Fortifying the Digital Frontier: Tailoring Cybersecurity Strategies for SMEs in Developing Economies

Table of Contents

[Summary 1](#_Toc163321610)

[Introduction 1](#_Toc163321611)

[Cybersecurity Frameworks 2](#_Toc163321612)

[NIST Cybersecurity Framework 2](#_Toc163321613)

[ISO/IEC 27001 3](#_Toc163321614)

[CIS Controls 3](#_Toc163321615)

[Challenges and Strategies in Developing Economies 4](#_Toc163321616)

[Challenges in Developing Economies 4](#_Toc163321617)

[Strategic Approaches to Overcome Challenges 4](#_Toc163321618)

[Operational Realities for SMEs in Cybersecurity 5](#_Toc163321619)

[Strategic Approaches for SMEs 5](#_Toc163321620)

[Framework Customisation for SMEs 6](#_Toc163321621)

[Key Insights and Strategic Pathways 8](#_Toc163321622)

[Concluding Reflections 8](#_Toc163321623)

[Citations 10](#_Toc163321624)

# Summary

This paper addresses the critical challenge of enhancing cybersecurity among Small and Medium Enterprises (SMEs) in developing economies, underscored by the expanding digital landscape and the escalating sophistication of cyber threats. Recognising the compounded vulnerabilities due to limited resources, varied digital literacy levels, and a general absence of specialised cybersecurity expertise, this research delves into a systematic evaluation of cybersecurity frameworks, best practices, standards, and controls, with a keen focus on their adaptability and applicability to the unique operational realities of SMEs.

The NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Controls are central to the investigation for their comprehensive yet flexible approach towards managing cybersecurity risks. These frameworks, characterised by their encompassing nature—spanning identification, protection, detection, response, and recovery processes—were assessed for their practicality and customisation potential in the context of SME operational and resource constraints.

The study further explores essential cybersecurity best practices pivotal for SMEs, including regular risk assessments, data encryption, implementing Multi-Factor Authentication (MFA), and promoting security awareness among employees. These practices lay the foundational pillars for establishing a robust cybersecurity posture, offering a buffer against prevalent cyber threats.

Addressing the gap in the current literature, this paper proposes tailored strategies for the effective implementation of cybersecurity measures within SMEs operating in developing economies. It prioritises actions that deliver substantial security enhancements at minimal costs and simplifies complex cybersecurity guidelines into executable steps. The paper advocates for leveraging support from governmental and industrial sectors and engaging in cybersecurity communities to foster a collective defence approach.

The paper concludes by underscoring the imperative need for SMEs in developing economies to adopt and effectively implement tailored cybersecurity frameworks, standards, and controls to safeguard their operational integrity and promote sustainable growth, calling for further research into innovative strategies that can alleviate implementation challenges and enhance the cybersecurity culture among SMEs, thereby fortifying their defences against an ever-evolving cyber threat landscape. This research contributes significantly to cybersecurity by offering a structured analysis of the challenges and solutions pertinent to SMEs in developing economies, highlighting the critical role of tailored cybersecurity measures in mitigating risks and enhancing resilience.

# Introduction

As businesses embrace digital transformation, Small and Medium Enterprises (SMEs) must navigate a complex cybersecurity landscape. Relying on digital technologies for operational efficiency, market expansion, and customer engagement exposes SMEs to cybersecurity threats. In developing economies, where SMEs are often the backbone of the economy, resource constraints, varying levels of digital literacy, and infrastructural limitations can exacerbate these risks. It's crucial for SMEs to implement adequate cybersecurity measures to ensure business continuity, protect sensitive data, and maintain customer trust.

The field of cybersecurity is expansive and constantly evolving, with fresh hazards arising as rapidly as technology advances. Consequently, various cybersecurity frameworks, best practices, standards, and controls have been established to assist businesses in safeguarding themselves against these threats (Dedeke & Masterson, 2019). However, implementing and applying these cybersecurity measures can be particularly daunting for small and medium-sized enterprises (SMEs) in developing economies (Kabanda, et al., 2018) (The European Union Agency for Cybersecurity, 2021). These obstacles arise from a scarcity of financial and human resources, inadequate specialised knowledge, and the dynamic nature of cyber threats, necessitating the continuous monitoring and updating of cybersecurity protocols (Perozzo, et al., 2022) (Kshetri, 2010) (Palhad & Civilcharran, 2023).

