Aug 25th, 11:45 AM - 12:10 PM

Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa

Caitlyn Murphy
University of Cape Town, mrpcai003@myuct.ac.za

Chimwemwe Queen Mtegha
University of Cape Town, mtgchi003@myuct.ac.za

Wallace Chigona
University of Cape Town, wallace.chigona@uct.ac.za

Teofelus Tonateni Tuyeni
University of Cape Town, tyntco002@myuct.ac.za

Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa

Caitlyn Murphy, University of Cape Town, South Africa, mrpcai003@myuct.ac.za

Chimwemwe Queen Mtegha, University of Cape Town, South Africa and Malawi University of Science and Technology, Malawi, mtgchi003@myuct.ac.za

Wallace Chigona, University of Cape Town, South Africa, wallace.chigona@uct.ac.za

Teofelus Tonateni Tuyeni, University of Cape Town, South Africa, tyntco002@myuct.ac.za

ABSTRACT

Technological advancements enable Small, Micro and Medium Enterprises (SMMEs) to increase business value and gain a competitive advantage. However, despite the myriad benefits of Information and Communication Technologies (ICTs), they have ushered in cyber threats. Cyberattacks have become more prevalent, especially in developing countries. As a result, most SMMEs in developing countries face challenges securing their digital environment. Governments worldwide have developed a National Cybersecurity Policy to protect their citizens, businesses and critical information infrastructure from cyberattacks. However, compliance with cybersecurity policy remains a challenge in many developing countries, especially among SMMEs. The study investigated the factors affecting compliance with the National Cybersecurity Policy by SMMEs in developing countries. This will aid policymakers in formulating National Cybersecurity Policies and providing an enabling environment for effective compliance by SMMEs in developing countries. We employed a qualitative approach using semi-structured interviews as a means of data collection. The sample for the study was 20 SMMEs in South Africa and was purposively selected. The findings showed that lack of awareness of the National Cybersecurity Policy, lack of understanding of the policy, resource constraints and lack of perceived benefits affect how SMMEs comply with the National Cybersecurity Policy.

Keywords

Cybersecurity, compliance, National Cybersecurity Policy, SMMEs, developing countries, South Africa.

INTRODUCTION

Small, Medium and Micro Enterprises (SMMEs) contribute significantly to a country's economic growth and development (Bhorat et al., 2018). It is reported that small enterprises in South Africa contribute around 35% of the Gross Domestic Product (GDP) (ILDP, 2014). The adoption of technology has proven beneficial for SMMEs. It increases efficiency by reducing production costs, increasing the value of goods and services, enhancing business procedures, and giving companies a competitive advantage (Afolayan & de la Harpe, 2020). However, the increase in technology adoption has led to many vulnerabilities. Unlike large businesses, SMMEs face several challenges in providing an enabling environment for their businesses due to limited access to financial resources and technical capabilities (Bada & Nurse, 2019; Kabanda et al., 2018; Selznick & LaMacchia, 2017). Interpol (2021) reported that over 90% of businesses in the African continent, mostly SMMEs, operate without cybersecurity measures (Interpol, 2021). As a result, they are at greater risk of cyberattacks, with more devastating consequences (Selznick & LaMacchia, 2017; Yudhiyati et al., 2021). Cybersecurity measures protect ICTs against malicious online actors (Bossong & Wagner, 2017). This is attained through developing and implementing cybersecurity measures such as the Cybersecurity Policies and Strategies. South Africa has the third-highest cybercrime globally (Hubbard, 2019). In addition, more than 8 million South Africans have experienced cybercrime (eNCA, 2016). This is a significant concern for the country's economy, as SMMEs make up 95% of the businesses and contribute to 60% of employment in the country (Dladla, 2021). In 2019, the number of registered SMMEs in the country was estimated to be over 787,300 (Moyo & Loock, 2021).

Governments worldwide strive to provide a secure environment for their citizens. Often, this is achieved through a National Cybersecurity Policy (Teoh & Mahmood, 2017). A National Cybersecurity Policy is a roadmap for governments to protect and secure their citizens and critical infrastructure from cyberattacks (Sabillon et al., 2016). A poor or non-existent National Cybersecurity Policy can be crippling to a nation and its economy (Rajasekharaiah et al., 2020). The terms" National Cybersecurity Policy" and "National Cybersecurity Strategy" are sometimes used interchangeably. We posit that National Cybersecurity Policy and National Cybersecurity Strategy are the same since many countries can adopt either one. For example, the government of South Africa published the Cybersecurity Policy in 2010, and gazetted National Cybersecurity Policy Framework (NCPF) in 2015 (Gcaza & von Solms, 2017). NCPF notes the need to promote a cybersecurity culture and compliance with minimum security standards and promote cybersecurity measures (SA Government Gazette, 2015). In this study, we define compliance as the "degree to which an individual acts in accordance with prescribed rules or request made by people in authority" (Wong et al., 2022, p. 2). However, despite NCPF emphasising cultivating a cybersecurity culture and complying with minimal cybersecurity standards (Bote, 2019), there is no evidence of government action in that direction (Bote, 2019; Gcaza & von Solms, 2017). In addition, the government has primarily focused on compliance with cybersecurity policy and regulations in critical infrastructures and government institutions without putting in measures to ensure compliance in all sectors of the country (Malatji et al., 2021). Furthermore, despite the adoption of NCPF in South Africa, the country is still experiencing high cybercrimes (Lejaka et al., 2019).

