Information Security Framework Adoption for South African Small and Medium Enterprise

Michael N. Moeti(✉), Makhulu R. Langa, and Khuliso Sigama

Tshwane University of Technology, Polokwane 0699, South Africa
{moetimn,langarm,sigamak}@tut.ac.za

Abstract. The small and medium enterprises (SMEs) sector is the backbone of the economy, a big employment creator, poverty reducer and the main engine for economic growth. SMEs rely heavily on technology to conduct their business but are constraint by lack of information security knowledge to protect themselves against cyber-attacks that may render their business an easy prey. This paper investigates factors that may influence SMEs in South Africa in the adoption of a security framework. These factors were applied in the development of an information security adoption framework for SMEs. The study collected qualitative data by means of interviews. ISO/IEC 27002 information security framework formed the theoretical basis for this study. Thematic analysis was employed for analysis of the collected data. The results indicate that close to 90% of SMEs do not have security policies or a risk management strategy. The study identified new, important themes critical in the development of an information security adoption framework for SMEs: ISM Best Practices and technical security architecture. The study contributes a conceptual framework that illustrates how the identified themes relate to concepts essential to information security adoption among SMEs.

Keywords: SMEs · Security policy · Thematic analysis

1 Introduction

The consensus among policy makers, practitioners, and economists and business experts is that small and medium enterprises (SMEs) are drivers of economies globally (Shin and Hwang 2015; Sungkawati et al. 2021). The SME sector is akin to the backbone of the economy, a big employment creator, poverty reducer and constitutes the main 'engine' for economic growth (Lekhanya 2015; Lekhanya et al. 2017). These sways are true for both developed and developing countries. However, SMEs are also encountering competitive pressure fueled by globalization, compliance with legislation, resource scarcity, the explosion of knowledge pertaining to information management and an increase in market expansion due to emerging technologies and innovation (Lekhanya et al. 2017). Information technology (IT) is a critical organizational resource supporting the competitive strategy of the organization. ICT has become the driving force behind businesses and is changing the way businesses operate. In today's high-speed global business world, organizations need to be always-on, always-connected computing for

P. Ndayizigamiye et al. (Eds.): IDIA 2022, CCIS 1774, pp. 218–233, 2023.
https://doi.org/10.1007/978-3-031-28472-4_14

employees and for their business partners and customers (Weinman 2017). Most business activities are conducted by computer networks, which facilitate communications among organizations.

The rapid improvements in technology have led to a rise in information security concerns. Aman et al. (2021) argues that technology has also brought unnecessary complexities and boundless opportunities for slip-ups. Technology development out-paces the development of control practices and adequate in-house expertise for small businesses. Moreover, the increased usage of the Internet and telecommunication devices has brought risks, threats, and vulnerabilities to small organizations (Saffady 2020). Most of the small organizations have insufficient resources, skills and knowledge to safeguard their information management systems (Valli et al. 2021). Although security is a well-recognized issue, it has been noted that many organizations, particularly SMEs, do not apprehend all the steps needed to shield themselves, Valli et al. (2021) further alluded, which makes them an easy prey to information technology bullies. With cyber-crime on the increase, security threats are becoming increasingly sophisticated and harder to detect. This may in turn lead to data leakage, down-time and reputation loss, which in turn lead to loss of existing customers resulting in a negative impact on the organization's bottom line and ultimately profit margins (King 2021).

Numerous studies (Jørgensen 2015; Nagahawatta et al. 2021; Shojaifar and Järvinen 2021) ranging from the academia to the practitioners have contributed to this research area, providing several methods, frameworks and models to define security policy adoption in SMEs. The terms SME or SMME are used interchangeably. SMEs needs to have a secure IT environment but very often this is upended by other priorities. This shortcoming makes small business entities insecure and prone to hackers and various forms of malpractices that threaten effective information management in small business entities. SMEs regularly find the task of keeping their business functions aligned with their security process highly challenging.

Unlike large organizations, SMEs frequently lack security measures and policies to secure their computer resources. Their network infrastructure is often maintained by end-users with limited computer technical skills and knowledge (Nagahawatta et al. 2021). Smith and Ali (2019) stated some of the common worst mistakes committed by computer users as follows:

- Opening email attachments from unverified sources.
- Failing to install software security patches for commonly used applications such as Microsoft Office.
- Writing their confidential information such passwords on paper.
- Downloading and installing games and screen savers from untrusted sources.
- Failing to run regular backups and or verifying the integrity of backups.

SMEs are not always aware of the security threats that may negatively affect their companies (Shojaifar and Järvinen 2021), as they don't fathom that security is more than just pre-venting viruses and blocking spam. They need a proper awareness on information security and the right measures of preventing security breaches. The aim of this study was to conceptualize a security framework for SMEs.

