Cultivating Collective Armor: Towards a Collaborative Cybersecurity Resilience Framework for SMEs

Nangamso Mmango[1] and Tapiwa Gundu[2]
[1]University of South Africa, Pretoria, South Africa
[2]Nelson Mandela University, Gqeberha, South Africa

nangamso.mmango@yahoo.com
tapgun@gmail.com

Abstract: As Small and Medium-sized Enterprises (SMEs) increasingly integrate digital technologies into their operations, they face escalating cybersecurity threats that challenge their limited financial and human resources. Historically, cybersecurity was not a primary concern for many SMEs due to their minimal reliance on cyberinfrastructure. However, the growing dependency on digital systems has exposed them to significant risks, necessitating robust cybersecurity measures. This research introduces a cybersecurity resilience framework specifically designed to enhance the cybersecurity posture of SMEs through collaborative efforts. Drawing upon principles of collective intelligence, shared resources, and shared responsibility, the proposed framework promotes a holistic approach that merges advanced technological solutions with collaborative practices among SMEs, industry stakeholders, and governmental entities. By enabling SMEs to pool their cybersecurity resources and capabilities, the framework aims to provide a comprehensive defence against cyber threats that could not be achieved by individual entities alone. The research delves into key collaborative literature to ground the framework in proven strategies and existing successful models of collaboration. It highlights how collective action can be a powerful tool in overcoming the inherent vulnerabilities of SMEs to cyber threats. To validate the effectiveness and applicability of the framework, it went through an expert review process involving cybersecurity professionals and stakeholders in the SME sector. This study not only underscores the necessity for SMEs to adapt to the evolving cybersecurity landscape but also provides a practical blueprint for collective defence. The framework's emphasis on shared responsibility and mutual aid presents a shift from traditional, isolated cybersecurity approaches to a more integrated and cooperative strategy. This has the potential to significantly enhance the resilience of SMEs against cyber threats, safeguarding their operations and contributing to the overall stability of the digital economy. Future research directions include the application of the framework across various industries and global contexts to evaluate its versatility and impact under different regulatory and threat environments.

Keywords: SMEs, Small and medium-sized enterprises, Cybersecurity resilience, Collective intelligence, Collaboration, Information sharing

1. Introduction

In today's interconnected world, the proliferation of digital technologies has significantly transformed the business landscape, offering unprecedented opportunities for innovation, scalability, and market reach (Shahadat *et al.*, 2023). However, this digital integration also comes with heightened vulnerabilities, particularly for Small and Medium-sized Enterprises (SMEs) (Gundu and Mmango, 2024). As these enterprises increasingly depend on digital infrastructures for their operations, they become prime targets for cyber threats that are both sophisticated and relentless. Unlike larger corporations, SMEs often lack the necessary resources (financial, technical, and human) to effectively combat these cyber threats. This disparity not only places them at greater risk of cyber incidents but also potentially jeopardises their financial stability, customer trust, and long-term viability.

Traditional cybersecurity approaches, which primarily focus on individual organisations fortifying their defences, are proving insufficient under the current threat landscape. The dynamic nature of cyber threats requires more than just isolated efforts; it demands a collaborative approach to cybersecurity (Safitra, Lubis and Fakhrurroja, 2023). Recognising this need, this paper proposes a Collaborative Cybersecurity Resilience Framework specifically tailored for SMEs. This framework is designed to leverage the collective intelligence, resources, and capacities of various SMEs, industry partners, and governmental entities.

Drawing from the principles of collective intelligence and shared responsibility, the proposed framework advocates for a holistic approach that integrates technological solutions with collaborative practices. This approach not only aims to enhance the individual cybersecurity postures of SMEs but also seeks to fortify the broader business ecosystem against potential cyber threats. By fostering a culture of information sharing, collaborative threat intelligence, and joint response mechanisms, the framework empowers SMEs to collectively defend against and respond to cyber incidents.

This introduction sets the stage for a detailed exploration of the proposed framework, including its conceptual underpinnings, operational mechanisms, and potential benefits. It also outlines the structure of the paper, which will delve into relevant literature, describe the framework's components, and discuss the findings from an expert review. The ultimate goal of this research is to offer SMEs a viable solution to enhance their cybersecurity resilience and ensure their sustainable growth in the digital age.

2. Related Literature

2.1 Small and Medium-sized Enterprises (SMEs)

SMEs play a pivotal role in driving economic growth, job creation, and social development (Gherghina et al., 2020). With a diverse and vibrant entrepreneurial landscape, SMEs contribute significantly to the country's Gross Domestic Product (GDP) and provide employment opportunities, particularly in sectors such as manufacturing, agriculture, retail, and services. However, SMEs in South Africa face a unique set of challenges that can hinder their growth and sustainability. These challenges include limited access to finance, inadequate infrastructure, regulatory burdens, skills shortages, and market access constraints. Additionally, factors such as political instability, economic uncertainty, and social inequality can further exacerbate the challenges faced by SMEs.