Few studies have analysed the compliance of SMMEs with the National Cybersecurity Policy in developing countries (Kabanda et al., 2018). In addition, many cybersecurity policy compliance studies focus on large-scale businesses and critical infrastructures. We are arguing that SMMEs are different from large-scale businesses. The challenges facing SMMEs may not be applicable to large-scale organisations, it is crucial to ensure the continuation of business procedures in these SMMEs(Yeboah-Boateng & Essandoh, 2014). Therefore, the study seeks to answer the following question:

- ***What factors affect compliance with the National Cybersecurity Policy by SMMEs in South Africa?***

Answering this research question may aid future research in addressing the challenges experienced by SMMEs in developing countries in complying with the National Cybersecurity Policy. We purposively sampled 20 SMMEs from the retail industry in the city of Cape Town. Of the 20 SMMEs, 32 respondents participated in the study. The paper adds to knowledge as there is a scarcity of literature contributing to SMMEs' compliance with the National Cybersecurity Policy in developing countries. Further, the findings of this research may inform policymakers on

how to formulate policies and provide essential tools to enable SMMEs to protect themselves from cyberattacks. In the paper, we used an inductive approach.

LITERATURE REVIEW

An Overview of SMMEs

The differentiation between SMMEs and SMEs (Small Medium Enterprises) varies from country to country. However, the leading indicators are the contribution to GDP and the number of employees. In the context of South Africa, the National Small Business Act of 1996 categorises small businesses into various groups, namely, survivalist, micro, very small, small and medium, hence the term "SMME"(ILDP, 2014). However, according to the literature, in South Africa, SME and SMME are used interchangeably (ILDP, 2014). **Table 1** summarises the World Bank's SMME indicators, including the number of employees, the total assets, and the total annual sales.

Enterprise Indicators (2/3)	**Number of Employees**	**Total assets**	**Total annual sales**
Medium	>50; ≤300	>$3,000,000; ≤$15,000,000	>$3,000,000; ≤$15,000,000
Small	>10; ≤50	>$100,000; ≤$3,000,000	>$100,000; ≤$3,000,000
Micro	<10	≤$100,000	≤$100,000

Table 1. SMME indicator using World Bank standards (Berisha, 2015)

SMMEs are among the most significant contributors to a country's Gross Domestic Product (GDP) and job creation (Keskġn et al., 2010). In addition, they are an essential source of income generation for many households in developing countries (Isaga et al., 2015). As a result, most governments in developing countries are becoming aware of the importance of SMMEs in their economic growth(Nieuwenhuizen, 2019). This has led to governments enhancing the adoption of ICTs for SMMEs to gain a competitive advantage through online digital government support systems (Malik et al., 2019; Osman et al., 2019). ICTs have the potential to transform business operations through access to and exchange of information (Malik et al., 2019).

The SMMEs in South Africa contribute significantly to the economy of the country. They contribute 60% to employment and 50% to the National Gross Domestic Product (Bhorat et al., 2018). However, according to prior literature, 75% of SMMEs fail to survive in the first three years (Ajibade & Khayundi, 2017). One of the contributing factors to the high failure rate is the high crime levels (Botha et al., 2021). The increase in cybercrime in the country may also contribute to the higher percentage of failure rates among SMMEs (Kelebetse et al., 2019). **Table 2** summarises the composition of SMMEs in the country.

Industry	**Estimated contribution to national GDP**	**Estimated employment opportunities created**
Agriculture	Between 0.91% and 1.3%	± 3.08%
Mining and quarrying	Between 2.82% and 4.03%	± 1.59%
Manufacturing	Between 4.74% and 6.77%	± 6.41%
Electricity, gas and water	Between 0.81% and 1.16%	± 0.49%
Construction	Between 1.32% and 1.89%	± 5.38%
Retail, wholesale and catering	Between 2.82% and 4.03%	± 12.05%

Transportation storage and communication	Between 3.34% and 4.78%	± 3.50%
Finance and business services	Between 7.84% and 11.20%	± 9.48%
Community and the social and personal service	Between 7.95% and 11.36%	± 13.16%

Table 2. SMME composition in South Africa (Bruwer et al., 2020)