Key Concepts

SME in South African Context

Rehman and Anwar (2019) pointed to the fact that the geographical placement of the SME as well as country specific legislation influence the numerous small or medium enterprise definition. A small to mid-size enterprise (SME) organization upholds revenues, assets and employs less than 250 employees. The standards of measuring whether an organization is an SME, also vary among countries and industries. In this paper South African standards of determining an SME are used. Defining an SME can be a challenging task (Lekhanya et al. 2017). SMEs comprise over 95% of the economy globally. They are the driving force behind many innovations, which contributes to employment creation, investments and exports (Lekhanya 2015). SMEs are naturally born survivors; they are content to survive if they make a decent existence (Alonso-Almeida et al. 2018). Most of their functions are often 'patched up together' lacking any degree of integration and sophistication. Policies and frameworks for information planning and disaster recovery are usually non-existent which makes them more vulnerable to cyber security issues (Srivastava et al. 2019).

As is the case in most countries, the definition of SMEs is a challenge. South African authors and researchers have exploited multiple ways to define an SME by looking at different perspectives such as the size, environment of operation, owner managed level and whether it is semi-formal or formal in relation to the economy development. The South African National Small Business Act 102 of 1996 officially provided definitions for small businesses which were revised by the National Small Business Amendment Acts of 2003 and 2004 (DTI 2008). Table 1 below, shows the enterprise definitions given in the National Small Business Act, for the classification of micro, small or medium enterprises.

According to Table 1 it is very clear that South African definitions are like that of other developing countries such as Ghana, Kenya and Nigeria (Mambula 2002; Quartey et al. 2017), whereby SMEs are classified as start-up enterprises or survivalist enterprises. Furthermore, most of the definitions are categorized according to the size of the enterprises, the total number of employees paid, the total annual turnover and total assets fixed value as well as the impact of the SMEs to the economy.

Generally, small and medium enterprises (SMEs) are regarded as the main engines for economic development since they play a pivotal role towards the growth of the country (Amoah et al. 2022). Furthermore, they are labor intensive, capital saving and capable of helping to create most of the employment the world needs by the end of the century (). In developing countries small organizations produce a considerable share of their gross domestic product (GDP) and are considered as a key source of employment generation, innovative business ideas as well as viewed as a breeding ground for entrepreneurship (Chipunza and Naong 2020).

In Nigeria SMEs, make up to 90% of all the available businesses and at least account for 70% of the country's employment. In Kenya, SMEs employ almost 87% of the workforce (Murithi 2021). In South Africa, the Department of Trade Industry (2020) indicated that more than half of all the employment comes from organizations having less than 200 workers and it contributes about 50% to 60% to the gross domestic product (GPD) with a possibility to increase regularly (Abor and Quartey 2010; Taiwo and

Table 1. Classification of micro, small or medium enterprises

Sector or sub-sectors in accordance with the standard industrial classification	Size or class	Total full-time equivalent of paid employees less than	Total annual turnover less than: total annual turnover less than	Total gross asset value (fixed property excluded) less than
Agriculture	Medium Small Very small Micro	100 50 10 5	R 4.00 m R 2.00 m R 0.40 m R 0.15 m	R 4.00 m R 2.00 m R 0.40 m R 0.10 m
Mining and quarrying	Medium Small Very small Micro	200 50 20 5	R 30.00 m R 7.50 m R 3.00 m R 0.15 m	R 18.00 m R 4.50 m R 1.80 m R 0.10 m
Manufacturing	Medium Small Very small Micro	200 50 20 5	R 40.00 m R 10.00 m R 4.00 m R 0.15 m	R 15.00 m R 3.75 m R 1.50 m R 0.10 m
Electricity, gas and water	Medium Small Very small Micro	200 50 20 5	R 40.00 m R 10.00 m R 4.00 m R 0.15 m	R 15.00 m R 3.75 m R 1.50 m R 0.10 m
Construction	Medium Small Very small Micro	200 50 20 5	R 20.00 m R 5.00 m R 2.00 m R 0.15 m	R 4.00 m R 1.00 m R 0.40 m R 0.10 m
Retail and motor trade and repair services	Medium Small Very small Micro	100 50 10 5	R 30.00 m R 15.00 m R 3.00 m R 0.15 m	R 5.00 m R 2.50 m R 0.50 m R 0.10 m
Wholesale trade, commercial agents and allied services	Medium Small Very small Micro	100 50 10 5	R 50.00 m R 25.00 m R 5.00 m R 0.15 m	R 8.00 m R 4.00 m R 0.50 m R 0.10 m
Transport, storage and communications	Medium Small Very small Micro	100 50 10 5	R 20.00 m R 10.00 m R 2.00 m R 0.15 m	R 5.00 m R 2.50 m R 0.50 m R 0.10 m

Falohun 2016). Furthermore, the 2019 StatsSA report estimated that more than 95% of South African businesses were SMEs and that these SMEs contributed over 60% of total employment in the country.

a. ***Information Security practice within SMEs***

Most of the information security frameworks and strategies that were originally developed for large organizations or government institutions may not be beneficial or practical in SMEs (Kaila and Nyman 2018). Small organizations generally lack resources such as finances, technology, skilled human resource, and proper infrastructure. With the lack of funds SMEs cannot have the same resources large organizations possess to secure their networks appropriately. Additionally, many owner-managed SMEs deem information security to be a low priority.