Despite these obstacles, SMEs in South Africa demonstrate resilience, innovation, and entrepreneurial spirit. Many SMEs leverage technology and digital platforms to overcome traditional barriers and access new markets. Moreover, the COVID-19 pandemic has heightened both the vulnerabilities and resilience of SMEs in South Africa. Many SMEs have faced unprecedented challenges due to lockdown measures, supply chain disruptions, and reduced consumer demand. However, the crisis has also spurred innovation and digital adoption among SMEs, accelerating trends towards e-commerce, remote work, and digital transformation.

2.2 Challenges Faced by SMEs in South Africa

Government initiatives like the Small Enterprise Development Agency (SEDA) and the Department of Small Business Development (DSBD) provide crucial support to SMEs in South Africa (Meyburgh, 2022), though many still struggle due to limited access and extensive need. Key challenges include restricted access to finance, exacerbated by high-interest rates and stringent lending criteria (Nanziri and Wamalwa, 2021), and significant infrastructural constraints such as unreliable power and poor internet connectivity that hinder operational efficiency and growth. Additionally, SMEs face a critical shortage of skilled labour, particularly in technology and innovation-driven sectors (Shaikh et al., 2021), compounded by the brain drain phenomenon (Ahlbäck, 2015). Market access is another significant barrier, with SMEs contending with limited marketing budgets, regulatory hurdles, and intense competition from larger corporations (Scheers, 2011). The socio-political environment further complicates the landscape, requiring SMEs to be adaptable and resilient amid political and economic instability (Griffiths, Gundry and Kickul, 2013; Hamiza, Takwi and Rashid, 2020). Cybersecurity also poses a growing challenge as SMEs become more reliant on digital technologies. Many lack adequate cybersecurity measures, making them vulnerable to attacks like phishing and ransomware. Addressing these challenges requires a collective effort from financial institutions, government, and educational bodies to develop tailored solutions and robust cybersecurity frameworks that protect SMEs and ensure their sustainable growth.

2.2.1 Cybersecurity threats

Small and Medium-sized Enterprises (SMEs) in South Africa face a variety of cybersecurity risks, and this study although it has discussed several other challenges faced by SMEs, its main focus is on the cybersecurity threat challenge. One of the most common threats is phishing attacks, where SMEs are targeted with fraudulent emails designed to steal sensitive information (Naqvi et al., 2023). These businesses are also particularly vulnerable to ransomware, a type of malware that locks access to the victim’s data, often forcing them to pay a ransom to regain access (Yuryna Connolly et al., 2020). Data breaches pose another significant risk, especially as SMEs may store critical customer and financial information but typically lack the sophisticated security measures larger corporations might have (Pantelis et al., 2021). Insider threats are also a concern, arising either from negligence or malicious intent, with employees potentially exposing the company to cyber threats by mishandling data or falling for phishing scams (Gundu, Maronga and Boucher, 2019). Additionally, while advanced persistent threats (APTs) are more commonly associated with larger entities, SMEs involved in critical supply chains might also find themselves targets of these prolonged, stealthy cyberattacks. Lastly, the use of outdated and unpatched software can leave SMEs susceptible to a variety of cyber threats, further

exacerbating their vulnerability in a landscape where cyber threats are becoming increasingly sophisticated. Traditional, cybersecurity strategies typically focus on implementing individual defence mechanisms, such as firewalls, antivirus software, and employee training programs. However, these measures often prove inadequate in addressing the dynamic and sophisticated nature of modern cyber threats (Mitrofan, Cruceru and Barbu, 2020). Moreover, SMEs may lack the financial resources and technical expertise required to deploy and maintain robust cybersecurity solutions effectively (Gundu and Mmango, 2024). In light of these challenges, there is a pressing need for a collaborative approach to cybersecurity that leverages collective intelligence and shared responsibility within the SME ecosystem. By pooling resources, knowledge, and expertise, SMEs can enhance their cybersecurity resilience and better defend against cyber threats.

3. Research Methodology

The research aims to establish a robust foundation by integrating the Qualitative Research Approach (QRA) and Design Science Research Methodology (DSRM). Qualitative research was the most suitable for this study as it seeks to uncover underlying meanings and perspectives of collaboration, and cybersecurity issues related to start-up entrepreneurs through literature review. This then highlighted the aspects that will make up the proposed framework for cybersecurity management of start-up entrepreneurs and their collaboration for cybersecurity resilience. Through the thematic analysis technic, this qualitative approach seeks to provide rich descriptions and interpretations of social phenomena, aiding in deriving meaningful conclusions. Design Science Research Methodology (DSRM) offers a systematic framework within Information Systems (IS) research for developing innovative solutions to real-world problems (Dresch, Lacerda and Antunes, 2015). Because DSRM priorities the creation of practical artefacts and solutions, that is the reason it was chosen for this study.