SMMEs and ICTs

With the advancement of technology, SMMEs are continuously relying on ICTs to enhance operational efficiency (Lejaka et al., 2019). Many SMMEs are adoption ICTs to gain a competitive advantage (Malik et al., 2019; Osman et al., 2019). ICTs have the potential to transform business operations through access to and exchange of information (Malik et al., 2019). In addition, they allow SMMEs to nurture a relationship of trust with their customers, enhance their professionalism, encourage open communications with customers, and improve customer service (Malik et al., 2019; Remmele & Peichl, 2021). Furthermore, ICTs have enhanced SMMEs' efficiency and effectiveness in service delivery to their consumers (Remmele & Peichl, 2021). The most predominantly technologies SMMEs use include mobile phones, computers, laptops, etc. (Walaza et al., 2020)

Many SMMEs in developing countries face challenges with adopting ICTs (Eze et al., 2019). However, the outbreak of the COVID-19 pandemic has changed the narrative as many SMMEs in developing countries were forced to adapt to online strategies to ensure the continuity of their businesses (Bruwer et al., 2020; Indriastuti & Fuad, 2020).

South Africa is one of the leading countries in the African continent in ICT adoption (Akande et al., 2014). The increase in ICT usage in the country was attributed to the presence of multinational companies (e.g., Huawei, Amazon, etc.) that invested in the country (Walaza et al., 2020). This has also led the ICT sector in the country to implement online tools, such as online trading and e-commerce. As a result, many SMMEs use online tools to enhance their businesses to gain a competitive advantage.

SMMEs and Cybersecurity

However, despite the benefits of ICTs, their adoption by SMMEs has coupled with cyber threats globally (Remmele & Peichl, 2021). SMMEs are concerned with taking advantage of the new opportunities that technologies offer them without considering the security implications (Abubakar et al., 2014). Unfortunately, SMMEs in developing countries are at a higher risk of cyberattacks due to a lack of necessary resources to implement cybersecurity measures (Alahmari & Duncan, 2020; Yudhiyati et al., 2021). In addition, the lack of cybersecurity policies, legislation, and knowledge in developing countries is a cause of concern for SMMEs (Botha et al., 2021). In 2015, SMMEs experienced 43% of cyberattacks (Yudhiyati et al., 2021).

Cyberattacks are increasing rapidly in Africa, targeting organisations of all sizes, including SMMEs (Lejaka et al., 2019). However, SMMEs fail to prioritise cybersecurity due to a lack of funding and support (Kabanda et al., 2018; Yudhiyati et al., 2021). As such, they have become the most prominent targets of cybercrime (Jideani et al., 2018; Solms & Kritzinger, 2011). Therefore, there is need to create cybersecurity awareness among SMMEs to adopt cybersecurity measures (Renaud & Ophoff, 2021). This is evidence of the importance of addressing cybersecurity within SMMEs, especially in developing countries in Africa. SMMEs should comply with minimal cybersecurity measures to the same extent as any large organisation. Large organisations' data, including SMMEs, must be protected against cyber threats. In addition, the organisation needs uninterrupted access to their resources to ensure business continuity (Buch et al., 2017). Therefore, there is a need for SMMEs to implement cybersecurity measures to avoid business disruption, resulting in a loss of profit, customers and trust (Taylor et al., 2014; Uwakweh, 2020). Some of the cyberattacks SMMEs experience include malware, Denial of Services (DoS), intrusion, ransomware and email spam (Ncubukezi et al., 2020). In addition, there is a need for tailored cybersecurity awareness-raising programs targeting SMMEs. Developed countries have created these tailored initiatives to protect SMMEs from

cyberattacks in their countries. However, many developing countries lag in developing a cybersecurity culture for their citizens.

National Cybersecurity Policy

A National Cybersecurity Policy defines what should be protected, how it should be protected, and defines citizens' rights and how they should enforce this cybersecurity policy (Sabillon et al., 2016). In most countries worldwide, cybersecurity is considered a matter of national importance (Gcaza & von Solms, 2017). The lack of a cybersecurity policy can be detrimental to a country's economy and the safety of its internet users in many activities. In addition, daily functions are dependent on cyberspace. For a country to thrive in the digital age, it must develop strategies for its citizens' protection within cyberspace. As digital capabilities continue to advance, so are the cyber threats (Teoh & Mahmood, 2017). (Sabillon et al., 2016). The best way to tackle cybersecurity is to address both the technological aspects of cybersecurity and the human elements (Pfleeger & Caputo, 2012), as humans are seen as the biggest weakness in cybersecurity (Gcaza & von Solms, 2017). Therefore, National Cybersecurity Policies address the need to develop a cybersecurity culture to ensure that internet users cultivate cybersecurity practices and behaviours (Gcaza et al., 2015).

Most National Cybersecurity Policies indicate the need to cultivate a cybersecurity culture to encourage organisations and citizens to enhance their cybersecurity behaviour. Cybersecurity culture aims to create and promote a way to behave daily that meets cybersecurity standards (Gcaza et al., 2015). Scholars have argued that if cybersecurity culture is implemented effectively, it can address the human elements and minimise cybercrime. Strategies by which governments and businesses can cultivate cybersecurity culture include: developing cybersecurity education and awareness, research and development, cybersecurity measures, and capacity development (Gcaza et al., 2015; Klimburg & Zylberberg, 2015) .