However, SMEs and large organizations have a lot in common despite their small footprint in the global marketplace. They use the same technology to conduct business, offer services to clients of which some are relatively located in remote areas, and they provide access to their database systems (Wang 2019). Large organization have the necessary platform for handling security issues within their human resources capabilities and funds galore to mitigate risks better than SMEs. Within SMEs it is believed that security can be provided with the help of configuring a firewall and deploying an anti-virus program (Lenhard 2022). On top of this, their ICT infrastructure is maintained by end-user, usually someone who has limited computer technical skills or knowledge of IT security.

The emerged technologies and information system have enabled work activities to be accomplished more efficient and effectively than ever before. This technology has also brought unnecessary complexities and a great room for error and developed much quicker than the development of security controls and adequate in-house expertise for both SMEs and large organizations (Saffady 2020).

b. ***Information Security policies within SMEs***

Information security policy is often referred to as a living document which is used to specify a set of rules, guidelines and behaviors on organizational assets, but it is continuously modified as technology and employee requirements change (Bryson 2018). This definition is directly in line with the international standard on information security management as it plans to secure the organization's physical and technological resources as well as the information it handles. Furthermore, an organization's security policy may include allowed or disallowed behavior, broad guiding protocols to be used to achieve goals, backup procedures, compliance and enforcement with the policy to ensure that necessary procedures are followed.

The fact that an organization has a security policy is an indication that it is committed to protect the confidentiality, integrity and availability of all the systems they use as well as the information it handles. However, if employees of the organization are not keen or are unwilling to follow security polices, the efforts to develop one are wasted (Spurling et al. 2018). Lenhard (2022) emphasized that in organizations without policies, particularly SMEs, security practices will be developed without clear ambitions and responsibilities. For example, most large organizations establish computer security technologies and practices to secure information resources, although security cannot be attained through technical tools only and their impact and effectiveness are far from over.

The recent concerns on security policies continues to grow in academic literature (Feng et al. 2019; Wu et al. 2021) and point out the need of empirical investigation to the security incidents. While in the last decade, IT security policies were never talked about and unheard to the outside world, currently they are regarded by organization of all sizes as one of the most important cornerstones of IT security. Organizations are now taking action to protect their own information and information entrusted to them by customers, suppliers and partners. They are forming structures and programs to address and evaluate both internal and external risks and threats to their electronic information (Menard et al. 2017). However, most academics and practitioners' communities, as Balozian et al. (2019) assert, have generally focused on common issues related to information security policies which include the awareness and behavior of employees with information systems.

2 Methodology

This paper employed an interpretivist approach to support the belief that reality is constructed by subjective perceptions and predictions (Littlejohn and Foss 2008). Researchers who select this paradigm are only interested in the social construction of meaning. People have a free will, purposes, goals, and intentions. Therefore, people should be studied as active agents. As a result, the researcher can draw themes from within a particular context (Farrugia 2019). It can then be said that human beings create their own reality associated with their own belief systems and values (Bakker and Lelkes 2022).

The reason behind applying an interpretivist approach in this paper was to understand the opinions of the key stakeholders from different SMEs in SA through interviews with an effort to understand reasons that may lead their organizations to adopt an information security framework. This approach allowed the researcher to understand the complexity of social and human variables within the information security adoption phenomenon and where it is located. Since these variables are difficult to measure, the researcher applied processes with an intense enquiry to understand and analyze the data. A focus group was selected for sampling to get the in-depth views of the participants (Subiantoro 2018). In total, twenty-four in-depth interviews were conducted with key stakeholders from different SMES (see Table 2). Participants experience and social factors are instrumental to the concepts that is being investigated, as well as the views that are generated during the interviews.

As suggested by McIntosh (2017), participants' identities should always remain anonymous to afford participants the freedom to share information regarding the phenomenon under investigation. A total number of ten participants were selected for this study. All the participants held an influential position in their organizations. There was a good mix of CEOs, senior managers, middle-level managers, and employees amongst the interviewees. To preserve the confidentiality of participants, each interviewee was assigned a special code. All the interviews were recorded and their duration varied between 45 to 60 min each. The interview guide was piloted to ensure validity and integrity.