3.1 Design Science Research Methodology

The DSRM process involves problem identification, objective definition, design and development of the artifact, demonstration of its functionality, and rigorous evaluation to assess its performance and impact as dipticted in Figure 1. By communicating the research findings to relevant stakeholders, DSRM ensures the dissemination of outcomes to inform future research and practice. Through the application of DSRM, the research endeavoured to create practical framework aimed at addressing the challenges faced by Small and Medium-sized Enterprises (SMEs) in cybersecurity resilience.

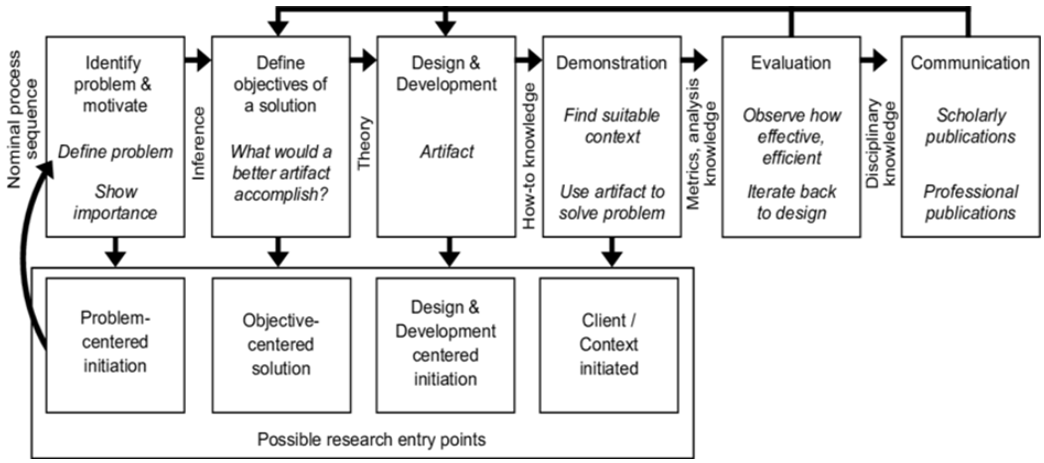

Figure 1: DSRM Process (Dresch, Lacerda and Antunes, 2015)

3.1.1 Problem identification

The identified problem is cyber threats that represent a formidable obstacle to the success of SMEs, presenting a diverse range of risks from cyberattacks to data breaches. Cyberattacks can disrupt essential business processes, leading to costly downtime and productivity losses. Additionally, financial implications such as theft of funds or ransom payments can strain SME budgets and jeopardise financial stability and reputation.

3.1.2 Objectives definition

In addressing the significant threat posed by cyberattacks and data breaches to SMEs, the objectives of this study are to identify and assess potential threats and design a framework, aimed at enhancing cybersecurity resilience among SMEs through a collaborative approach. The framework leverages shared intelligence and resources, improving SMEs' ability to withstand cyberattacks through collective risk assessments, shared threat intelligence, and coordinated incident responses. The last objective involves expert review to refine the framework for practical application.

3.1.3 Design and development

Building on the findings of the literature review, the design and development phase centred on crafting a comprehensive framework aimed at assisting SMEs in enhancing their cybersecurity posture through collaboration. The framework was tailored to give guidance on how they can collaborate to address the specific needs and challenges faced by SMEs, combating their drawbacks in terms of factors such as limited resources, technical expertise, and evolving threat landscapes.

3.1.4 Demonstration

After the development of the first version of the framework, the next critical step was to demonstrate its functionality and effectiveness in addressing the identified problem. This demonstration was provided to the experts who were evaluating the framework.

3.1.5 Evaluation

Experts in cybersecurity and entrepreneurship undertook a rigorous evaluation of the framework, a crucial step in the research or development process. This evaluation aimed to assess the framework's usability and anticipated impact. This thorough evaluation process ensures that the framework effectively enhances cybersecurity measures, mitigating risks and safeguarding against cyber threats while promoting changes in business behaviour towards prioritising cybersecurity.

3.1.6 Communication

This study employs various channels of communication to disseminate research findings, including academic conferences, journal publications, social media platforms, SMEs imbizo (conventions), business summits, business blogs, and other relevant platforms. The aim is to ensure that the insights gained from the study, including the developed framework, reach a diverse range of stakeholders. The study utilises social media platforms to reach a wider audience, including SMEs, policymakers, and practitioners, facilitating broader discussions and knowledge dissemination.

4. Introducing the Proposed Framework

The section outlines the proposed framework aimed at strengthening the cybersecurity defences of SMEs through a collaborative approach. It details the essential components of the framework, including its foundation based on literature.