National Cybersecurity Policy Framework of South Africa

The South African cabinet approved the NCPF in 2012 and gazetted it in 2015. The aim of the policy is to, inter alia, amongst others, protect national Critical Information Infrastructure, promotion of a cybersecurity culture and compliance with standards and facilitate collaboration on cybersecurity incidents between the government, industry, and civil society(Malatji et al., 2021; Parliament of the Republic of South Africa, 2017). The approval of NCPF paved the way for the development of various cybersecurity legislation, policies and strategies.

Below are the objectives that NCPF addresses (SA Government Gazette, 2015, p. 80).

- Centralise coordination of Cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies in support of Cybersecurity in order to combat cybercrime, address national security imperatives and to enhance the information society and knowledge based economy;
- Foster cooperation and coordination between Government, the private sector and civil society by stimulating and fostering a strong interplay between policy, legislation, societal acceptance and technology;
- Promote international cooperation;
- Develop requisite skills, research and development capacity;
- Promote a culture of Cybersecurity; and
- Promote compliance with appropriate technical and operational Cybersecurity standards.

SMMEs' Compliance with National Cybersecurity Policy

Compliance or adherence to the regulations is mainly affected by the individuals' motivation to conform and the cost of compliance(Bulgurcu et al., 2010; Wong et al., 2022). The benefits of complying with cybersecurity policies include protecting the organisations' information and technology resources and leveraging human capital (Bulgurcu et al., 2010).

Despite the benefits of the National Cybersecurity Policy's for the country, compliance in many organisations remains challenging, especially in SMMEs (Coertze & von Solms, 2013). Main challenges affecting cybersecurity are the human actors and their behaviours (Chowdhury et al., 2020; Zimmermann & Renaud, 2019) ; 50% of cyber incidences are attributed by human behaviours(Pham, 2017). The human behaviours create more vulnerabilities and affect overall cybersecurity therefore affecting cybersecurity policy compliance. (Barry et al., 2021; Hina et al., 2019). (Jansen Van Vuuren et al., 2014)

Institutional governance is another factor affecting compliance (Barry et al., 2021; Hina et al., 2019). Unfortunately, many developing countries' institutional context does not provide an enabling environment for promoting compliance, specifically at the national level. As a result, many SMMEs in developing countries establish incentives to ensure their employees' compliance by drafting internal security policies. In addition, when policies are implemented at the national level, adequate structures are lacking to monitor their implementation and impact (Jansen Van Vuuren et al., 2014).

RESEARCH METHODOLOGY

This study adopted an interpretive approach since we were interested in exploring the factors affecting SMMEs in complying with the National Cybersecurity Policy. Due to the interpretive and exploratory nature of the study, the qualitative method was applied. A qualitative approach enabled a more profound understanding of the underlying factors within the social and cultural context of the investigated phenomenon. We employed semi-structured interviews to gain in-depth knowledge of the factors affecting compliance among SMMEs in developing countries. The interview questions also sought to understand the respondent's practice with regard to cybersecurity measures. Since the study is exploratory, we deemed it appropriate to adopt an inductive approach to theory.

We used purposive sampling to select the appropriate SMMEs. The study respondents were drawn from 20 SMMEs in the retail industry from Cape Town. Our choice of Cape Town was mainly based on convenience. Further, Cape Town is part of the Western Cape Province, a province with the third a highest number of SMMEs in the country; after Gauteng and KwaZulu-Natal provinces and with the highest SMME growth rate (Kavese, 2021). In addition, the retail industry in South Africa experiences high cybercrime rates in the country (Jideani et al., 2018; von Solms, 2015). Furthermore, since the SMMEs in the retail industry are among the top five highest contributors to the GDP, they are more vulnerable to cybercrime. The SMMEs in the sample were categorised into micro, small, and macro (Recall Table 1). The micro SMMEs were coded SMME_B_X, the small SMME_C_X, and the macro SMME_D_X. The respondents' level of cybersecurity knowledge ranged from low to high. **Table 3** summarises the demographic profile of the respondents from the SMMEs in the study.

Demographic Characteristics		**Number of Respondents**
***Age Range*:**		
	56 years above	5
	46-55 years	7
	36-45 years	8
	26-35 years	6
	18-25 years	6
Respondents Positions:		
	Head of IT department	7

	Sales representatives	8
	Employees from the IT department	5
	Cybersecurity specialist	4
	Chief Operating Officer	8

Table 3. Demographic profile of respondents

The interviews were audio recorded and transcribed. Finally, the data collected was analysed using thematic analysis (Braun & Clarke, 2006).

We obtained ethics approval from the University of Cape Town to conduct the study. Participation in the study was voluntary, and we maintained the confidentiality of the participants. We kept the recordings in a secure location to ensure safety and privacy.

EMPIRICAL ANALYSIS AND DISCUSSIONS

The study found that the following factors affected SMMEs in complying with NCPF: (i) awareness of the policy, (ii) understanding of the policy, (iii) perceived benefit, and (iv) resource availability. The findings are summarised in **Figure 1**. The factors are discussed in detail in the subsequent sections.