Within this context, developing a cybersecurity threat mirror tailored to address the unique needs of small and medium-sized enterprises (SMEs) in developing economies is essential and reasonable. This undertaking calls for thoroughly exploring existing cybersecurity frameworks, including the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, to assess their applicability, flexibility, and efficacy within the SME context. Additionally, it requires examining strategic methods to overcome operational challenges, using custom-designed cybersecurity frameworks, and mobilising support from the governmental, private sector, and international entities (Karake, et al., 2019) (Teufel, et al., 2020).

This paper aims to provide a thorough and informative guide on cybersecurity for small and medium-sized enterprises (SMEs) in developing economies. It aims to shed light on essential frameworks, best practices, and strategic pathways to achieve a robust cybersecurity posture. By navigating the unique challenges and leveraging potential support mechanisms, SMEs can embark on a journey toward enhancing their cybersecurity posture and fortifying their position in the digital economy. This exploration endeavours to equip SMEs with the necessary knowledge and tools to navigate the cybersecurity landscape effectively, ensuring their resilience against an ever-evolving array of cyber threats.

# Cybersecurity Frameworks

## NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is designed to help organisations manage and mitigate cybersecurity risk (National Institute of Standards and Technology, 2024). It is structured around five core functions that form the backbone of a comprehensive cybersecurity program:

1. Identify: Establishing a baseline understanding of the organisation's systems, assets, data, and capabilities, which are critical to managing cybersecurity risk.
2. Protect: Implementing safeguards to ensure delivery of critical infrastructure services.
3. Detect: Developing and implementing appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond: Taking action regarding a detected cybersecurity incident.
5. Recover: Maintaining plans for resilience and restoring any capabilities or services impaired due to a cybersecurity incident.

The flexibility of the NIST CSF is critical for SMEs. Small businesses can focus on the "Identify" and "Protect" functions as foundational steps, prioritising asset management, risk assessment, and protective technologies tailored to their needs and resources.

* Identify: SMEs should start by thoroughly inventorying their digital and physical assets to understand what needs to be protected.
* Protect: Basic cybersecurity measures, including employee training, access control, and data encryption, can be effective starting points.

This approach allows SMEs to gradually build their cybersecurity capabilities without overwhelming their resources.

## ISO/IEC 27001

ISO/IEC 27001 is an international standard for managing information security. It outlines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The standard is based on a risk management process designed to apply to any organisation (Watkins, 2022).

SMEs can benefit from ISO/IEC 27001 by focusing on the most relevant aspects of the standard that apply to their business. Implementing an ISMS can help SMEs systematically manage their information security risks, including legal, physical, and technical controls.

* SMEs should start by identifying their most sensitive information and assessing potential risks.
* Implementing critical controls, such as access management, incident management, and information security policies, can significantly improve security.

Adopting ISO/IEC 27001 can enhance client trust and open new business opportunities by demonstrating a commitment to information security.

## CIS Controls

The Critical Security Controls for Effective Cyber Defence (CIS Controls) offer a prioritised set of actions for cyber defence that provide specific and actionable ways to stop today's most pervasive and dangerous attacks (Center for Internet Security, n.d.). The controls are divided into basic, foundational, and organisational categories, each addressing a specific aspect of cybersecurity.

SMEs can start with the basic controls, which cover essential hygiene and are designed to be implementable even by organisations with limited resources:

1. Inventory and Control of Hardware Assets: Knowing what devices are connected to the network.
2. Inventory and Control of Software Assets: Understanding and managing the software used in the organisation.
3. Continuous Vulnerability Management: Regularly identifying, assessing, and mitigating vulnerabilities.
4. Controlled Use of Administrative Privileges: Managing the use and access of administrative accounts.
5. Secure Configuration for Hardware and Software: Establishing, maintaining, and enforcing security configurations.

By focusing on these basic controls, SMEs can significantly reduce their cyber risk exposure with manageable effort and cost.