Table 2. Participants details per SME

Background information of the participants (Source: Author) Code	Unit/Division	Position	Years of experiences within the current position
A	CE-I	Manager	10
B	CE-I	CEO	2
C	CE-I	Employee	9
D	CE-I	Manager	1
E	CE-I	Manager	2
F	CE-I	Manager	10
G	CE-I	CEO	5
H	CE-I	Employee	1
I	CE-I	Project Manager	5
J	CE-I	Project Manager	5

2.1 Thematic Analysis Process

The goal of this study was to conceptualize a security framework for SMEs that could be implemented to improve information systems security. This study used content analysis to identify themes affecting the adoption of information security within SA SMEs. To validate the identified themes, interviews were conducted, and thematic analysis was used to confirm the themes. The content analysis was used to review high-quality literature (Webster and Watson 2002). The approach considered only the Senior Scholars' Basket of Journals, and the top 50 journals, such as ACM/IEEE transactions of the AIS journal ranking (Vom Brocke et al. 2015; Fink 2019). Themes that were identified and new ones that emerged were analysed using thematic analysis. This was for verification of the themes, and determining their influence on the adoption of the security framework. During further analysis of the interviews, several related concepts emerged which guided the researcher to construct a final information security adoption framework.

This became even more evident after transcribing and reading through the first few interviews. t For this reason the researcher then employed a more data driven approach during the initial phases of analysis. The data driven approach allowed the themes to emerge primarily from the data, as opposed to using a theoretical framework upfront to seek out predetermined themes from data. After the identification of any relevant themes from the raw data, the researcher was able to relate this back to the theory obtained in the related literature. The hermeneutic cycle of Myers (2019) was employed numerous times across all six phases of analysis, with a strong focus on the identification of latent as opposed to semantic themes. The mechanisms that constituted the actual process of analysis consisted of the following phases:

Phase One: The transcription of all the interviews was conducted with great care. Phase one is recognized as an important part of the analysis process, due to the fact that it is the

foundation of all the analysis work and has given the researcher the opportunity to get acquainted with the data. Transcribing all the interviews further aided this familiarization process. During this phase the researcher made an initial list of relevant concepts that may be part of all possible themes. This in turn assisted in the execution of phase two, since at least some initial analysis had been performed.

Phase Two: Phase two execution required coding the entire data corpus, which resulted in a coding framework containing information beyond the core concepts of this research paper. This process involved analyzing each interview transcript bearing in mind the list that was created in the initial phase. Phase one coding was more data than theory driven, so as not to miss any information that might have been of interest later. This included the creation of codes for specific data extracts. According to phase two its mechanisms and data extracts could be coded multiple times. This is illustrated with examples in Table 3, where column two contains multiple codes for the data extract it is associated with (in column one). The third column in Table 3 allows for easy navigation of each participants' transcript.

Some of the codes could also be associated with more than one data extract. This type of coding is illustrated in Table 4, where the first row contains an example of three data extracts associated with one code (in column two). During the execution of phase two, the researcher was cautious not to interpret the data extracts, but to rather create a coding framework based on that which was said.

Phase Three: In phase three, the researcher identified candidate themes and associated sub-themes from the coded data extracts. An extract of one such candidate theme (and sub-themes) is given in Table 4. The alphabetic column three, is used to identify the participant from whom the code originated and subjected to further analysis. Using this form of data organization became useful during phase four where the identified themes had to be refined and their associated extracts collated. The researcher has taken great care not to eliminate any themes at this stage, but rather to form as many candidate themes as possible.

Phase Four: Phase four consisted of a dual process whereby the candidate themes were refined on two levels. Firstly, the collated data extracts had to undergo scrutiny as to whether they tied into the candidate themes with which they were associated. Secondly, once complete, evaluating the themes across the entire data set occurred. This ensured that the identified themes were valid in relation to the data set as a whole and that it captured the meanings as they were portrayed by the participants (Table 5).

This two-step process resulted in some themes being eliminated, renamed, or merged with other candidate themes. An extract of one such theme, together with the data extracts collated under its name, is illustrated in Table 6.

Phase Five: After reading the entire interview data corpus the researcher used the output of phase four (refined themes) to construct the final thematic map (see Fig. 1). As suggested by Braun and Clarke (2005), these themes were organized to avoid overlapping, which is illustrated by the fact that there is no association between the two main themes

Table 3. Data extracts that have been coded multiple times.

Data extract	Code	Line in transcript
"The major thing as far as our lot is concerned is protection and that's the thing, we get worried about from the most. Being exploited. And that is kind of foremost in our minds about if were not secured that might destroy the organization reputation and integrity. Assurance of protection increases confidents and leads to better decision making"	Concerned about protection from intruders	1
"A lot of people see security policy as something they don't use. I would not even just talk about the security threats etc. but take it from the most basic. Let's understand information security then work through the security issues etc. I think there is a lot of hype. Unnecessary hype in terms of the security. I think we are so many other things we are making a mountain out of a mole hill"	Understanding policy first then security Information security surrounded in hype	2
"Yes, and the reason being I want to know, because it firstly would be a test in terms of how they react to things. The fact that it didn't affect me would be a good sign. So, it's part of understanding how they react in terms of when they're at risk. Secondly if there's consistent breach, I would possibly want to improve the security in organization"	Training and awareness on security issues should be considered Insight into their incident response practices Constant breach prompts improved	3

("Trust in information security" and "Views as Subscribers"). As phase five primary contained the main output, it was the final thematic map which enabled the researcher to interpret the data extracts associated with these themes.

