

[21] P. Kigen, C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi, and B. Shiyayo, “Kenya Cyber Security Report 2014 Rethinking Cyber Security - “An Integrated Approach: Processes, Intelligence and Monitoring,” 2014.

[22] J. Park, D. Cho, J. Kyu, and Lee Byungtae, “Economics of Cybercrime: The Role of Broadband and Socioeconomic Status,” 2017.

[23] D. Kim, D. Ferrin, and R. Rao, “Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration,” J. Inf. Syst. Res., vol. 20, no. 2, pp. 237–257, 2009.

[24] E. Yıldırım, “The Effects of User Comments on e-Trust: An Application on Consumer Electronics,” J. Econ. Bus. Manag., vol. 1, no. 4, pp. 360–364, 2013.

[25] D. Wall, Cybercrime: The Transformation of Crime in the Information Age. Polity, 2007.

[26] K. K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” Comput. Secur., vol. 30, no. 8, pp. 719–731, 2011.

[27] L. Harris and C. Dennis, Marketing the e-Business, 2nd ed. Routledge: Taylor & Francis, 2007.

[28] C. Ammni, Global Consumer Behavior. John Wiley & Sons, 2013.

[29] Department of Communications Telecommunications and Postal Services, “Presentation on E-Commerce , Cybercrime , and Cybersecurity in the Republic of South Africa,” 2013.

[30] F. Mohideen, “The Cybersecurity State of our Nation: A Critique of South Africa’s Stance on Cybersecurity in Respect of the Protection of Critical Information Infrastructure,” in 11th International Conference on Cyber Warfare and Security: ICCWS2016, 2016.

[31] J. Jansen van Vuuren, M. M. Grobler, L. Leenen, K. F. P. Chan, and Z. C. Khan, “Morphological Ontology Design Engineering: A Methodology to Modell III - Structured Problems,” in Mixed Methods Research for Improved Scientific Study, M. L. Baran, Ed. IGI Global, 2016, pp. 262–272.

[32] J. Jansen van Vuuren, L. Leenen, J. Phahlamohlaka, and Z. Jannie, “Development of a South African Cybersecurity Policy Implementation Framework,” Proc. 8th Int. Conf. Inf. Warf. Secur., 2013.

[33] South African Government Gazette, South Africa Protection Personal information Act, 2013, no. 10505. 2013, pp. 1–148.

[34] Botha, M. Eloff, and I. Swart, “Evaluation of online resources on the implementation of the protection of personal information act in south africa,” in 10th International Conference on Cyber Warfare and Security: ICCWS2015, 2015, p. 39.

[35] J. Botha, M. . Eloff, and I. Swart, “The Effects of the PoPI Act on small and medium enterprises in South Africa,” IEEE, pp. 1–8, 2015.

[36] Government Gazette, Electronic Communication and Transactions Act, vol. 446, no. 49. 2002.

[37] Department of Justice, Cyber Crime and Cybersecurity Bill. 2015, p. 128.

[38] L. Shen, “The NIST cybersecurity framework: Overview and potential impacts,” Scitech Lawyer, vol. 10, no. 4, p. 16, 2014.

[39] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” Natl. Inst. S, pp. 1–41, 2014.

[40] L. Shen, “The NIST Cybersecurity Framework: Overveiw and Potential Impacts,” Scitech Lawyer, vol. 10, no. 4, pp. 16–19, 2014.

[41] M. Scofield, “Benefiting from the NIST Cybersecurity Framework,” Information and Management, p. 25, 2016.

[42] E. D. Perakslis and M. Stanley, “A Cybersecurity Primer for Translational Research,” Sci. Transl. Med., vol. 8, no. 322, pp. 2–322, 2016.