Each of these frameworks provides a different approach to cybersecurity. Still, all emphasise the importance of risk management, the need for a tailored approach based on the organisation's specific context, and the critical role of leadership in cybersecurity efforts. For SMEs, starting with foundational aspects of these frameworks and gradually building a more comprehensive cybersecurity program as resources allow is a practical strategy (Australian Cyber Security Centre, 2017). Collaboration through industry partnerships or government programs can also provide additional support and resources for implementing these frameworks.

# Challenges and Strategies in Developing Economies

Addressing the challenges and outlining practical strategies for implementing cybersecurity frameworks in SMEs, particularly in developing economies, requires a nuanced understanding of these entities' specific obstacles. These challenges can significantly impact adopting and maintaining robust cybersecurity practices (Van Dijk, 2022) (Kabanda, et al., 2018) (PricewaterhouseCoopers, 2021) (Help Net Security, 2021).

## Challenges in Developing Economies

1. Limited Financial Resources: SMEs often operate with tight budgets, making it difficult to allocate funds for cybersecurity measures, which they might see as non-essential overhead rather than a critical investment.
2. Lack of Cybersecurity Awareness: SMEs in developing economies are generally unaware of cybersecurity risks and best practices. This knowledge gap can lead to underestimating the importance of cybersecurity and not taking the necessary precautions.
3. Insufficient Access to Cybersecurity Expertise: Developing economies may have a limited pool of cybersecurity professionals. SMEs struggle to find and afford skilled cybersecurity staff to design and implement security measures.
4. Regulatory and Compliance Challenges: Navigating the complex landscape of laws and regulations regarding data protection and cybersecurity can be daunting. SMEs might lack the legal expertise to ensure compliance, especially in international trade.
5. Technology Infrastructure Gaps: In some developing economies, the technology infrastructure might not be robust enough to support advanced cybersecurity measures. Limited internet bandwidth and outdated hardware can hinder the implementation of security solutions.

## Strategic Approaches to Overcome Challenges

Financial Resource Allocation

* Cost-effective Solutions: Encourage the adoption of free or low-cost cybersecurity tools and services that can provide essential protection without significant investment. Examples include open-source antivirus software, firewalls, and encryption tools.
* Government Subsidies and Incentives: Advocate for government programs that offer financial assistance, subsidies, or tax incentives for SMEs to invest in cybersecurity infrastructure and training.

Enhancing Cybersecurity Awareness

* Education and Training Programs: Implement national or regional campaigns to raise awareness about cybersecurity risks and best practices. These programs could include workshops, online courses, and resources tailored to the needs of SME owners and employees.
* Industry Partnerships: Develop partnerships between SMEs, cybersecurity firms, and academic institutions to facilitate knowledge exchange and provide access to the latest cybersecurity research and technologies.

Access to Cybersecurity Expertise

* Shared Security Services: Promote models that allow SMEs to share access to cybersecurity professionals or services. This could include cooperative groups that hire a cybersecurity team to serve multiple SMEs, reducing individual costs.
* Cybersecurity as a Service (CaaS): Encourage the use of CaaS models, where SMEs can outsource their cybersecurity needs to specialised firms. This approach can provide access to high-level expertise without needing in-house staff.

Navigating Regulatory and Compliance Challenges

* Simplified Guidelines: Work with regulatory bodies to develop simplified cybersecurity compliance guides tailored to SMEs. These guides can help demystify legal requirements and provide clear steps for compliance.
* Compliance Assistance Programs: Establish programs to assist SMEs in meeting regulatory requirements, possibly including audits, compliance checklists, and advisory services.

Addressing Technology Infrastructure Gaps

* Public-Private Infrastructure Development: Collaborate with private sector partners to invest in technology infrastructure improvements that support cybersecurity needs, such as more reliable internet service and modern hardware and software access.
* Cloud-Based Solutions: Promote cloud-based cybersecurity services, which can offer SMEs advanced security measures without substantial internal hardware and can be scaled according to the SME's size and needs.

The successful implementation of cybersecurity frameworks in SMEs within developing economies hinges on addressing these challenges through targeted strategies (Van Dijk, 2022) (Kabanda, et al., 2018). By focusing on accessible education, leveraging cost-effective and scalable technology solutions, and fostering public-private partnerships, SMEs can overcome the barriers to robust cybersecurity practices. This approach not only enhances the individual security posture of SMEs but also contributes to the broader digital security and economic stability of developing economies.