4.1 Foundation in the Literature

The constructs of the "Collaborative Cybersecurity Resilience Framework for SMEs" framework are deeply rooted in established literature on collaboration as summarised in Table 1. This section outlines how each component of the framework aligns with recognised practices, principles, and research findings from the literature on collaboration. By grounding our approach in a strong theoretical basis, we ensure that the strategies implemented are not only practical but also supported by academic and professional studies.

Table 1: Summary of Literature review

Theme	Short Description	Articles
Define the Need and Scope	**Identify Risks:** Assess the common cybersecurity risks facing start-ups in your network or region. **Determine Scope:** Decide whether the collaboration will focus on specific sectors, technologies, or geographical areas.	(Nguyen *et al.*, 2020; Pedersen *et al.*, 2021; Busch *et al.*, 2024)
Build a Core	**Assemble a Leadership Group**: Gather a small team of committed individuals	(Sun *et al.*, 2020; Tang, Vezzani and

Theme	Short Description	Articles
Team	from different start-ups who are passionate about cybersecurity. **Define Roles**: Assign roles such as project leader, financial advisor, technical expert, and communications officer.	Eriksson, 2020; Devi *et al.*, 2023)
Conduct Preliminary Research	**Understand Best Practices:** Research existing cybersecurity frameworks and best practices. Consider frameworks like NIST or ISO/IEC standards as references. **Survey Potential Participants**: Engage with other start-ups to understand their specific needs and the challenges they face in cybersecurity.	(Andrews-Todd and Forsyth, 2020; Ramezani and Camarinha-Matos, 2020)
Prepare a Clear Value Proposition	**Highlight Benefits:** Emphasize the mutual benefits such as shared knowledge, reduced costs through pooled resources, and enhanced collective security. **Address Specific Needs:** Tailor your message to show how the collaboration addresses specific cybersecurity challenges faced by each startup.	(Afifi, Kalra and Ghazal, 2020; Penuel *et al.*, 2020; Xu, Wang and Wang, 2023)
Use Existing Networks	**Leverage Contacts**: Start with your existing business contacts, industry groups, and professional networks to find interested parties. **Attend Industry Events**: Participate in startup conferences, cybersecurity seminars, and business networking events to meet potential collaborators.	(Ramezani and Camarinha-Matos, 2020; Sun *et al.*, 2020)
Organise an Introductory Meeting or Event	**Host a Webinar or Workshop**: Provide a platform where startups can learn about cybersecurity threats and the importance of collaborative defence strategies. **Facilitate Discussions**: Allow for open discussion so that participants can voice their concerns and interests.	(Soller, Wiebe and Lesgold, 1994; Steiber and Alänge, 2020; Busch *et al.*, 2024)
Follow Up Persistently	**Regular Updates:** Keep potential collaborators informed with updates on progress, developments, and upcoming meetings. **Personal Engagement**: Engage personally with key decision-makers to understand their reservations and work through any objections.	(Hwang and Cha, 2018; Afifi, Kalra and Ghazal, 2020; Nguyen *et al.*, 2020)
Facilitate Easy Onboarding	**Simplify Joining Process**: Make the process of joining the collaboration as simple and straightforward as possible. **Provide Support**: Offer support for new members to integrate into the network smoothly, including technical assistance and access to shared resources.	(Penuel *et al.*, 2020; Sutrisno *et al.*, 2023; Xu, Wang and Wang, 2023)
Develop Shared Tools and Resources	**Identify Resources**: Determine what resources are needed, such as funding, technical tools, and human capital. **Resource Sharing Agreements**: Develop agreements on how resources will be shared and managed.	(Steiber and Alänge, 2020; Tang, Vezzani and Eriksson, 2020; Devi *et al.*, 2023; Sutrisno *et al.*, 2023)
Showcase Immediate and Long-Term Benefits	**Immediate Gains:** Demonstrate quick wins that can be achieved through collaboration, such as immediate access to shared cybersecurity tools or collective bargaining power. **Long-Term Strategy**: Outline the long-term strategic advantages, like ongoing improvement in cybersecurity posture and resilience against future threats.	(Hwang and Cha, 2018; Andrews-Todd and Forsyth, 2020; Al-Omoush, de Lucas and del Val, 2023)
Outreach and Expansion	**Share Successes:** Publicize successful outcomes to attract more participants and support. **Expand Network:** Consider expanding the collaboration as more startups and resources become available.	(Soller, Wiebe and Lesgold, 1994; Pedersen *et al.*, 2021; How and Cheah, 2023)

4.2 Collaborative Cybersecurity Resilience Framework for SMEs

The framework includes actionable strategies and steps for creating a cohesive and proactive collaboration among participating SMEs as illustrated in Figure 2. Each component of the framework is clearly defined and designed for easy adoption and efficient coordination among the interested SMEs.

