Cybersecurity Issues and Solutions Within the South African Small and Medium-Sized Enterprises

Benediction Kitwa Kalombola and Tabisa Ncubukezi
Cape Peninsula University of Technology, Cape Town, South Africa

222689900@mycput.ac.za
ncubukezit@cput.ac.za

Abstract: This systematic literature review paper presents the main cybersecurity issues and their challenges within the Small and Medium-sized Enterprises (SMEs) in South Africa. The SME's play a very crucial role in the growth of the country's economy and Gross Domestic Product (GDP). However, following the global pandemic, the economy has become increasingly dependent on technology as a driver in different sectors. With the rapid adoption of technology, SMEs constantly face significant cybersecurity issues and challenges that regularly demand proactive and effective measures. These measures guard against exposure to sophisticated cyber-attacks. This study examines the state of cybersecurity within South African SMEs by assessing the effective use of cybersecurity measures, exploring the extent of their implementation, and identifying best practices to strengthen cyber resilience within these SMEs. To achieve this aim, a systematic literature review is conducted to examine high-quality peer-reviewed journals from 2021 to July 2025, providing more insight into the issues associated with cybersecurity in SMEs. Results highlight the vulnerability of SMEs to various cyber threats, including phishing, insider threats, and ransomware. The lack of awareness among employees, inadequate cybersecurity measures, limited resources, the shortage of professional experts, and the absence of effective measures specifically tailored to the needs of SMEs. Additionally, the mitigation strategies emphasize the adoption of robust security measures that are specifically tailored to the needs of SMEs. To enhance cyber resilience, this study also recommends the use of cybersecurity measures tailored to SMEs, encouraging employee education training programs, and the creation of reliable strategies.

Keywords: Best practices, Cybersecurity, Cybersecurity challenges, Cybersecurity issues, Cybersecurity measures, Cyber threats, Small businesses, Systematic literature review

1. Introduction

In South Africa, small and medium-sized enterprises (SMEs) play a crucial role in driving economic growth; however, SMEs have become increasingly vulnerable to cyber threats with the rapid adoption of technology. Despite the benefits associated with digital transformation in improving operational activities, it has also introduced new threats, leaving SMEs exposed to threats such as data breaches, ransomware, and phishing, mainly due to the lack of awareness, limited resources, and ineffective measures (Fakir, 2024; Saeed *et al.*, 2023; Ncubukezi, 2022a). Additionally, because SMEs often rely on outdated security measures and ineffective strategies, they are frequently left vulnerable to threats, particularly in the financial and healthcare sectors (Mahlangu, 2023; Ncubukezi, 2022b).

SMEs encounter issues and challenges in adopting effective cybersecurity measures due to inadequate management and regulations, the absence of skilled professionals, and resources (Shingange, 2022). According to Phahlamohlaka *et al.*, (2022), there is a gap between the practical implementations and available frameworks, including the Zero Trust Architecture (ZTA), National Cybersecurity Policy Framework (NCPF) and the National Institute of Standards and Technology (NIST), which is further enlarged by SMEs unawareness and inability to adopt advanced tools such as multi-factor authentication, encryption, and artificial intelligence (AI) and machine learning (ML) for early threat detection (Admass *et al.*, 2024). Considering that SMEs employ almost 60% of the working population and constitute around 90% of registered businesses in the nation, the impact of cyber threats on the financial institutions is enormous in South Africa. Because human mistakes are the primary reasons that trigger data breaches, Reshmi (2021) argues that this is largely due to the lack of adequate cybersecurity training among employees.

Cybersecurity has become a critical concern for South African SMEs. Businesses are increasingly exposed to sophisticated threats and face challenges in protecting their data (Ncubukezi & Mwansa, 2021). As technology adoption advances, it has become increasingly crucial for SMEs to comprehend the complexities of cybersecurity threats in order to survive and thrive (Benjamin *et al.*, 2024). The problem stems from the lack of effective security measures and the reliance on outdated systems, which are now less effective in mitigating sophisticated threats. The emergence of advanced cyber threats causes several damages within SMEs, including operational disruption, loss of reputation, and economic loss, making it difficult for these businesses to protect the sensitive data they handle (Dave *et al.*, 2023; Mahlangu, 2023).