Phase Six: Phase six concluded the process of analysis resulting in the creation of a narrative based on the researcher's interpretations of -

- the identified themes and the data extracts associated with them;
- the context within which these data extracts were embedded; and
- each SME's operational and security context.

Table 4. Data extracts classified under the same code

Data extract	Code	Line in transcript
Ineffectiveness of top management is a major concern The only concern that has ever been raised is lack of resources and support from management. What happens if management's involvement is absent?	Top Management's influence	1
Combine your knowledge combine your skills, combine your understanding, and then come with recommendation[s]. Whereas [an] individual SME you might feel isolated you might be scared even financially is it the right way to go Why do you have recreated, at each SME re-establish, redevelop you know why you have to have your skill… You can't have one SME have the complete skill set to serve all the needs of the organization We know that's the truth. So, what do we do? Rather combine those strengths	Advantages ISM best practices	2

Table 5. Data extracts classified under the same code

Candidate theme	Sub-themes	Code [associated participants]
Knowledge of information security	Technical security architecture Information Security Incident Response Information security training and awareness	1

Table 6. Redefined theme with collated extracts

Refined theme	Data extracts [associated participants]
Security policy	

Throughout this narrative the researcher highlighted the contextual differences between the participating SMEs. This involved not only providing the reader with participatory statements to support these arguments, but also interpretations of the relationship between these statements and operational context of these participants and SMEs. Where

applicable, references to the literature were made and thus also formed part of the interpretations made within that context. In the following section the reader is presented with the resultant narrative, wherein all the main and sub-themes are discussed.

2.2 Theoretical Framework

The ISO 27001 standard was published in 2005 under the title "Information technology—Security techniques—Information security management systems—Requirements". It describes the requirements that an ISMS must fulfill to achieve certification. As a theoretical framework, the standard is aimed at organizations from all sectors and of all sizes. However, there is some doubt over the suitability for SMEs (Fanta 2016). Concrete measures for the fulfillment of requirements are not stipulated by the standard but must rather be developed and implemented on a company-specific basis. Certification requirements of ISO 27001 are elucidated through the elaboration of terms and concepts and supplemented with an implementation guideline within ISO 27002. The focal point of ISO 27001 is the requirement for planning, implementation, operation, and continuous monitoring and improving of a process-oriented ISMS. The approach should be aligned with the PDCA cycle (Fig. 4). The coverage and scope of an ISMS should be defined for planning and implementation. Risks should be identified and assessed (Torten 2018) and control objectives should be defined for the information and information systems. Suitable measures for protecting operations should be derived from these.

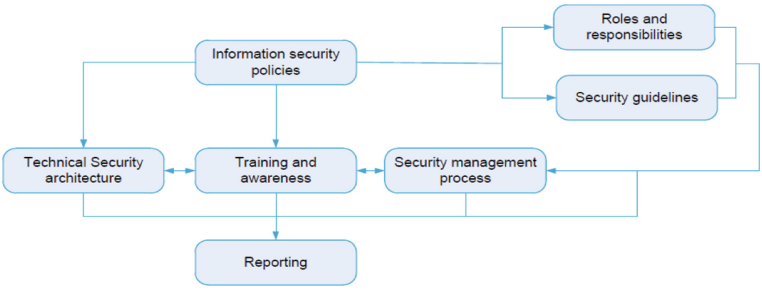

Fig. 1. ISO/IEC 27002 information security framework (Disterer 2013).

ISO 27000, "Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary," International Organization for Standardization ISO, (Disterer 2013). Figure 1 depicts the importance of information security policies for the roles and responsibilities, and security guidelines. They play a huge role in the development of technical architecture, training and awareness, security management, SMEs' size, and top manager's intentions. However, a lack of data security, lack of data privacy and size of IT resources hinder CC adoption.

3 Research Findings and Discussion

During further analysis of the illustrated themes (see Fig. 3), several related concepts emerged. From this the researcher decided to create a new conceptual framework. Used

in combination, these new conceptual frameworks guided the interpretation process. To better illustrate these new frameworks the conceptual framework is provided before interpreting the main theme with which it is associated (Fig. 1). It is anticipated that this will not only assist the reader in understanding how the concepts are related, but more importantly why they are related (Fig. 2).