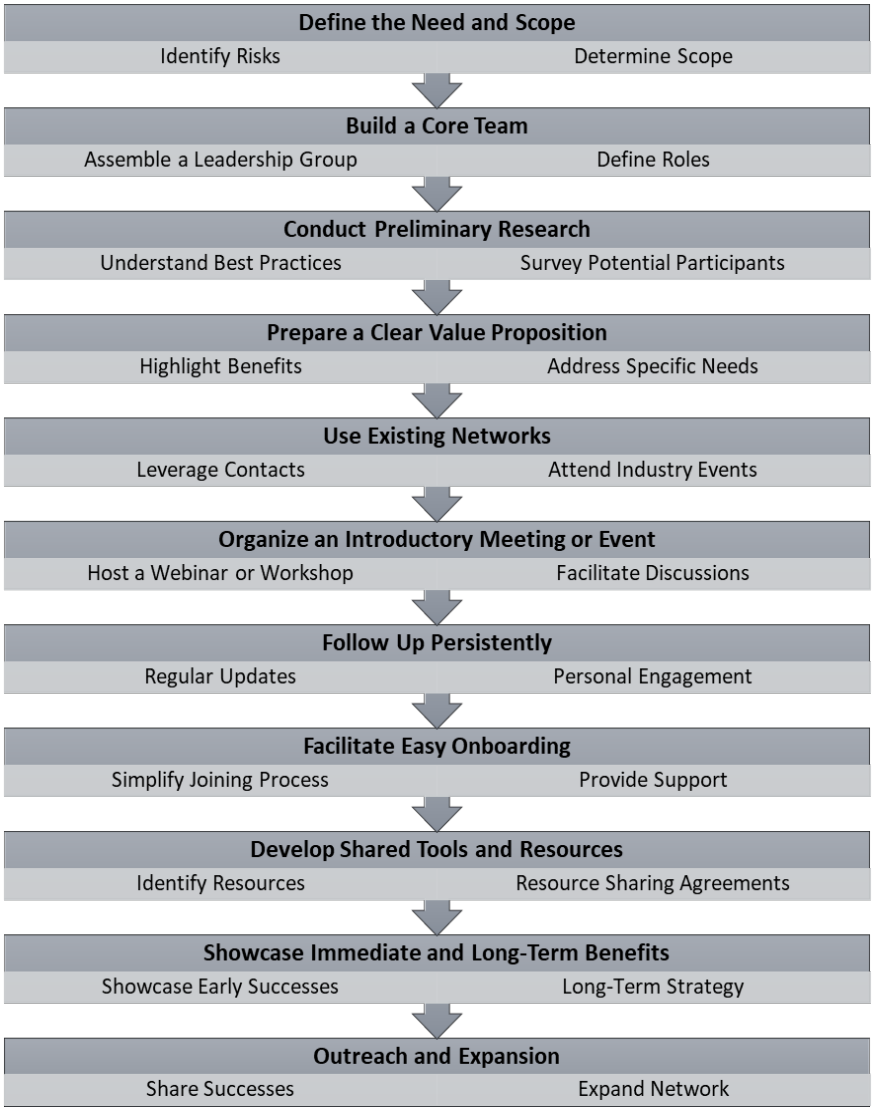

Figure 2: Collaborative Cybersecurity Resilience Framework for SMEs

Implementing the framework provides several significant benefits to SMEs. Through collaborative risk assessments, SMEs gain a comprehensive understanding of potential cybersecurity threats and vulnerabilities. This collective intelligence allows for better-informed decision-making and prioritisation of security efforts, focusing resources on the most critical areas. The shared understanding of risks leads to a more robust defence against cyber threats. The framework leads to Information-sharing platforms that provide a centralized venue for exchanging real-time threat intelligence, best practices, and mitigation strategies. This ensures that all participating SMEs have access to the latest information and can learn from each other's experiences and insights. Such platforms also facilitate rapid dissemination of information about emerging threats and effective defensive measures, keeping all members up-to-date and better prepared.

Engaging in policy advocacy and collaboration with regulatory bodies enables SMEs to contribute to the development of cybersecurity policies that reflect their interests and needs. This active participation helps shape a regulatory environment that supports secure, sustainable growth for SMEs, ensuring that their voices are heard and considered in policy decisions.

5. Discussion

Securing SMEs from cyber threats using collaboration yields a multitude of benefits from safeguarding their operations, finances, and reputation. By ensuring the protection of sensitive customer and business data, SMEs mitigate the risk of data breaches and safeguard against both financial and reputational damage. This is crucial for maintaining the trust of customers and partners, who expect their data to be handled securely. Defending against cyber threats also ensures uninterrupted business operations, minimizing downtime and maintaining productivity levels. This continuity is essential for safeguarding revenue streams and maintaining customer satisfaction, as operational disruptions can lead to significant losses and damage to customer relationships.