While several studies addressed the key importance of affordable and customized security measures in which SMEs' real-world challenges are considered, there is still a gap regarding the specific issues and challenges encountered by SMEs along with practical and tailored solutions (Benjamin *et al.*, 2024). The lack of modern and tailored security measures leaves the SMEs vulnerable and constantly exposed to sophisticated cyber threats. Without addressing this, both SMEs and financial institutions will remain vulnerable to cyber threats and suffer the associated consequences. Hence, the study intends to examine the major issues and challenges, exploring the extent of implementation of existing security measures, and providing best practices and effective measures to enhance cyber resilience within SMEs.

To achieve the aim, this work will carry out the following objectives:

- To investigate the major cybersecurity issues experienced by the SMEs in South Africa.
- To explore the extent of implementation of existing measures.
- To investigate the best practices for effective security measures.

2. Literature Review

Several studies have examined the ever-evolving field of cybersecurity. Despite this, a thorough examination of this study is imperative, considering the specific obstacles that most Small and Medium-sized Enterprises (SMEs) face in South Africa (Fakir, 2024). While studies provide recommendations about security threats, the challenges experienced by SMEs remain largely unaddressed (Benjamin *et al.*, 2024). Hence, there is a need for local studies that strongly focus on the specific challenges faced by these businesses. SMEs are becoming more vulnerable to sophisticated cyber threats. However, studies have revealed the challenges these businesses frequently experience in adopting effective security measures, highlighting the need for more advanced strategies tailored to them (Saeed *et al.*, 2023). However, there is still a gap between awareness, current strategies and the actual implementation and regulations (Phahlamohlaka *et al*., 2022). The gradual growth of the technology-driven economy has brought both benefits and emerging threats to SMEs, despite their significant contribution to the economy. Due to digital transformation, these businesses face several issues and challenges in protecting their digital assets, primarily due to a lack of effective security measures and resource constraints (Fakir, 2024), leaving them vulnerable and defenceless against sophisticated threats (Dave *et al.*, 2023). While more advanced frameworks, such as NIST and Zero Trust Architecture (ZTA), exist, their adoption remains limited due to the lack of skilled professionals, financial support, and proper policies required for their implementation (Bokan & Santos, 2021; Lokare *et al.*, 2025). Despite growing awareness of cybersecurity risks, a gap remains between knowledge, strategies, and actual practical actions, especially in resource-constrained environments, including SMEs (Lokare et al., 2025; Admass et al., 2024).

2.1 Summary of Existing Literature

Benjamin et al. (2024) highlight that SMEs are the primary target of cyber threats due to the lack of effective measures and skilled professionals while adopting technology. SMEs are frequently exposed to cyber threats due to inadequate security measures, underscoring the need for more comprehensive and tailored security measures to enhance the protection of their digital data and ensure smooth business operations. Mahlangu (2023) examines the growing concern that emerging ransomware attacks have become a critical concern for financial institutions. The leadership, as well as the behaviour of people, plays a vital role in strengthening endurance within organizations (Mahlangu, 2023), drawing attention to the fact that defense against ransomware is unlikely to be effectively eradicated with technical implementations only. In consideration of risks and challenges faced by financial institutions and businesses, Mahlangu (2023) advocates for measures specifically tailored to these institutions (Mahlangu, 2023). Admass et al. (2024) investigate the role of Machine Learning (ML) and Artificial Intelligence (AI) to strengthen cybersecurity. Admass et al. (2024) highlight the difficulties resulting from insufficient knowledge and flexibility commonly encountered by the majority of SMEs, despite the fact that potential solutions could arise from technological advances such as these. In most cases, SMEs are unable to guarantee effective security due to universal security measures that fail to meet the specific needs of SMEs (Admass et al., 2024). Hence, there is an urgent need for specifically tailored measures to address the challenges faced by SMEs. The study by Saeed *et al.* (2023) highlights that while the adoption of technology may contribute to business growth, it also exposes frequent SMEs to cyber threats. In addition to fostering risk-based security strategies, Saeed *et al.* (2023) underline a pressing need for proactive measures tailored to SMEs, while also suggesting the adoption of flexible and innovative strategies. The study by Fakir (2024) examines the most significant challenges associated with adopting cybersecurity. Because almost every organization operates with various activities and management structures, the difficulties

also vary from one to another organization (Fakir, 2024). Hence, there is a need for more adaptive approaches tailored to the specific needs and challenges faced by SMEs, due to the ineffectiveness of the majority of generic solutions. Additionally, there is a need for continued investigations to closely monitor the advancement of cybersecurity requirements within SMEs (Fakir, 2024).