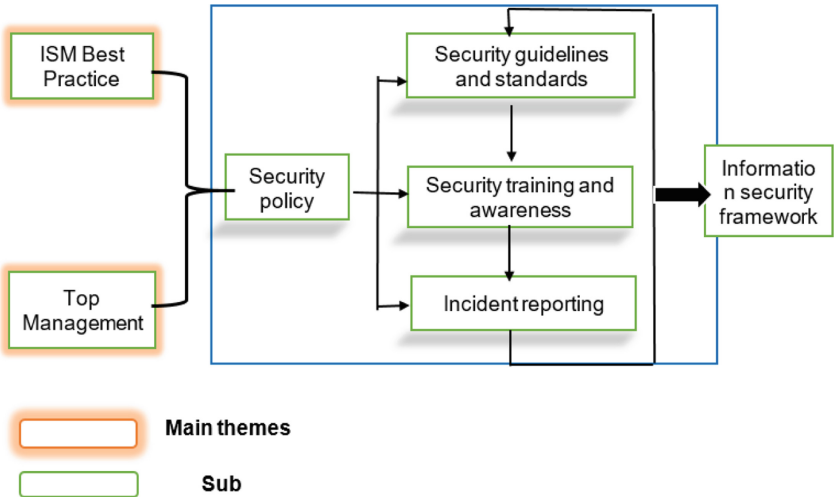

Fig. 2. Conceptual security framework for SMEs.

The proposed technical security framework and all its components developed by this study, could be utilized to mitigate the risks that could destruct the reputation and integrity of an organization. The benefits of this framework are that it is built or customized according to the SME's needs to solve specific information security problems. The modern economy has required organizations of all sizes to have information security practices, policies, frameworks and procedures in place. Without this they are vulnerable and could be exploited by threats. Furthermore, Gbadeyan, Butakov and Aghili (2017) emphasized that information security frameworks at least provide the skeletal structure an organization can look to for its security initiatives.

The developed framework is categorized into three main sections. The highest (third) level consists of living documents (policies) which are aligned with the SME's vision and mission and must be continually updated on a regular basis. This is to ensure compliance and provides rules for securing resources within an SME. The intermediate (second) level includes standards which describe statements of what must be done to comply with policy. Finally, the lowest (first) level contains practices, procedures and guidelines, including details of how employees should comply with information security policy and standards of the organization (Whitman 2016).

The findings of this study indicate that management influence has a positive impact on the overall security effectiveness of an organization. SMEs therefore, need to leverage the empirical evidence obtained from this study to improve their IT usage and security.

4 Conclusion

Most SMEs in South Africa lack strong and adequate security measures to protect their information against internal and external security threats. SMEs face security threats that cause potential loss of organization information (Jahankhani et al. 2022). These losses might be caused by the absence of security policies or ineffectual security policies within SMEs. SMEs have experienced vulnerabilities on their networks, such as data losses and theft of data. This might have been caused by a lack of security awareness among employees and managers (Saffady 2020). Information security practices, strategies and techniques for any organization, whether big or small are a necessity to protect and provide a clear road map of information security. This entails that SMEs which do not have information security in place, will have difficulty in dealing with security issues as well as managing people and protocols within the organization. This will lead to inconsistent decision making and jeopardizing of security by both internal and external members of the society. Sharing information security policies with all stakeholders is a crucial step. A training session would openly engage employees in a positive attitude to information security, which will ensure that they obtain an understanding of the procedures and instruments in place to protect the information, for example confidentiality and information sensitivity issues. Such training awareness should investigate vital topics, namely how to use/collect/disseminate/delete data, maintain data integrity, confidentiality, appropriate usage of IT technologies and correct usage of social networking.

5 Recommendations

The researcher would like to highlight several recommendations for South African SMEs who have either started or are considering a move towards employing information security practices. As with most projects a successful information security strategy adoption process should be founded on frequent communication. This should not only be done internally amongst key stakeholders, but most definitely also by the employees of the intended security solution. Regarding communication, the researcher would like to highlight the following recommendations:

Engage with Users: Key stakeholders should do this as soon as possible. After all, these are the people who will be making use of the system and in turn either deem it a useful service or not. Such engagements should include awareness campaigns with a specific focus on information security.

Engage with Other Key Stakeholders: This can take the form of regular meetings or the establishment of a forum where matters of urgency can be discussed. It is important to note that these discussions should be widely attended. If possible, engage all stakeholders. If the SME is in a pre-adoption phase, these types of discussions are vital, since they allow for the formation of information policies, guidelines, requirements and any further strategic decision making. Once adopted, such meetings may not be needed as frequently and should take place to monitor what has been implemented and make changes as required.

Employ Specialised Staff: The presence of an information security officer enhances the adoption and operation of information security practices. In fact, from the information gathered during this study the researcher deems the presence of such a staff member as not just a recommendation, but rather a requirement. Such members of staff should be tasked with the creation of security incident response procedures as well as communicating with origination members at all levels. This would entail the sharing of information that might directly affect the users, such as disclosing breaches in security. If no awareness campaigns have been conducted and the user base is uneducated, such forms of disclosure could be counterproductive, hence the need to educate and make users aware of information security.