# Operational Realities for SMEs in Cybersecurity

1. Resource Limitations: Unlike larger corporations, SMEs typically have limited financial, human, and technical resources dedicated to cybersecurity. This scarcity of resources affects their ability to implement comprehensive cybersecurity measures (Aiyer, et al., 2021).
2. Cybersecurity Expertise Gap: SMEs often lack in-house cybersecurity expertise, which makes it challenging to identify, assess, and mitigate cyber risks effectively. They may also struggle to stay updated with the latest threats and security practices (Boehm, et al., 2022).
3. Dynamic Threat Landscape: The cybersecurity threat landscape constantly evolves, with new vulnerabilities and attack methods emerging regularly. Keeping pace with these changes requires continuous monitoring and updating of security measures, which can be particularly challenging for SMEs.
4. Supply Chain Vulnerabilities: Many SMEs are part of larger supply chains and may be targeted as the weakest link by attackers looking to infiltrate larger corporations. This interconnectivity increases the risk and potential impact of cyberattacks.
5. Compliance and Regulatory Pressures: Navigating the complex web of data protection laws and industry regulations can be daunting for SMEs, especially those that operate across borders or in highly regulated sectors.

## Strategic Approaches for SMEs

Prioritising Key Assets and Risks

* Risk Assessment: Conduct regular risk assessments to identify and prioritise critical assets and vulnerabilities. This helps SMEs focus their limited resources on protecting the most vital parts of their business (AL-Dosari & Fetais, 2023).

Implementing Cost-effective Security Measures

* Leverage Open Source and Low-cost Solutions: Utilise open-source or affordable cybersecurity tools that offer significant protection without a hefty price tag. Many reputable free tools, such as antivirus protection, firewalls, and encryption, are available for basic needs.
* Security-as-a-Service (SaaS): Consider subscribing to SaaS offerings, which can provide enterprise-grade security solutions at a fraction of the cost of in-house implementations.

Building Cybersecurity Knowledge and Awareness

* Training and Education: Implement ongoing cybersecurity awareness programs for all employees. Regular training can significantly reduce the risk of successful phishing attacks and other user-targeted threats (Bada & Nurse, 2019).
* Collaborate for Knowledge Sharing: Join industry groups, online forums, or local business associations to share knowledge and learn from others' cybersecurity experiences.

Adapting to the Evolving Threat Landscape

* Automated Security Solutions: Use computerised tools for continuous monitoring and threat detection. This can help compensate for the lack of in-house cybersecurity expertise.
* Regular Updates and Patch Management: Ensure all software and systems are updated to protect against known vulnerabilities. Automated patch management systems can facilitate this process.

Securing the Supply Chain

* Vendor Risk Management: Assess the security practices of suppliers and partners. Require vendors to adhere to specific cybersecurity standards and consider conducting audits to ensure compliance.
* Contractual Agreements and Standards: Include cybersecurity requirements in contracts with suppliers and partners to ensure they maintain adequate security measures.

Navigating Compliance and Regulatory Requirements

* Simplified Compliance Checklists: Develop simplified checklists based on standard regulatory requirements relevant to the SME's industry and operational scope.
* External Compliance Assistance: Seek external assistance or consultancy for navigating complex compliance landscapes, especially for SMEs operating in multiple jurisdictions or highly regulated industries.

Addressing operational realities with strategic approaches allows SMEs to build a resilient cybersecurity posture despite constraints (Van Dijk, 2022). By prioritising critical assets, leveraging cost-effective solutions, fostering a culture of security awareness, adapting to changing threats, securing the supply chain, and navigating compliance efficiently, SMEs can mitigate risks and safeguard their operations against cyber threats (Pawar & Palivela, 2022) (Ajmi, et al., 2019). These strategies underscore the importance of a proactive and informed approach to cybersecurity within the operational and resource realities specific to SMEs.