Shingange (2022) focuses on the lack of connection that exists between the design of measures and their implementation in practice, while investigating the challenges associated with cybersecurity laws and regulations in South Africa. Shingange (2022) highlights the ongoing absence of communication between private industries and governments, which weakens the overall effectiveness of cybersecurity operations. Due to a failure to enforce current laws and regulations, there is a need to critically evaluate and strengthen them (Shingange, 2022).To ensure successful progression, there is a need for greater coordination along with further visible enforcement. In 2021, Reshmi investigated ransomware attacks and their prevention mechanisms. While more advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML) have the potential to identify threats early, their application remains limited within SMEs. This study suggests a wider integration of AI/ML to enhance security against ransomware.

The CENSOR model, as outlined by Tsiodra et al. (2023), is a risk-based model for cybersecurity decision-making. It is specifically beneficial to the SMEs as it guides them in prioritizing their limited resources by evaluating threats according to their significance. The authors also provide an illustration demonstrating how SMEs can apply this model to allocate resources more effectively. Tsiodra et al. (2023) explore the relationship between the magnitude of cyber threats that SMEs encounter and the level of investment that SMEs make. Hence, the critical importance of establishing an appropriate balance between budgeting and maintaining effective security. In the same way, Hermanus (2023) examined the vulnerabilities associated with information security within the financial environment in Cape Town. As reported by the participants in the interviews, organizations continue to face serious problems towards the full adoption such as insufficient resources, the shortage of professional experts, and a poor organized response strategy, despite the fact that some enterprises started putting into effect security awareness training, regulations to the protection of information, intrusion detection systems as well as authentication and authorization systems (Hermanus (2023). Hence, this reveals that some enterprises are becoming aware and starting to take effective action; however, the complete adoption is constrained by operational issues.

In 2023, Musa investigated the cybersecurity issues faced by SMEs from a systems engineering perspective. This study highlights the lack of ongoing monitoring, employee training, and incident response, as the majority of SMEs rely on basic strategies such as antivirus, and password policies. The absence of skilled professionals, resource shortages, and the need for tailored security measures are a few barriers preventing the adoption of cybersecurity. In their review of literature, Alveera & Sukira (2024) delt with cybersecurity within the SMEs, highlighting their susceptibility to cyber-attacks from malicious computer programs and ransomware, regardless of the importance of these SMEs to the growth of the economy within the country, which is mainly the consequence of several factors, including the limited financial resources, inadequate or outdated infrastructures, and regular misperception of the complexity of cybersecurity. Additionally, Alveera & Sukira (2024) highlight the fact that SMEs are often given little attention compared to large corporations, which are mainly prioritized by government initiatives for cybersecurity. This study recommends the adoption of rigorous security mechanisms specifically tailored to the needs of SMEs, conducting risk assessments, and educating team members about cyber threats to ensure robust cybersecurity for SMEs (Alveera & Sukira, 2024).

In 2024, Mugwagwa *et al.* highlight that due to poor awareness, resource constraints, and the absence of skilled professionals, SMEs remain vulnerable to complex threats like insider threats, ransomware, and phishing, highlighting the need for effective malware detection, multi-factor authentication, encryption, along regular employee education to effectively enhance cyber resilience within SMEs. In summary, while there is a growing awareness of cybersecurity, a significant gap remains between awareness, strategic plans, and actual implementation. While cutting-edge technologies like AI/ML can enhance cyber resilience within SMEs, their adoption remains limited due to financial constraints, resource shortages, and a lack of skilled professionals, which are primary issues faced by SMEs in South Africa, preventing them from implementing effective cybersecurity measures.