Enhanced cybersecurity protects SMEs from financial losses associated with cyberattacks, which can include ransomware payments, legal fees, regulatory fines, and the costs related to data recovery and system restoration. By preserving their financial stability, SMEs can allocate resources more effectively towards growth and development rather than crisis management. A secure operation also preserves an SME's reputation and trustworthiness among customers, partners, and stakeholders. A single data breach can cause irreparable damage to a brand's reputation, making cybersecurity a critical component of reputation management. Demonstrating strong cybersecurity measures can also provide SMEs with a competitive advantage in the marketplace. It instils confidence in customers and partners, distinguishing these businesses from less secure competitors. This advantage is increasingly important as customers become more aware of and concerned about digital security.

Compliance with cybersecurity regulations and standards is another critical benefit, helping SMEs avoid legal liabilities, penalties, and the reputational damage that can result from non-compliance. This fosters trust and credibility within the regulatory landscape, which is becoming more stringent as the digital threat landscape evolves. A secure SME is also better positioned to pursue growth opportunities, expand into new markets, and attract investment. Stakeholders and potential investors recognize a commitment to cybersecurity and effective risk management as key indicators of a company's long-term viability and governance standards. Finally, effective cybersecurity measures provide SME owners and stakeholders with peace of mind, knowing that their business and assets are protected against cyber threats. This allows them to focus more on strategic initiatives and business growth, rather than being preoccupied with the potential for digital disruptions.

5.1 Anticipated Challenges of Implementing the Collaborative Cybersecurity Resilience Framework for Start-Up Entrepreneurs

While the framework presents a promising approach to enhancing cybersecurity resilience among SMEs, several anticipated challenges may arise during its implementation. One significant challenge could be the reluctance of some SMEs to engage in collaborative efforts due to concerns about sharing sensitive information or perceived competition with other businesses. Overcoming this resistance will require fostering a culture of trust and transparency among participants, as well as emphasizing the mutual benefits of collaboration in strengthening cybersecurity defences. Many SMEs operate with limited financial and human resources, making it challenging to allocate resources for cybersecurity initiatives. Implementing the framework's capacity-building initiatives and participating in collaborative activities may require SMEs to invest additional time, money, and personnel, which could strain their already stretched resources.

Compliance with existing legal and regulatory frameworks, such as data protection laws and industry-specific regulations, may pose challenges to information sharing and collaboration among SMEs. Navigating these legal and regulatory complexities while ensuring privacy and confidentiality will require careful consideration and possibly advocacy efforts to address any barriers that hinder collaboration.

SMEs may lack the technical expertise or infrastructure to implement advanced cybersecurity measures or participate effectively in information-sharing platforms. Providing accessible and user-friendly tools and resources, as well as offering training and support, will be essential to overcoming these technical barriers and ensuring broad participation in the framework.

Maintaining long-term engagement and commitment to the framework, as well as adapting it to evolving cyber threats and technological advancements, will be critical for its sustainability. SMEs may face challenges in keeping up with rapid changes in the cybersecurity landscape and may require ongoing support and guidance to remain resilient over time. Addressing these anticipated challenges will require proactive measures, collaboration among stakeholders, and ongoing evaluation and refinement of the framework to ensure its effectiveness and relevance in safeguarding SMEs against cyber threats.

6. Conclusion

SMEs face a unique set of challenges, including limited access to finance, inadequate infrastructure, regulatory burdens, skills shortages, and market access constraints. However, they demonstrate resilience and innovation, leveraging technology and government support initiatives to overcome barriers and drive economic growth. The research highlights the growing vulnerability of Small and Medium-sized Enterprises (SMEs) to cybersecurity threats as they navigate the digital landscape. It emphasises these SMEs do not have adequate knowledge and resources to address these threats. To address this challenge, the study introduces a framework, which advocates for a collaborative approach to bolstering cybersecurity resilience among SMEs. The framework is grounded in principles of collective intelligence and shared accountability, aiming to merge technological solutions with collaborative practices involving SMEs, industry partners, and governmental bodies.

The research methodology in this study integrates the qualitative research approach with Design Science Research Methodology (DSRM), emphasising the development of a practical solution to a real-world problem. The literature review gathered relevant insights from reputable academic databases, employing rigorous selection criteria to ensure the credibility and relevance of sources.

The proposed "Collaborative Cybersecurity Resilience Framework for SMEs" offers a proactive and collaborative approach to cybersecurity, recognising the interconnectedness of SMEs and their shared vulnerabilities to cyber threats. By embracing collective intelligence and shared responsibility, SMEs can enhance their cybersecurity posture and mitigate the risks posed by increasingly sophisticated cyber-attacks.