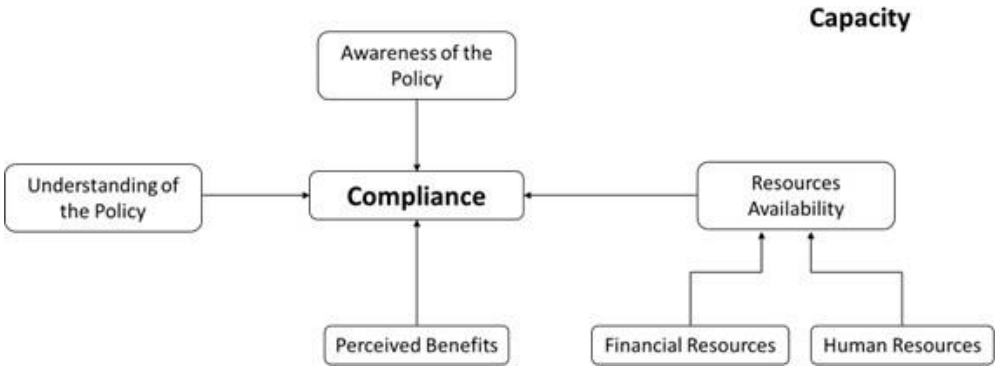

Figure 1. Conceptual Framework of Factors Affecting SMMEs to Complying

Awareness of the National Cybersecurity Policy Framework

The SMMEs lacked awareness of NCPF. Most SMMEs were unaware of the purpose of the framework. For example, SMME_B_15 indicated that it was their first time hearing about the policy. The only cybersecurity-related policy they had heard of was the POPI Act through media outlets. A few SMMEs that were aware of the policy were unaware of the cybersecurity measures they needed to implement.

> *"We are aware of the NCPF, but we are not aware of the cybersecurity standards that the NCPF states. Furthermore, we are unsure whether we meet the standards expected by the policy."* (SMME_B_8)

This finding is supported by literature that noted that NCPF did not explicate how best people could protect themselves from cybercrime (Bote, 2019). In addition, NCPF did not provide the minimal cybersecurity measures needed in small businesses and large organisations. Instead, it merely stated a need to "promote a cybersecurity culture and demand compliance with minimum security standards" (SA Government Gazette, 2015, p. 77). The lack of awareness of NCPF contributed to inadequacy in implementing the cybersecurity measures and, therefore, affected their compliance.

> *"Compliance is critical to us, but we need to know about the NCPF. We have never come across any standards to adhere to, but we are always happy to make changes where need be."* (SMME_B_1).

This finding is supported by existing literature that SMMEs lack awareness of cybersecurity measures and therefore are not compliant with them (Donalds & Osei-Bryson, 2020; Wong et al., 2022). However, despite being unaware of NCPF, eight out of the 32 respondents specified that they had implemented cybersecurity measures to secure their business environment in their organisations. For example, SMME_C_7 highlighted that their organisation installed antiviruses and conducted regular updates. In addition, they had a firewall and two-factor authentication. These SMMEs could have learnt the security practices from other sources. Conversely, it is a common practice in many countries that after a policy has been developed and approved, the leading government agencies have to create awareness for the implementers. In some instances, they are involved or consulted during the policy formulation which enhances their level of awareness.

Understanding of the National Cybersecurity Policy Framework

The terms awareness and understanding are closely related however, they are different. term understanding differs from the term awareness. Understanding is defined as knowing what to do and how to do it (Watson, 2002; Zwilling et al., 2022). The understanding of some of the cybersecurity concepts in the NCPF. This may have affected the implementation of the NCPF objectives. This finding corroborates with Dlamini et al. (2012), Von Solms (2015) and Jideani et al. (2018), who posit that SMMEs lack knowledge of cybersecurity. For instance, when we asked some of the respondents to explain what they thought cybersecurity culture was, they did not fully explain the concept.

> *"I understand cybersecurity culture as an idea of protecting data*." (SMME_C_20).
>
> *"I am guessing that cybersecurity culture is a protocol put in place to protect company data."* (SMME_C_24).

Only one respondent who was a cybersecurity specialist elaborated what cybersecurity culture meant:

> *"I define cybersecurity culture as how one should behave when conducting themselves online. This implies being aware of the cyber-threats and knowing how to mitigate through one's behaviour."* (SMME_D_29)

The empirical findings implied that one must understand the policy to be able to comply with it. Therefore, we recommend comprehensive awareness-raising initiatives for cybersecurity policies to sensitize and enhance the understanding of implementers, specifically SMMEs. Furthermore, the policies may be simplified to adopt vocabulary which is easy to understand for non-technical people. The study further found that the roles and responsibilities of SMMEs in the NCPF are not clearly stated. This makes it difficult for SMMEs to comply with the NCPF.