## Framework Customisation for SMEs

Simplification and Prioritisation

Frameworks like NIST CSF, ISO/IEC 27001, and CIS Controls are comprehensive but can be overwhelming for SMEs. Tailoring involves simplifying these frameworks to focus on the most impactful controls and practices that offer SMEs the best return on investment (AL-Dosari & Fetais, 2023) (Chidukwani, et al., 2022) (The European Union Agency for Cybersecurity, 2021).

Recent research has demonstrated that small businesses can significantly enhance their cybersecurity posture by prioritising the "Identify" and "Protect" functions within the NIST Cybersecurity Framework. This approach has proven to be an effective strategy, requiring only minimal resource investment.

Sector-specific Adaptations

Different industries face unique cyber threats and regulatory requirements. Customising frameworks to address these sector-specific challenges can significantly improve their applicability and effectiveness for SMEs within those sectors.

The Global Cyber Alliance's cybersecurity toolkit for small businesses is tailored to SMEs' needs. It simplifies cybersecurity into actionable steps, helping companies to implement critical protections. SMEs have widely adopted the toolkit, demonstrating the value of industry-specific guidance (Global Cyber Alliance, 2023).

Cost-effective Implementation Strategies

Given SMEs' limited financial resources, tailored frameworks emphasise cost-effective strategies, utilising open-source tools, cloud services, and shared cybersecurity services to minimise expenses.

Implementations of ISO/IEC 27001 in small financial service providers in developing countries can focus on critical risk areas and leverage external expertise for training, enhancing security without significant investment. This approach can improve client trust and compliance with international standards (The British Standards Institution, 2013).

Government-Led Initiatives and Policies

Governments play a critical role in supporting SMEs through cybersecurity initiatives and policies that encourage or subsidise the adoption of tailored cybersecurity practices. Singapore's "SMEs Go Digital" program offers pre-approved digital solutions, including cybersecurity services, with funding support. This initiative has been instrumental in encouraging SME adoption of cybersecurity measures, demonstrating the effectiveness of government support in facilitating cybersecurity improvements among SMEs (Infocomm Media Development Authority, n.d.).

PPPs are essential for mobilising resources, expertise, and technology from both the public and private sectors to support SMEs in improving their cybersecurity. In Malaysia, the government and private sector collaboration led to the "Cybersecurity for SMEs" program, which offers training, resources, and assessment tools. This program has helped many SMEs identify vulnerabilities and implement appropriate cybersecurity measures, showcasing the potential of PPPs in enhancing cybersecurity awareness and capabilities among SMEs (Neumetric, 2024).

International Cooperation and Assistance

International organisations and cooperation efforts are vital in supporting cybersecurity advancements in developing economies, benefiting SMEs. Projects by the World Bank and the International Telecommunication Union (ITU) to build cybersecurity capacity in developing countries have provided technical and financial assistance for implementing national cybersecurity strategies. These efforts indirectly benefit SMEs by enhancing the overall cybersecurity ecosystem (International Telecommunication Union, n.d.) (The World Bank, 2023) (The World Bank, 2023).

The evidence from these examples underscores the importance of tailoring cybersecurity frameworks to meet the specific needs of SMEs. By focusing on simplification, sector-specific adaptations, cost-effective strategies, and leveraging government and international support, SMEs can implement cybersecurity measures that are both effective and sustainable (Pijnenburg Muller, 2015). Tailored approaches help SMEs protect themselves against cyber threats and contribute to the broader goal of creating a secure digital economy (Kabanda & Tanner, 2018).

The exploration of designing a robust and effective cybersecurity threat mirror specifically for Small and Medium Enterprises (SMEs) in developing economies reveals a multifaceted challenge that demands a nuanced, tailored approach. The significance of cybersecurity frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, cannot be overstated in their potential to guide SMEs towards establishing a strong cybersecurity posture. However, implementing these frameworks necessitates a strategic adaptation considering SMEs' unique operational, financial, and technical realities.