Future studies could assess the framework's applicability and effectiveness across various geographical regions and industry sectors. This would help to understand how cultural, economic, and regulatory differences impact the implementation and success of collaborative cybersecurity practices.

Acknowledgements

We would like to extend my sincere gratitude to Nelson Mandela University for their invaluable support and funding, which made this research project possible. The financial assistance provided by the university significantly contributed to the successful completion of this study. We would also like to express my deepest appreciation to Matlafatso Financial Accountants and Tax Advisors for their generous financial support. Their contributions were instrumental in advancing this research and achieving the project's objectives.

References

Afifi, M., Kalra, D. and Ghazal, T. (2020) 'Integration of Collaboration Systems in Hospitality Management as a Comprehensive Solution', *International Journal of Advanced Science and Technology*, 29, pp. 3155–3173.

Ahlbäck, M. (2015) 'How to avoid brain drain? Knowledge management as a competitive advantage. Case: Finnish SME growth companies'. Available at: https://aaltodoc.aalto.fi/handle/123456789/19398 (Accessed: 5 May 2024).

Al-Omoush, K.S., de Lucas, A. and del Val, M.T. (2023) 'The role of e-supply chain collaboration in collaborative innovation and value-co creation', *Journal of Business Research*, 158, p. 113647. Available at: https://doi.org/10.1016/j.jbusres.2023.113647.

Andrews-Todd, J. and Forsyth, C.M. (2020) 'Exploring social and cognitive dimensions of collaborative problem solving in an open online simulation-based task', *Computers in Human Behavior*, 104, p. 105759. Available at: https://doi.org/10.1016/j.chb.2018.10.025.

Busch, T. *et al.* (2024) 'Moving beyond "the" business case: How to make corporate sustainability work', *Business Strategy and the Environment*, 33(2), pp. 776–787. Available at: https://doi.org/10.1002/bse.3514.

Devi, E.T. *et al.* (2023) 'Designing an information-sharing system to improve collaboration culture: a soft systems methodology approach in the digital service creation process', *Journal of Enterprise Information Management*, 36(5), pp. 1240–1269. Available at: https://doi.org/10.1108/JEIM-08-2022-0294.

Dresch, A., Lacerda, D.P. and Antunes, J.A.V. (2015) 'Design Science Research', in A. Dresch, D.P. Lacerda, and J.A.V. Antunes Jr (eds) *Design Science Research: A Method for Science and Technology Advancement*. Cham: Springer International Publishing, pp. 67–102. Available at: https://doi.org/10.1007/978-3-319-07374-3_4.

Gherghina, Ștefan C. *et al.* (2020) 'Small and Medium-Sized Enterprises (SMEs): The Engine of Economic Growth through Investments and Innovation', *Sustainability*, 12(1), p. 347. Available at: https://doi.org/10.3390/su12010347.

Griffiths, M.D., Gundry, L.K. and Kickul, J.R. (2013) 'The socio-political, economic, and cultural determinants of social entrepreneurship activity: An empirical examination', *Journal of Small Business and Enterprise Development*. Edited by C. Henry and L. Treanor, 20(2), pp. 341–357. Available at: https://doi.org/10.1108/14626001311326761.

Gundu, T., Maronga, M.I. and Boucher, D. (2019) 'Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace', in *Proceedings of 4th International Conference on the*, pp. 85–94.

Gundu, T. and Mmango, N. (2024) 'A Cybersecurity Collaborative Model: Best Practices Sharing Among South African Tourism and Hospitality Businesses', *International Conference on Tourism Research*, 7(1), pp. 222–231. Available at: https://doi.org/10.34190/ictr.7.1.2159.

Hamiza, O., Takwi, F. and Rashid, T. (2020) 'The Role of Socio-Political Environment in Business Success: A Case of Small Businesses in Uganda', *International Journal of Academic Research in Business and Social Sciences*, 10. Available at: https://doi.org/10.6007/IJARBSS/v10-i10/8006.

How, M.-L. and Cheah, S.-M. (2023) 'Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era', *Businesses*, 3(4), pp. 585–605. Available at: https://doi.org/10.3390/businesses3040036.

Hwang, I. and Cha, O. (2018) 'Examining technostress creators and role stress as potential threats to employees' information security compliance', *Computers in Human Behavior*, 81, pp. 282–293. Available at: https://doi.org/10.1016/j.chb.2017.12.022.

Meyburgh, M. (2022) 'Funding for small businesses in South Africa', *TAXtalk*, 2022(95), pp. 57–60. Available at: https://doi.org/10.10520/ejc-taxtalk_v2022_n95_a15.

Mitrofan, A.-L., Cruceru, E.-V. and Barbu, A. (2020) 'Determining the Main Causes that Lead to Cybersecurity Risks in SMEs', *Business Excellence and Management*, 10(4), pp. 38–48.