As stated in the preceding section, awareness of the existence of the NCPF and cybersecurity risks is critical to compliance. Therefore, a lack of awareness contributes to a lack of understanding, which in turn affected how the SMMEs complied with the NCPF.

Perceived Benefits of the National Cybersecurity Policy Framework

The findings from the study showed that SMMEs did not perceive the benefits of complying with the NCPF. Many SMMEs felt that since their organisation was small and did not have any critical information to be protected, there was no need to comply.

> *"Our organisation is small and does not need to comply with minimal cybersecurity standards; for small businesses, serious cybersecurity issues do not threaten the majority of them."* (SMME_B_1).

In addition, the SMMEs which "*had never experienced any cyber-attacks since their operation*" did not see the need to comply with the NCPF. Literature also supports the finding as many SMMEs do not know and perceive the importance of securing their digital environments (Kabanda et al., 2018). The lack of understanding of the policy could have contributed to the failure to perceive the benefits.

> *"Since the operation of our business, we usually operate online. Therefore, we are aware of the NCPF, but we do not understand the objectives of the NCPF and its benefits in implementing the measures."* (SMME_B_9)

According to the findings, there was a lack of government incentives in promoting SMMEs to comply with the NCPF. As a result, SMMEs did not perceive the benefits NCPF yielded for their organisations, which affected their overall compliance. This finding is consistent with Li et al., (2010) that perceived benefits effect compliance to security policies. SMMEs are profit driven entities and therefore, are more likely to comply with security policies when there are potential benefits.

Resource Availability

Availability of resources is twofold: (i) financial resources for compliances and (ii) skilled human resources. The SMMEs that were aware of the NCPF did not allocate sufficient financial resources or funding toward cybersecurity matters. Second, SMMEs did not have the human resource to assist in securing their digital environments. The SMMEs did not allocate the resources mainly because they did not have enough resources. However, others did not allocate the resources towards cybersecurity because they did not perceive cybersecurity as critical. For a budget to be allocated to cybersecurity, the SMMEs must reflect it in their strategic planning. They could only do that if they perceived cybersecurity as critical. In addition, since they lacked resources, most SMMEs relied on third-party security measures.

> *"We are a small business, and as of now, all we are trying to target is building our client base. So normally, we use social media as our platform, which already has the two-factor authentication in place, so I do not see the need for a budget."* (SMME_B_3)

This finding is in line with the Interpol (2021) report, which stated that most African companies do not implement security standards and use free and pirated software due to a lack of resources. In addition, SMMEs had a perceived trust in social media cybersecurity standards so much that they did not budget for any cybersecurity measures in their businesses.

> *"For small businesses, the majority of us are not threatened by severe cybersecurity issues. The most common occurrence relating to this issue is Instagram hacking for which two-factor authentication has been created as a solution."* (SMME_C_14).

Human resources also contributed to the lack of compliance among SMMEs in developing countries.

> *"We are a small business and a small team trying to get everything we need. Unfortunately, we don't have funds to employ an additional administrator to handle cybersecurity issues in our organisation."* (SMME_C_2).

CONCLUSION

Using the context of South Africa, this study explored the factors affecting SMMEs in complying with the National Cybersecurity Policy. Undoubtedly the National Cybersecurity Policy enables the government to protect its citizens from cyber-attacks. However, developing countries need to enforce compliance to leverage cyber resilience. SMMEs are the most crucial sector of any country as they provide an economic transformation. The study contributes to literature on National Cybersecurity Policy compliance by exploring the obstacles SMMEs face in complying with the policy. The barriers include a lack of awareness and understanding of the NCPF. The possible low levels of awareness of the NCPF may suggest that the government did not prioritise awareness-raising implementation strategies among SMMEs in South Africa. A lack of cybersecurity knowledge contributed to the lack of awareness and understanding of the NCPF. Some respondents, for instance, were aware of the POPI Act, but were not aware of the NCPF; this could have been a result of the wide media coverage of the former. Generally,

there is a need to raise what cybersecurity entails for SMMEs to understand the policy itself. Furthermore, the lack of perceived benefits and resources also affected the compliance factor among SMMEs.

It is imperative for governments to develop compliance strategies for SMMEs. Developing countries can achieve this by clarifying the National Cybersecurity Policy and the role of SMMEs in assisting in the fight against cybercrimes. In addition, guidelines need to be explained either in the National Cybersecurity Policy or a separate document on the minimally acceptable cybersecurity standards that SMMEs need to follow as a guideline. In addition, there is a need for public and private sectors in the countries to develop cybersecurity awareness-raising programmes tailored for SMMEs. Furthermore, there is a need to assign a government entity specifically for SMMEs to ensure they have enough resources to build capacity in the country.

We acknowledge that the sample drawn for the study was limited to the city of Cape Town. This may have implications on the findings and limit their generalisability to SMMEs based in other parts of the country. In addition, time was a limiting factor in this research. Therefore, the sample was kept small enough to manage in the timeframe. We recommend that future research represent SMMEs from a range of cities in South Africa to enhance generalisability.