# Key Insights and Strategic Pathways

* Customisation and Simplification: Tailoring cybersecurity frameworks to align with SMEs' needs and resource constraints is crucial. This involves prioritising critical controls, simplifying implementation steps, and focusing on the most impactful measures that can prevent the majority of cyber threats.
* Overcoming Operational Realities: The operational challenges of limited budgets, lack of expertise, and the dynamic nature of cyber threats call for innovative solutions. Strategies such as leveraging cost-effective tools, engaging in public-private partnerships, and adopting a phased approach to cybersecurity are essential.
* Sector-specific Strategies: Acknowledging the diverse threat landscapes across different sectors, cybersecurity frameworks should be adapted to address industry-specific vulnerabilities and regulatory requirements, enhancing their relevance and effectiveness for SMEs within those sectors.
* Supportive Ecosystem: Government initiatives, public-private partnerships, and international cooperation are pivotal in facilitating SMEs' access to cybersecurity resources, expertise, and funding. These collaborative efforts can significantly lower SMEs' barriers to effective cybersecurity implementation.

# Concluding Reflections

Recent research highlights the vital significance of cybersecurity for small and medium-sized enterprises (SMEs), especially in developing economies. It also highlights the obstacles and promising avenues for effectively implementing cybersecurity frameworks, standards, and controls. Although comprehensive frameworks like NIST CSF, ISO/IEC 27001, and CIS Controls provide valuable direction, their successful adoption in the context of SMEs necessitates tailored customisation, robust support, and a thorough comprehension of the distinct challenges these entities encounter.

Future research must prioritise developing and evaluating targeted adaptation strategies and support mechanisms that can bolster cybersecurity resilience among small and medium-sized enterprises (SMEs) in developing economies. Such research would help identify and address the unique challenges that SMEs in these contexts face and ultimately contribute to advancing cybersecurity practices and standards across the global business landscape.

Through the customisation of cybersecurity frameworks, utilisation of government-led initiatives, cultivation of public-private partnerships, facilitation of international cooperation, and emphasis on awareness and training, it is feasible to enhance the cybersecurity stance of small and medium enterprises significantly. These tactics safeguard SMEs from cyber threats and advance the larger objective of establishing a more secure and durable digital economy.

As the risk of cyberattacks continues to grow, safeguarding the cybersecurity of small and medium-sized enterprises (SMEs) in developing nations presents a multifaceted and demanding undertaking. Nevertheless, by adopting a strategic mindset, pooling resources, and customising methods, this process can yield substantial benefits through strengthened security, heightened resilience, and improved business continuity. It is, therefore, crucial for all parties involved to appreciate the value of cybersecurity and take pre-emptive steps to defend SMEs against possible cyber threats.

# Citations

Aiyer, B., Anant, V. & Di Mattia, D., 2021. Securing small and medium-size enterprises: What’s next?. [Online]   
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next  
[Accessed 1 April 2024].

Ajmi, L. et al., 2019. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. [Online]   
Available at: https://ieeexplore.ieee.org/abstract/document/8769470  
[Accessed 1 April 2024].

AL-Dosari, K. & Fetais, N., 2023. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. Electronics, 12(17), p. 3629.

Australian Cyber Security Centre, 2017. Strategies to Mitigate Cyber Security Incidents. [Online]   
Available at: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents  
[Accessed 1 April 2024].

Bada, M. & Nurse, J. R. C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3).

Boehm, J. et al., 2022. Cybersecurity trends: Looking over the horizon. [Online]   
Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon  
[Accessed 1 April 2024].

Center for Internet Security, n.d. The 18 CIS Critical Security Controls. [Online]   
Available at: https://www.cisecurity.org/controls/cis-controls-list  
[Accessed 1 April 2024].

Chidukwani, A., Zander, S. & Koutsakis, P., 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. [Online]   
Available at: https://ieeexplore.ieee.org/abstract/document/9853515  
[Accessed 1 April 2024].

Dedeke, A. & Masterson, K., 2019. Contrasting cybersecurity implementation frameworks (CIF) from three countries. Information and Computer Security, 27(3), pp. 373-392.

Global Cyber Alliance, 2023. GCA Cybersecurity Toolkit for Small Business Handbook. [Online]   
Available at: https://gcatoolkit.org/wp-content/uploads/2021/06/GCA-Toolkit-Handbook.pdf  
[Accessed 1 April 2024].

Help Net Security, 2021. What are the most common cybersecurity challenges SMEs face today?. [Online]   
Available at: https://www.helpnetsecurity.com/2021/07/07/smes-cybersecurity-challenges/  
[Accessed 1 April 2024].