3. Methodology

A comprehensive systematic literature review is employed in this study to investigate the state of cybersecurity in South African SMEs, with a strong focus on the major issues and challenges, as well as the

extent of implementation of existing security measures. The objective is to provide best practices for enhancing their resilience to cybersecurity. The systematic literature review is adopted in this study along with the analysis of the contents to discover, critically review, and prioritize key research that directly aligns with the previously established questions (using a systematic literature review) and come up with commonly identified issues and challenges, as well as important and repeated solutions and recommendations (content analysis).

3.1 Selection Criteria

To ensure a comprehensive examination of the available literature, the data used were collected from various important databases, including Google Scholar, IEEE Xplore, ScienceDirect, and MDPI. Additionally, South Africa's sources were particularly included to enable a more objective and in-depth examination of the challenges associated with cybersecurity in the South African SMEs.

3.2 Search Strategy

To gather relevant sources of information, a systematic search was conducted. The search was conducted using keywords and phrases including "Cybersecurity" AND "South Africa" AND "SMEs," “Cybersecurity in SMEs,” “Cybersecurity,” “Cybersecurity challenges,” “Information security in SMEs,” Online security,” “Cybersecurity issues,” “Digital security,” “Cyber issues,” “Cyber resilience strategies for SMEs,” and “Data breaches.”

3.3 Prisma Flow Diagram

This study adheres to the PRISMA principle to ensure clarity in the selection of literature, with the aim of identifying, examining, and selecting the most suitable studies for this research. In accordance with predefined inclusion and exclusion criteria, the overall approach consisted of several narrowing phases. For this reason, the following Figure 1 below presents an illustration of the method by which information progresses throughout the different stages of this process of review:

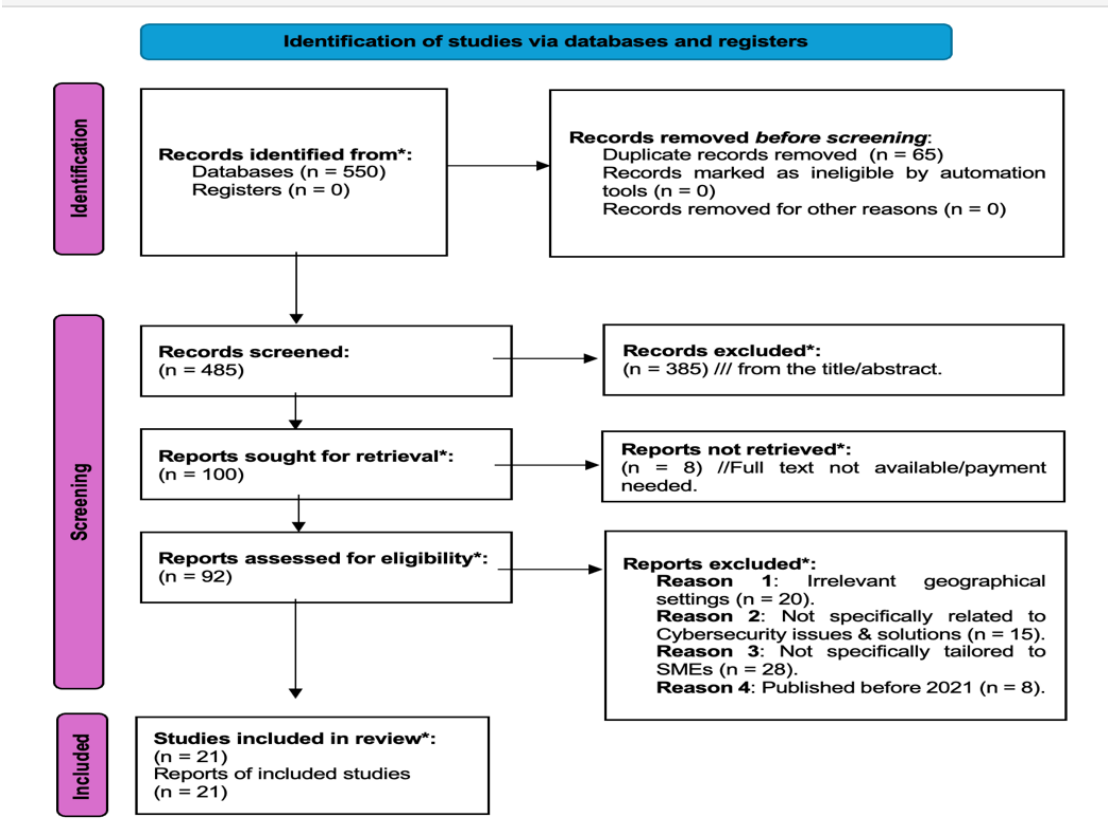

Figure 1: Prisma Flow Diagram

3.4 Inclusion and Exclusion Criteria for Relevant Literature

To gather more accurate and relevant studies, the inclusion and exclusion criteria were defined in this study. Therefore, this research examined various studies that discuss cybersecurity issues and challenges within SMEs, with a focus on studies that emphasize the development of security measures specifically tailored to the needs of SMEs. Additionally, only English articles published between year 2021 and July 2025 were considered to collect the most recent information. On the other hand, excluded studies were those that did not focus on SMEs' issues, challenges, and their needs. Additionally, articles published before 2021 were excluded to ensure that this investigation aligns successfully with the latest information and developments. By following these guidelines, the review was focused on the predefined objectives.

3.5 Data Analysis

To identify important themes, challenges, and technological innovations associated with cybersecurity for SMEs, the content analysis was conducted on the selected literature, aiming to identify issues and challenges encountered by SMEs and potential innovative solutions to enhance their cyber resilience. Finally, the results were combined to provide actionable recommendations to enhance cyber resilience within South African SMEs.

4. Results and Discussions

A total of four interrelated points were revealed from the review of the literature: the different kinds of threats commonly associated with cybersecurity that SMEs experience, the issues preventing them from adopting and using effective security measures, and the extent to which these measures are successfully implemented. SMEs have begun to understand the necessity of introducing effective cybersecurity measures, as the digital economy resulting from technological advancements continues to evolve. The use of these effective cybersecurity measures has become crucial for ensuring the protection of the digital assets they contain while maintaining business operations. The goal of this systematic literature review was to explore the primary issues, challenges, and potential solutions related to the effective implementation of cybersecurity in South African SMEs. Categorized into four key themes, the results of this research indicate that while threats to cybersecurity are gradually being recognized, the potential to effectively establish robust and effective countermeasures remains remarkable. In this section, the findings will be discussed along with their connection to the research objectives and questions.

4.1 Common Cybersecurity Threats Experienced by SMEs in South Africa

SMEs remain vulnerable to various cyber threats identified in the literature, including poor password policies, ransomware attacks, phishing, and insider threats (Mugwagwa et al., 2024; Reshmi, 2021). For businesses and financial institutions, ransomware poses a significant concern due to its potential to result in financial loss and business disruption (Mahlangu, 2023). SMEs have become vulnerable to various threats because of digital transformation, despite the benefits it has brought. Despite the growing awareness of cybersecurity among SMEs, the results of the study indicate that they frequently experience various issues and challenges that restrict them from effectively making use of all necessary measures, including the lack of skilled professionals, poorly structured organizations, outdated systems, and budget constraints (Hermanus, 2023; Musa, 2023; Benjamin *et al*., 2024). Issues with policies and regulations are also quite important. According to Shingange (2022), an inefficient approach to cybersecurity governance has resulted from the lack of strong enforcement and inadequate interaction between the public and commercial sectors. It is common for many SMEs to operate without clearly established cybersecurity policies and regulations, instead relying on improvised solutions, which highlights that cybersecurity is a problem that extends beyond technology and has a profound impact on the way organizations and their systems interact. Given this, there is a need for robust organizational support, effective leadership, and thoughtful policy interventions.

Additionally, Tetteh (2024) emphasizes that more structured threat detection, combined with incident reporting, is essential for achieving more effective cybersecurity in SMEs. According to Tetteh (2024), cyber resilience across the nation has become weaker due to the inability of SMEs to report security breaches, which limits the opportunities for education across the industry. Therefore, there is a need for simplified frameworks that allow SMEs to effectively report incidents and assess risks in a more adaptive manner.