Perform a Threat Assessment: Many key stakeholders were not aware of the specific threats. This highlights the need to not only become familiar with these threats, but to also identify the likelihood of them occurring within the operational context of their SME. Measures need to put in place to address internal threats, since most of the participants' regard this as a concern.

Although these recommendations are aimed at both start-ups and well-develop SMEs, it would be wise for organizations to investigate them further before starting an information security adoption campaign. The researcher anticipates that such investigations will allow future researchers to break these recommendations up into even more detailed components.

References

Abor, J., Quartey, P.: Issues in SME development in Ghana and South Africa. Int. Res. J. Financ. Econ. **39**(6), 215–228 (2010)

Alonso-Almeida, M.D.M., Bagur-Femenias, L., Llach, J., Perramon, J.: Sustainability in small tourist businesses: the link between initiatives and performance. Curr. Issue Tour. **21**(1), 1–20 (2018)

Aman, A.H.M., Shaari, N., Ibrahim, R.: Internet of things energy system: Smart applications, technology advancement, and open issues. Int. J. Energy Res. **45**(6), 8389–8419 (2021)

Amoah, J., Belas, J., Bélas, J., Dziwornu, R., Khan, K.A.: Enhancing SME contribution to economic development: a perspective from an emerging economy. J. Int. Stud. (2022)

Balozian, P., Leidner, D., Warkentin, M.: Managers' and employees' differing responses to security approaches. J. Comput. Inf. Syst. **59**(3), 197–210 (2019)

Bakker, B.N., Lelkes, Y.: The structure, prevalence, and nature of mass belief systems. Cambridge Handb. Political Psychol. **89** (2022)

Bryson, J.M.: Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement. Wiley, Hoboken (2018)

Chipunza, L.T., Naong, M.N.: Demographic variables as drivers of innovation in small accommodation businesses: a case of South Africa and Zimbabwe. Afr. J. Sci. Technol. Innov. Dev. 1–9 (2020)

Cooper, D.R., Schindler, P.S., Sun, J.: Business Research Methods, vol. 9, pp. 1–744. McgrawHill, New York (2006)

Da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. **49**, 162–176 (2015)

Disterer, G.: ISO/IEC 27000, 27001 and 27002 for information security management (2013)
Fanta, A.B.: Complementarity between relationship lending and collateral in SME access to bank credit: evidence from Ethiopia. J. Afr. Bus. **17**(3), 308–318 (2016)
Farrugia, L.: WASP (write a scientific paper): the ongoing process of ethical decision-making in qualitative research: Ethical principles and their application to the research process. Early Hum. Dev. **133**, 48–51 (2019)
Felderer, M., Katt, B.: A process for mastering security evolution in the development lifecycle (2015)
Feng, N., Wang, M., Li, M., Li, D.: Effect of security investment strategy on the business value of managed security service providers. Electron. Commer. Res. Appl. **35**, 100843 (2019)
Fink, A.: Conducting Research Literature Reviews: From the Internet to Paper. Sage Publications (2019)
Gbadeyan, A., Butakov, S., Aghili, S.: IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. Ann. Telecommun. **72**(5–6), 347–357 (2017). https://doi.org/10.1007/s12243-017-0568-5
Hartmann, S.B., Nygaard, L.Q.V., Pedersen, S., Khalid, M.S.: The potentials of using cloud computing in schools: a systematic literature review. Turkish Online J. Educ. Technol. **16**(1), 190–202 (2017)
Jahankhani, H., Meda, L.N.K., Samadi, M.: Cybersecurity challenges in small and medium enterprise (SMEs). In: Jahankhani, H., Kilpin, D.V., Kendzierskyj, S. (eds.) Blockchain and Other Emerging Technologies for Digital Business Strategies. ASTSA, pp. 1–19. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-98225-6_1
Jørgensen, K.: Integration of safety in management tasks in onshore transport SME's. In: 8th International Conference on Working on Safety: Smart Prevention for Sustainable Safety, WOS 2015, pp. 50–62. Scientific Committee (2015)
Kaila, U., Nyman, L.: Information security best practices. Technol. Innov. Manag. Rev. (2018)
King, E.E.: Bring your own device security awareness and security behavior: a quantitative explanatory study. Doctoral dissertation, Capella University (2021)
Kotler, P., Burton, S., Deans, K., Brown, L., Armstrong, G.: Marketing. Pearson Higher Education (2015)
Lekhanya, L.M.: Public outlook on small and medium enterprises as a strategic tool for economic growth and job creation in South Africa. J. Gov. Regul. (2015)
Lekhanya, L.M., Olajumoke, N.G., Nirmala, D.: Exploring fast moving consumer goods (FMCG) Small, Medium, and Micro enterprises manufacturers' need for innovation to achieve growth. Economics **8**(2), 8–16 (2017)
Lenhard, T.H.: Configuration of security systems. In: Lenhard, T.H. (ed.) Data Security: Technical and Organizational Protection Measures against Data Loss and Computer Crime, pp. 87–92. Springer Fachmedien Wiesbaden, Wiesbaden (2022). https://doi.org/10.1007/978-3-658-35494-7_18
Littlejohn, S.W., Foss, K.A.: Theories of Human Communication, 9th edn. Thomson Higher Education, Belmont (2008)
Mambula, C.: Perceptions of SME growth constraints in Nigeria. J. Small Bus. Manag. **40**(1), 58–65 (2002)
McIntosh, M. (ed.): Globalization and Corporate Citizenship: The Alternative Gaze: A Collection of Seminal Essays. Routledge (2017)
Menard, P., Bott, G.J., Crossler, R.E.: User motivations in protecting information security: protection motivation theory versus self-determination theory. J. Manag. Inf. Syst. **34**(4), 1203–1230 (2017)
Myers, M.D.: Qualitative Research in Business and Management. Sage (2019)
Oppong, S.: Between Bandura and Giddens: structuration theory in social psychological research? (2014)