Infocomm Media Development Authority, n.d. SMEs Go Digital. [Online]   
Available at: https://www.imda.gov.sg/how-we-can-help/smes-go-digital  
[Accessed 1 April 2024].

International Telecommunication Union, n.d. Enhancing Cybersecurity in Least Developed Countries. [Online]   
Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CYBLDC.aspx  
[Accessed 1 April 2024].

Kabanda, S. & Tanner, M., 2018. Exploring SME cybersecurity practices in developing countries. Journal of Organisational Computing and Electronic Commerce, 28(3), pp. 269-282.

Kabanda, S., Tanner, M. & Kent, C., 2018. Exploring SME cybersecurity practices in developing countries. Journal of Organisational Computing and Electronic Commerce, 28(3), pp. 269-282.

Karake, Z., Shalhoub, R. A. & Ayas, H., 2019. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. Cheltenham, Gloucestershire: Edward Elgar Publishing, Incorporated.

Kshetri, N., 2010. Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly, 1 January, pp. 1057-1079.

National Institute of Standards and Technology, 2024. The NIST Cybersecurity Framework (CSF) 2.0. [Online]   
Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf  
[Accessed 1 April 2024].

Neumetric, 2024. ASEAN Cybersecurity Guidelines: A Framework for Regional Security. [Online]   
Available at: https://www.neumetric.com/asean-cybersecurity-guidelines/#:~:text=Encourage%20Public%2DPrivate%20Partnerships%3A%20Strengthen,collective%20%26%20coordinated%20approach%20to%20cybersecurity.  
[Accessed 1 April 2024].

Palhad, A. & Civilcharran, S., 2023. Cybersecurity in developing countries: A case of South African Small-Medium Enterprises (SMEs). s.l., Researchgate.

Pawar, S. & Palivela, H., 2022. LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1).

Perozzo, H., Zaghloul, F. & Ravarini, A., 2022. CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. Complex Systems Informatics and Modeling Quarterly, December, pp. 53-66.

Pijnenburg Muller, L., 2015. Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. [Online]   
Available at: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI+Report+03-15-Muller.pdf?sequence=3  
[Accessed 1 April 2024].

PricewaterhouseCoopers, 2021. SMEs in the world of Cyber - An Insight. [Online]   
Available at: https://www.pwc.com/mt/en/publications/technology/smes-in-the-world-of-cyber.html  
[Accessed 1 April 2024].

Teufel, S., Teufel, B., Aldabbas, M. & Nguyen, M., 2020. Cyber Security Canvas for SMEs. Communications in Computer and Information Science, Volume 1339, pp. 20-33.

The British Standards Institution, 2013. The Small Business Guide to Standards. [Online]   
Available at: https://www.bsigroup.com/Documents/standards/smes/bsi-small-business-guide-to-standards-en-gb.pdf?epslanguage=en-AU  
[Accessed 1 April 2024].

The European Union Agency for Cybersecurity, 2021. Cybersecurity For SMEs: Challenges and Recommendations, Athens: European Union Agency For Cybersecurity.

The World Bank, 2023. Sectoral Cybersecurity Maturity Model. [Online]   
Available at: https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P17263707c36b702309f7303dbb7266e1cf.pdf  
[Accessed 1 April 2024].

The World Bank, 2023. Strengthening Cybersecurity and Resilience of Critical Infrastructure. [Online]   
Available at: https://documents1.worldbank.org/curated/en/099705012152346616/pdf/IDU044546588061b004aaf08b5805c55aaee4128.pdf  
[Accessed 1 April 2024].

US Small Business Administration, n.d. Strengthen your cybersecurity. [Online]   
Available at: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity  
[Accessed 1 April 2024].

Van Dijk, V., 2022. A Cybersecurity Standard For SME. [Online]   
Available at: https://www.securityscientist.net/content/files/2022/07/Vincent-van-Dijk---A-Cybersecurity-Standard-for-SME---2020-2022.pdf  
[Accessed 1 April 2024].

Watkins, S., 2022. Iso/iec 27001 An Introduction to Information Security and the ISMS Standard.. Ely: IT Governance Publishing Ltd.