4.2 Challenges Associated with the Effective Use of Cybersecurity Measures

The gap between knowledge and practical actions remains large. The reliance on obsolete systems, financial constraints, a lack of skilled professionals, and the need for tailored security measures are the primary

obstacles (Hermanus, 2023; Musa, 2023; Benjamin et al., 2024). Moreover, further challenges include the breakdown of collaboration between the private and public sectors, inconsistent directions for implementation, and a failure to enforce regulations, as well as inadequate management and weak internal processes (Shingange, 2022; Fakir, 2024). Additionally, the failure of SMEs to report cyber incidents significantly impacts the general and national response efforts. This highlights an ongoing issue with inadequate reporting and the lack of a structured prioritization framework (Tetteh, 2024). By utilising a practical model introduced in this study, Small and medium-sized enterprises are enabled to focus their resources on addressing the most urgent issues and challenges, which in turn enhances their overall resilience.

Although small and medium-sized enterprises (SMEs) are becoming aware of cybersecurity risks and challenges they experience, the review shows that the efforts they make to put in place practical and effective preventive measures are still at the basic level, which include antivirus software, constrained awareness education, and password regulations, while more advanced and sophisticated tools such as ongoing monitoring, systems for intrusion detection, and the Zero Trust Architecture (ZTA) remain rarely, or not used (Hermanus, 2023; Musa, 2023; Erdogan *et al*., 2023; Lokare *et al*., 2025). This circumstance illustrates a clear disconnect between awareness and action. Small and medium-sized enterprises (SMEs) often struggle to acquire cutting-edge technologies, primarily due to financial constraints and limited resources. Additionally, their ability to maintain or enhance complicated systems is limited due to their lack of technical expertise. In many cases, the use of cybersecurity is generally more of a response to specific incidents than an anticipatory measure, as highlighted in section 4.2 "Long-term Strategy," where businesses commonly wait for incidents to occur before taking action.

4.3 Extent of Implementation of Cybersecurity Measures

According to the reviewed articles, many SMEs are using basic security precautions, ranging from password rules, limited awareness training for employees, and anti-virus programs, while preventive and more sophisticated strategies exist, but continue to be left behind (Hermanus, 2023; Musa, 2023; Erdogan et al., 2023; Lokare et al., 2025). Additionally, certain organizations possess disaster recovery plans, but these plans often lack clear procedures. Due to their high costs and complexity, emerging technologies such as threat identification based on intelligence and machine learning (AI/ML), intrusion detection systems, and ongoing monitoring are rarely adopted (Admass et al., 2024; Lokare et al., 2025).

A variety of effective approaches for enhancing SMEs' resilience to cybersecurity threats are highlighted in this research, pointing out the adoption of risk-based strategies to enable SMEs to focus their resources on the greatest threats (Tsiodra *et al.*, 2023; Tetteh, 2024) and the necessity for international models, including the NIST framework for cybersecurity and the ZTA, to be adjusted for resource-constrained environments (Fakir, 2024; Bokan & Santos, 2021). Moreover, studies underlining the necessity for ongoing staff education and training which is indispensable for preventing errors among employees (Mugwagwa *et al.*, 2024; Benjamin *et al.*, 2024) while also promoting encryption, multi-factor authentication, and the need to identify threats at their early stage by integrating more advanced technologies such as AI/ML (Admass *et al.*, 2024; Reshmi, 2021). Additionally, studies promote collaboration between the private and public sectors to offer SMEs adequate funding and support (Shingange, 2022).

4.3.1 Best practices and recommendations

Studies suggest that to reconcile the divide between knowledge and practical action, it is necessary to tailor cybersecurity approaches to the needs of SMEs, adapting frameworks like Zero Trust Architecture (ZTA) and NIST to resource-constrained environments (Fakir, 2024; Bokan & Santos, 2021). To reduce human errors, a continuous educational program becomes crucial (Mugwagwa et al., 2024; Benjamin et al., 2024), as well as risk-based approaches for effective resource allocation (Tsiodra et al., 2023). Moreover, advanced measures such as AI/ML, multi-factor authentication, and encryption can enhance security through early threat detection (Admass et al., 2024; Reshmi, 2021). Additionally, studies suggest that the government should strengthen collaboration between the private and public sectors, increase policy monitoring, and provide more detailed recommendations tailored to the benefit of SMEs.