REFERENCES

1. Abubakar, A. D., Bass, J. M., & Allison, I. (2014). Cloud Computing: Adoption Issues for Sub-Saharan African SMES. *The Electronic Journal of Information Systems in Developing Countries* , *62*(1), 1–17. www.ejisdc.org
2. Afolayan, A. O., & de la Harpe, A. C. (2020). The role of evaluation in SMMEs' strategic decision-making on new technology adoption. *Technology Analysis and Strategic Management*, *32*(6), 697–710. https://doi.org/10.1080/09537325.2019.1702637
3. Ajibade, P., & Khayundi, F. (2017). The role of records management in small micro and medium enterprises (SMMEs) in South Africa and its implications for business sustainability. *African Journal of Library, Archives & Information Science*, *27*(2), 175–188. https://www.researchgate.net/publication/322340131
4. Akande, A. O., van Belle, J.-P. W., & van Belle, J.-P. (2014). *ICT Adoption in South Africa-Opportunities, Challenges and Implications for national development*. https://www.researchgate.net/publication/285593353
5. Alahmari, A., & Duncan, B. (2020, June 1). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CyberSA49311.2020.9139638
6. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium- sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018- 0080
7. Barry, T., Jona, J., & Soderstrom, N. (2021). *The impact of country institutional factors on Firm Disclosure: Cybersecurity disclosures in Chinese cross-listed firms.*
8. Berisha, G. (2015). Defining Small and Medium Enterprises: a critical review. *Academic Journal of Business, Administration, Law and Social Sciences*, *1*(1), 17–28. www.iipccl.org
9. Bhorat, Haroon., Asmal, Zaakhir., Lilenstein, K., & van der Zee, K. (2018). *SMMEs in South Africa : Understanding the constraints on growth and performance*. Development Policy Research Unit.
10. Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3
11. Bote, D. (2019). *The South African National Cyber Security Policy Framework: A critical analysis*. North-West University. Botha, A., Smulders, S. A., Combrink, H. A., & Meiring, J. (2021). Challenges, barriers and policy development for South
12. African SMMEs–does size matter? *Development Southern Africa*, *38*(2), 153–174. https://doi.org/10.1080/0376835X.2020.1732872

13. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

14. Bruwer, J. P., Hattingh, C., & Perold, I. (2020). Probable measures to aid South African Small Medium and Micro Enterprises' sustainability, post-COVID-19: A literature review. *Post-COVID-19: A Literature Review (June 12, 2020) (2020)*.

15. Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of Cyber Security and Cybercrime. *STM Journals*, *4*(2), 18–23. https://www.researchgate.net/publication/327110771

16. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *Source: MIS Quarterly*, *34*(3), 523–548.

17. Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101963. https://doi.org/10.1016/j.cose.2020.101963

18. Coertze, J., & von Solms, R. (2013). A software gateway to affordable and effective Information Security Governance in SMMEs. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*. https://doi.org/10.1109/ISSA.2013.6641035

19. Dladla, L. G. (2021). The Economics of the Covid-19 Pandemic and its Effects on Small Businesses in South Africa. *Asian Journal of Economic and Finance* , *3*(1), 59–69. www.arfjournals.com

20. Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*. https://doi.org/10.1016/j.ijinfomgt.2019.102056

21. eNCA. (2016, July 16). *8.8 million South Africans hit by cyber crime*. https://www.enca.com/technology/88-million-south-africans-hit-by-cyber-crime

22. Eze, S. C., Chinedu-Eze, V. C., Bello, A. O., Inegbedion, H., Nwanji, T., & Asamu, F. (2019). Mobile marketing technology adoption in service SMEs: a multi-perspective framework. *Journal of Science and Technology Policy Management*, *10*(3), 569–596. https://doi.org/10.1108/JSTPM-11-2018-0105

23. Gcaza, N., & von Solms, R. (2017). A Strategy for A Cybersecurity Culture: A South African Perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(6), 1–17. www.ejisdc.org

24. Gcaza, N., von Solms, R., & van Vuuren, J. (2015). An Ontology for a National Cyber-Security Culture Environment. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, 1–10. https://www.researchgate.net/publication/306292545

25. Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, *87*. https://doi.org/10.1016/j.cose.2019.101594

26. Hubbard, J. (2019). SA business underplayingthe danger of cybercrime. *Finweek*, *2019*(4), 37–38. www.thecyberacademy.co.za

27. ILDP. (2014). *Informal Small Medium and Micro Enterprises (SMME) Retailers in South Africa*. https://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/financial+institutions/resources/msme-opportunity-south-africa

28. Indriastuti, M., & Fuad, K. (2020). Impact of covid-19 on digital transformation and sustainability in small and medium enterprises (smes): A conceptual framework. *Conference on Complex, Intelligent, and Software Intensive Systems*, 471–476.

29. Interpol. (2021). *African Cyberthreat Assessment Report*.

30. Jansen Van Vuuren, J. C., Leenen, L., & Zaaiman, J. J. (2014). Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa. *9th International Conference on Cyber Warfare and Security*, 107–115.