Nanziri, L.E. and Wamalwa, P.S. (2021) 'Finance for SMEs and its effect on growth and inequality: evidence from South Africa', *Transnational Corporations Review*, 13(4), pp. 450–466. Available at: https://doi.org/10.1080/19186444.2021.1925044.

Naqvi, B. *et al.* (2023) 'Mitigation strategies against the phishing attacks: A systematic literature review', *Computers & Security*, 132, p. 103387. Available at: https://doi.org/10.1016/j.cose.2023.103387.

Nguyen, T. *et al.* (2020) 'How does integrated knowledge translation (IKT) compare to other collaborative research approaches to generating and translating knowledge? Learning from experts in the field', *Health Research Policy and Systems*, 18(1), p. 35. Available at: https://doi.org/10.1186/s12961-020-0539-6.

Pantelis, G. *et al.* (2021) 'On Strengthening SMEs and MEs Threat Intelligence and Awareness by Identifying Data Breaches, Stolen Credentials and Illegal Activities on the Dark Web', in *Proceedings of the 16th International Conference on Availability, Reliability and Security*. New York, NY, USA: Association for Computing Machinery (ARES '21), pp. 1–7. Available at: https://doi.org/10.1145/3465481.3469201.

Pedersen, E.R.G. *et al.* (2021) 'Toward Collaborative Cross-Sector Business Models for Sustainability', *Business & Society*, 60(5), pp. 1039–1058. Available at: https://doi.org/10.1177/0007650320959027.

Penuel, W.R. *et al.* (2020) 'Principles of Collaborative Education Research With Stakeholders: Toward Requirements for a New Research and Development Infrastructure', *Review of Educational Research*, 90(5), pp. 627–674. Available at: https://doi.org/10.3102/0034654320938126.

Ramezani, J. and Camarinha-Matos, L.M. (2020) 'Approaches for resilience and antifragility in collaborative business ecosystems', *Technological Forecasting and Social Change*, 151, p. 119846. Available at: https://doi.org/10.1016/j.techfore.2019.119846.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023) 'Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity', *Sustainability*, 15(18), p. 13369. Available at: https://doi.org/10.3390/su151813369.

Scheers, L.V. (2011) 'SMEs' marketing skills challenges in South Africa', *African Journal of Business Management*, 5(13), pp. 5048–5056. Available at: https://doi.org/10.5897/AJBM10.007.

Shahadat, M.M.H. *et al.* (2023) 'Digital Technology Adoption in SMEs: What Technological, Environmental and Organizational Factors Influence in Emerging Countries?', *Global Business Review*, p. 09721509221137199. Available at: https://doi.org/10.1177/09721509221137199.

Shaikh, D.A.A. *et al.* (2021) 'A Two-Decade Literature Review on Challenges Faced by SMEs in Technology Adoption'. Rochester, NY. Available at: https://papers.ssrn.com/abstract=3823849 (Accessed: 5 May 2024).

Soller, A., Wiebe, J. and Lesgold, A. (1994) 'A Machine Learning Approach to Assessing Knowledge Sharing During Collaborative Learning Activities', in *Computer Support for Collaborative Learning*. Routledge.

Steiber, A. and Alänge, S. (2020) 'Corporate-startup collaboration: effects on large firms' business transformation', *European Journal of Innovation Management*, 24(2), pp. 235–257. Available at: https://doi.org/10.1108/EJIM-10-2019-0312.

Sun, C. *et al.* (2020) 'Towards a generalized competency model of collaborative problem solving', *Computers & Education*, 143, p. 103672. Available at: https://doi.org/10.1016/j.compedu.2019.103672.

Sutrisno, S. *et al.* (2023) 'The Role of Information Technology in Driving Innovation and Entrepreneurial Business Growth', *Jurnal Minfo Polgan*, 12(1), pp. 586–597. Available at: https://doi.org/10.33395/jmp.v12i1.12463.

Tang, T., Vezzani, V. and Eriksson, V. (2020) 'Developing critical thinking, collective creativity skills and problem solving through playful design jams', *Thinking Skills and Creativity*, 37, p. 100696. Available at: https://doi.org/10.1016/j.tsc.2020.100696.

Xu, E., Wang, W. and Wang, Q. (2023) 'The effectiveness of collaborative problem solving in promoting students' critical thinking: A meta-analysis based on empirical literature', *Humanities and Social Sciences Communications*, 10(1), pp. 1–11. Available at: https://doi.org/10.1057/s41599-023-01508-1.

Yuryna Connolly, L. *et al.* (2020) 'An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability', *Journal of Cybersecurity*, 6(1), p. tyaa023. Available at: https://doi.org/10.1093/cybsec/tyaa023.