The need for more effective and robust cybersecurity measures has become paramount, particularly within SMEs, which continue to remain more vulnerable and are constantly exposed to cyber threats as a result of being primary targets. Thus, the following recommendations resulting from the results and conclusions drawn from this research will enable SMEs to further strengthen their resilience and utilization of cybersecurity in South Africa:

- **Promote awareness on cybersecurity**: To effectively handle human-related vulnerabilities while improving the culture of companies, there is a need for regular awareness and educational campaigns about cybersecurity.
- **Adapt frameworks tailored to SMEs' needs:** A necessity for both policymakers as well as experts in cybersecurity to design more reasonable security measures that adapt to the specific business processes, size, and the available resources of SMEs.
- **Promote the utilization of risk-based solutions**: As recommended by Tetteh (2024) and Tsiodra *et al.* (2023), SMEs could first detect and address high-risk spots, concentrating the insufficient resources they have on the biggest threats to cybersecurity.
- **Foster cooperation**: To ensure long-term viability within the SMEs, the findings of this research suggest collaboration between the private sector, government agencies, and industries in order to offer more affordable accessibility to support, financial resources, and equipment.
- **Promote the reporting of security incidents**: To gain more insight from cyber disasters and effectively strengthen cyber resilience within the nation, this study recommends the start-up of more secure and accessible ways to report incidents.

Table 1: Summary of cybersecurity threats, challenges, and practices in SMEs

Theme	Key Findings
Common cybersecurity threats	In S.A, SMEs are constantly confronted with a range of threats such as ransomware, malware, data breaches, and phishing, which frequently arise from weak credentials, lack of proper monitoring, and outdated systems.
Challenges to implementation	Primary obstacles consist of the lack of skilled cybersecurity professionals, poor enforcement of regulations, a general lack of awareness, lack of financial resources, and the struggle to convert national policies (e.g. NCPF) into effective action.
Extent of cybersecurity implementation	Despite the growing awareness about the importance of cybersecurity, implementation remains low. SMEs frequently rely on basic security measures such as Antivirus and firewalls, while neglecting more advanced strategies such as AI-based threat detection, well-structured risk management frameworks, and the MFA.
Best practices and recommendations	To enhance cybersecurity, it is essential to engage in ongoing training, refining password policies, using budget-friendly frameworks, using the CENSOR for resource allocation, promoting cooperation between governments, SMEs, and private sectors cybersecurity providers, and setting priorities based on risks.

5. Conclusion and Future Work

This study aimed to investigate issues and challenges associated with cybersecurity experienced by SMEs in South Africa, exploring the extent of implementation of existing security measures and providing potential best practices. The research reveals a poor state of cybersecurity within SMEs regardless of the growing awareness of cybersecurity threats. These businesses face ongoing challenges in adopting cutting-edge technological solutions due to a lack of employee awareness, insufficient resources, and a shortage of skilled professionals. Moreover, the practical integration of advanced security frameworks, such as ZTA and NIST, remains limited due to their high implementation cost, despite the potential they offer, which explains the reliance of SMEs on basic security strategies, including antivirus software and password policies. Additionally, the results suggest that SMEs often opt for a reactive plan of action, prioritizing a response to incidents over proactive preparation. However, cybersecurity should be considered both a strategic and an administrative issue, rather than a technical one only, as it is an essential way to handle all these issues. For South African SMEs to enhance their cyber resilience, it is necessary to integrate cybersecurity into their organizational culture. For this reason, the ultimate necessity is for security measures that are more affordable, more tailored to the specific needs of SMEs, capable of accommodating issues associated with their activities and resource constraints, thus strengthening the resilience of SMEs in South Africa to cybersecurity threats.

For future work, - further studies could be conducted on the improvement of small and medium-sized enterprises' (SMEs) potential towards threat detection and response in real-time, by incorporating algorithms as well as data structures within a programmed information security system, which could provide more

understanding on how the usage of these approaches could be improved to be beneficial in environments with restricted resources.