31. Jideani, P., Leenen, L., Alexander, B., & Barnes, J. (2018). Towards an Electronic retail cybersecurity framework. *2018 Conference on Information Communications Technology and Society* , 1–6.

32. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

33. Kavese, K. (2021). *PERFORMANCE AND DEVELOPMENTS OF SMMEs IN THE EASTERN CAPE*. https://www.ecsecc.org/datarepository/documents/smmes-ec-2020_t1R77.pdf

34. Kelebetse, O., Tangirala, S., Sethate, T., & Kuruba, G. (2019). Role of internal controls in business resilience and growth of small businesses in Gaborone. *Archives of Business Research*, *7*(10), 184–194. https://doi.org/10.14738/abr.710.7245

35. Klimburg, A., & Zylberberg, H. (2015). *Cyber Security Capacity Building: Developing Access*. https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf

36. Lejaka, T. K., da Veiga, A., & Loock, M. (2019, April 30). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. *2019 Conference on Information Communications Technology and Society, ICTAS 2019*. https://doi.org/10.1109/ICTAS.2019.8703609

37. Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability (Switzerland)*, *13*(1), 1–33. https://doi.org/10.3390/su13010291

38. Malik, J., Gandhi, R., Vishwavidyalaya, P., Malik, J. K., & Choudhury, S. (2019). *A Brief review on Cyber Crime-Growth and Evolution*. https://www.researchgate.net/publication/340756419

39. Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020, December 8). A Review of the Current Cyber Hygiene in Small and Medium- sized Businesses. *2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020*. https://doi.org/10.23919/ICITST51030.2020.9351339

40. Nieuwenhuizen, C. (2019). The effect of regulations and legislation on small, micro and medium enterprises in South Africa. *Development Southern Africa*, *36*(5), 666–677. https://doi.org/10.1080/0376835X.2019.1581053

41. Osman, M. A., Malanga, D. F., & Chigona, W. (2019). Realities of Microenterprises' ICT Use for Business Activities and for Acquring Online Government Support: A Study in Western Cape Province, South Africa. *The African Journal of Information and Communication*, *24*, 1–23. https://doi.org/10.23962/10539/28659

42. Parliament of the Republic of South Africa. (2017). *Department of Telecommunication and Postal Services: Cybersecurity*. https://static.pmg.org.za/170822Cybersecurity.pdf

43. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

44. Pham, H. T. (2017). Investigating the Impact of Lean Management on Innovation in Vietnamese SMEs. *International Business Research*, *10*(11), 1. https://doi.org/10.5539/ibr.v10n11p1

45. Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering*, *981*(2). https://doi.org/10.1088/1757-899X/981/2/022062

46. Remmele, B., & Peichl, J. (2021, August 17). Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro-And Small Enterprises. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469198

47. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 24–46. https://doi.org/10.1108/ocj-03-2021-0004

48. SA Government Gazette. (2015). *The National Cybersecurity Policy Framework (NCPF)*. https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

49. Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering (IJCSSE)*, *5*(5). www.IJCSSE.org

50. Selznick, L. F., & LaMacchia, C. (2017). Cybersecurity liability: How technically savvy can we expect small business owners to be. *J. Bus. & Tech. L.*, *13*, 217.

51. Solms, B. von, & Kritzinger, E. (2011). Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa–Has the CIIP and Cyber Security Rubicon Been Crossed? *International Conference on E-Infrastructure and e-Services for Developing Countries*, 116–124.

52. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

53. Teoh, C. S., & Mahmood, A. K. (2017, August 3). National cyber security strategies for digital economy. *International Conference on Research and Innovation in Information Systems, ICRIIS*. https://doi.org/10.1109/ICRIIS.2017.8002519

54. Uwakweh, O. (2020). *Cybersecurity in the Retail Industry: Third Party Implications*. University of Cincinnati.

55. von Solms, B. (2015, August 11). Improving South Africa's Cyber Security by cyber securing its small companies. *2015 IST- Africa Conference, IST-Africa 2015*. https://doi.org/10.1109/ISTAFRICA.2015.7190538

56. Walaza, M., Loock, M., & Kritzinger, E. (2020). A Framework to Enhance ICT Security Through Education, Training & Awareness (ETA) Programmes in South African Small, Medium and Micro-sized Enterprises (SMMEs): A Scoping Review. *Computer Science On-Line Conference*, 45–58.

57. Watson, A. (2002). *What does it mean to understand something and how do we know when it has happened?* http://www.pmtheta.com/uploads/4/7/7/8/47787337/what_does_it_mean_to_understand_something.pdf

58. Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*. https://doi.org/10.1016/j.ijinfomgt.2022.102520

59. Yeboah-Boateng, E. O., & Essandoh, K. A. (2014). Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. *International Journal of Emerging Science and Engineering*, *2*(4).

60. Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, *19*(4), 446–462. https://doi.org/10.1108/JICES-03-2021-0035

61. Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

62. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269