Nagahawatta, R., Warren, M., Lokuge, S., Salzman, S.: Security Concerns Influencing the Adoption of Cloud Computing by SMEs: A Literature (2021)
Quartey, P., Turkson, E., Abor, J.Y., Iddrisu, A.M.: Financing the growth of SMEs in Africa: what are the constraints to SME financing within ECOWAS? Rev. Dev. Financ. **7**(1), 18–28 (2017)
Rehman, A.U., Anwar, M.: Mediating role of enterprise risk management practices between business strategy and SME performance. Small Enterp. Res. **26**(2), 207–227 (2019)
Rodriguez, A.R., de Sevilla Müller, L.P., Brecha, N.C.: The RNA binding protein RBPMS is a selective marker of ganglion cells in the mammalian retina. J. Comp. Neurol. **522**(6), 1411–1443 (2014)
Saffady, W.: Managing Information Risks: Threats, Vulnerabilities, and Responses. Rowman & Littlefield Publishers (2020)
Shin, D.W., Hwang, E.: A Lagrangian multiplier test for market microstructure noise with applications to sampling interval determination for realized volatilities. Econ. Lett. **129**, 95–99 (2015)
Shojaifar, A., Järvinen, H.: Classifying SMEs for approaching cybersecurity competence and awareness. In: The 16th International Conference on Availability, Reliability and Security, pp. 1–7 (2021)
Smith, D.T., Ali, A.I.: You've been hacked: a technique for raising cyber security awareness. Issues Inf. Syst. **20**(1) (2019)
Spurling, G., Felton-Busch, C., Larkins, S.: Aboriginal and Torres Strait Islander health. Aust. J. Prim. Health **24**(5), i–ii (2018)
Srivastava, S.R., Dube, S., Shrivastaya, G., Sharma, K.: Smartphone triggered security challenges—issues, case studies and prevention. In: Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, pp. 187–206 (2019)
StatsSA website. https://www.statssa.gov.za/?p=13900. Accessed 17 Dec 2020
Subiantoro, I.H.: Pertunjukan Ritual Seren Taun Di Cigugur Kabupaten Kuningan Jawa Barat. Doctoral dissertation, PPS ISI Yogyakarta (2018)
Sungkawati, E., Suarniati, N.W., Hernanik, N.D., Anugerah, R.: SMEs creative economy in the Covid-19. Arch. Bus. Rev. **9**(1) (2021)
Taiwo, J.N., Falohun, T.O.: SMEs financing and its effects on Nigerian economic growth. Eur. J. Bus. Econ. Accountancy **4**(4) (2016)
Torten, R.J.: A quantitative regression study of the impact of security aware-ness on information technology professionals' desktop security behavior. Doctoral dissertation, Capella University (2018)
Vagle, M.D.: Crafting Phenomenological Research. Routledge (2018)
Valli, C., Martinus, I., Stanley, J., Kirby, M.: CyberCheck.me: a review of a small to medium enterprise cyber security awareness program. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.-S., Tinetti, F.G. (eds.) Advances in Security, Networks, and Internet of Things. TCSCI, pp. 233–242. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-71017-0_17
Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. Commun. Assoc. Inf. Syst. **37**(1), 9 (2015)
Wang, E.S.T.: Role of privacy legislations and online business brand image in consumer perceptions of online privacy risk. J. Theor. Appl. Electron. Commer. Res. **14**(2), 59–69 (2019)
Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. MIS Q. xiii–xxiii (2002)
Weinman, J.: The evolving cloud. IEEE Cloud Comput. **4**(3), 4–6 (2017)
Wu, Y., Tayi, G.K., Feng, G., Fung, R.Y.: Managing information security outsourcing in a dynamic cooperation environment. J. Assoc. Inf. Syst. **22**(3), 2 (2021)
Yeomans, L.: Qualitative methods in business research (2017)