AI declaration: For the development of this work, no AI tools were used.

Ethics declaration: Since the study adopts a systematic review of previous literatures which focus on secondary data publicly made available without direct human interaction or raw data collection, no ethical approval was required. However, in order to preserve academic integrity and avoid plagiarism, all sources have properly been referenced.

References

Admass, W., Munaye, Y. & Diro, A. 2024. Cyber security: State of the art, challenges and future directions. Amsterdam: Elsevier BV.

Alveera, T. & Sukira, M. 2024. Cybersecurity challenges and resilience strategies in South African SMEs. Cape Town: UCT Press.

Benjamin, L., Adegbola, A., Amajuoyi, P., Adegbola, M. & Adeusi, K. 2024. Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Vol. 19. GSC.

Bokan, B. & Santos, J. 2021. Managing cybersecurity risk using threat-based methodology for evaluation of cybersecurity architectures. New York: IEEE.

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N. & Khut, D. 2023. The new frontier of cybersecurity: Emerging threats and innovations. Toba: IEEE.

Erdogan, T., Rahman, M. & Kwon, H. 2023. Assessing cybersecurity maturity among small and medium-sized enterprises. New York: IEEE.

Fakir, J. 2024. An investigation of cybersecurity implementation challenges among South African SMEs. Master's dissertation. Johannesburg: University of the Witwatersrand.

Hermanus, K. 2023. Information security vulnerabilities in financial institutions in Cape Town. Master's dissertation. Cape Town: University of Cape Town.

Lokare, A., Bankar, S. & Mhaske, P. 2025. Integrating cybersecurity frameworks into IT security: A comprehensive analysis of threat mitigation strategies and adaptive technologies. arXiv preprint. Available at: https://doi.org/10.48550/arXiv.2502.00651. (Accessed : 15 August 2025).

Mahlangu, N. 2023. Strategies to mitigate ransomware-related cyber-attacks in South African financial institutions. Master's dissertation. Johannesburg: University of the Witwatersrand.

Mugwagwa, T., Phiri, N. & Dube, C. 2024. Cybersecurity issues in South African SMEs: Risks and solutions. Pretoria: University of South Africa Press.

Musa, L. 2023. A systems engineering approach to cybersecurity challenges in South African SMEs. Master's dissertation. Durban: University of KwaZulu-Natal.

Ncubukezi, T. and Mwansa, L., 2021. Best practices used by businesses to maintain good cyber hygiene during Covid19 pandemic. *Journal of Internet Technology and Secured Transactions*, *9*(1), pp.714-721.

Ncubukezi, T., 2022a. Human errors: A cybersecurity concern and the weakest link to small businesses. In Proceedings of the 17th *International Conference on Information Warfare and Security* (p. 395).

Ncubukezi, T., 2022b. Impact of information security threats on small businesses during the COVID-19 pandemic. In *European Conference on Cyber Warfare and Security*, 21(1), pp. 401-410.

Phahlamohlaka, J., Theron, J. & Aschmann, M. 2022. National Cybersecurity Implementation in South Africa: The Conundrum Question. Vol. 21. Pretoria: ArmisteadTec.

Pieterse, H. 2021. The cyber threat landscape in South Africa: A 10-year review. Pretoria: LINK.

Reshmi, T. 2021. Information security breaches due to ransomware attacks – a systematic literature review. Amsterdam: Elsevier Ltd.

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E. & Alabbad, D. 2023. Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. Basel: MDPI.

Shingange, J. 2022. Problematizing the South African cybersecurity policy landscape. Master's dissertation. Stellenbosch: Stellenbosch University.

Tetteh, A.K., 2024. Cybersecurity needs for SMEs. Issues in Information Systems, 25(2), pp.33–42. IACIS.

Tsiodra, M., Panda, S., Chronopoulos, M. & Panaousis, E. 2023. Cyber risk assessment and optimization: A small business case study. Vol. 1. New Jersey: IEEE.

Venkatasubramanian, D., Goyal, S., Ezhilarasan, G., Sharma, Y., Vijayalakshmi, V. & Garg, P. 2024. Evaluating the effectiveness of multi-factor authentication for preventing cyber attacks. Kamand: IEEE.