World Journal of Information Systems 1(2) 29-36
DOI: https://doi.org/10.17013/wjis.v1i2.11

Article

Proposal for a Cybersecurity Framework for the Digital Transformation of Small and Medium-Sized Enterprises in Mozambique: Position Paper

Micaela Amade[1], Henrique São Mamede[1,2], Leonilde Reis[3], Ramiro Gonçalves[2,4], José Martins[2], Frederico Branco[2,4]

[1] Universidade Aberta, Lisboa, Portugal
[2] INESC TEC, Porto, Portugal
[3] Instituto Politécnico de Setúbal, Setúbal, Portugal
[4] Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal

Correspondence: **mroberto@ucm.ac.mz**, **jose.mamede@uab.pt**, **leonilde.reis@esce.ips.pt**, **ramiro@utad.pt**, **jose.l.martins@inestec.pt**, **fbranco@utad.pt**

(Article history: Received March 10, 2024; Received in revised form April 15, 2024; Accepted May 12, 2024; Available online June 15, 2024)

Abstract: With the advent of Information and Communication Technologies in recent decades, organizations face several challenges today. Adopting Digital Transformation (DT) offers numerous opportunities for Small and Medium Enterprises (SMEs) to improve their efficiency and operations, reaching new markets, shareholders, and customers. However, there are potential risks associated with this process. With Digital Transformation, the radius of connectivity and interconnection between devices and systems increases in Mozambique and worldwide, creating more significant space cyberattacks. As Small and Medium-sized Enterprises (SMEs) connect to the digital world and move forward with adopting innovative digital technologies, they become more vulnerable to digital security risks. Hence, managing digital security risks effectively is crucial to realising the benefits of Digital Transformation. This position paper proposes to present the research work that will culminate in the proposal to develop a framework that fits Mozambican Small and Medium Enterprises through a Design Science Research (DSR) methodology, which can help to assist Mozambican Small and Medium Enterprises in the Digital Transformation (DT) process.

© 2024 ITMA. All rights reserved.

Keywords: Digital Transformation; Cybersecurity; SMEs.

1. Introduction

The 21st century is characterised by technological advances on a global scale in different areas with the potential to transform various areas of society radically. With this growth, institutions and organizations worldwide have embraced new technologies to improve their portfolio of customer services. This transformation, although gradual, gives rise to a resizing in the modus operandi of SMEs and their customers.

Undoubtedly, SMEs play a pivotal role in the business sector, making substantial contributions to promote a sustainable and digital economy. They are indispensable for the prosperity of both local and global economies [1]. In Mozambique, 98.6% of all companies are formed by SMEs, and according to Mozambican regulations, an organization is considered small if it comprises 11 to 30 employees and medium if it has 31 to 100 employees [2].

Digital Transformation offers countless opportunities for SMEs to improve their operations, reach new markets and customers, and improve efficiency. However, there are potential risks associated with this process. For [3], several cyber risks in the DT can harm the organization's security. The assets of SMEs are often at risk of cyberattacks, including potential threats such as data breaches, destruction, and denial of access to information. These incidents can likely adversely affect various business operations [1]. SMEs underestimate cyber threats, believing they are not vulnerable due to their size, but reality shows that they have become the most valuable target for cyberattacks [1].

Regarding the Cybersecurity status in Mozambique, low legal commitments characterise the country [4]. Organizations have safeguards applied to cyber risk, but most do not follow their sector's best practices [5]. Most boards are unaware of cyber risk; ransomware is the most common threat. Although the Mozambican Government has identified Cybersecurity as a priority segment of the country's DT process [6], the budget allocated for Cybersecurity management is still not enough to cover the growing threat landscape, and most organizations are not prepared to respond to cyber incidents due to the lack of a cyber incident response plan [5]. SMEs seek to adopt emerging technologies to improve operational efficiency and expand their markets without considering cybersecurity risks that might threaten business continuity, data reliability, and customer privacy.

© 2024 ITMA. All rights reserved.

The present paper has the following structure: the topic introduction, showing the importance of the proposed research and its relevance; the purpose and research questions, where the main objective is presented and each research question is specified; the literature review, which provides a preliminary review of existing research on the topic, establishes the theoretical foundation of the research, and the gap the study aims to fill; the research methodology to be used; and conclusion that the framework will facilitate a secure and efficient digital transition for SMEs in Mozambique.

1. Purpose and research questions

Considering the current limitations and challenges, it is crucial to comprehend and address the specific cybersecurity risks that Mozambican SMEs face during the digital transformation process and develop practical and effective solutions to mitigate them. By evaluating the economic and operational impact of Cybersecurity risks on Mozambican SMEs, focusing on how these risks affect their operations and business continuity, and creating a customised cybersecurity Framework, Mozambican SMEs can reduce vulnerabilities to cyber risks in the process of Digital Transformation, increase the overall resilience, ensure that SMEs have robust strategies in place for business continuity and recovery in the event of cyber incidents and also raising awareness and building capacity.

The central question will be: Is it possible to incorporate a cybersecurity framework into SMEs Digital Transformation process in the Mozambican context? Sub-question: What is the primary cybersecurity risks that SMEs may encounter during the Digital Transformation process? What is the economic and operational impact of Cybersecurity risks on SMEs, and how do they affect their operations and business continuity? What is the current state of Cybersecurity maturity in SMEs in Mozambique? How do we mitigate cybersecurity risks for SMEs during the Digital Transformation process?

2. Literature Review

A preliminary literature review was conducted using Google Scholar and Scopus databases, was selected articles from the last ten years. An analysis was carried out on articles related to DT models and their relevance to SMEs, particularly in developing countries, cybersecurity risks, and the current state of Cybersecurity in Mozambique, including challenges and frameworks, focusing on their application in SMEs.

Digital Transformation (DT) is now critical for almost all companies worldwide. The benefits of DT for SMEs can include improve process efficiency and quality, increase

© 2024 ITMA. All rights reserved.

staff productivity, better customer satisfaction, more accessible access to new markets, strengthened business relations with big companies, higher return on investments in Information and Communication Technologies (ICT), reduced administrative overheads and greater focus on core business [7].

The internet penetration rate in Mozambique increased by 17% in 2021, indicating a significant growth in digital access [8][8], [9]. However, there is a discrepancy in connectivity between urban and rural areas [6]. This variation may result in differences in cybersecurity preparedness among SMEs, rendering those in less connected areas more susceptible to cyberattacks. Initiatives like digital villages are being implemented to reduce this discrepancy and improve connectivity and ICT access in rural areas.

The digital landscape in Mozambique is characterised by growing Internet penetration and strong government focus on digital infrastructure and Cybersecurity. This environment provides a promising backdrop for the DT of SMEs. The government prioritised Cybersecurity in its DT strategy [6].

SMEs constantly evolve in the cyber threat landscape because they have limited resources to face the threats [10]. Underestimation of Cybersecurity threats by SMEs also leads to an increase in their vulnerability and risks, which, unfortunately, can become challenges for them and other related parties[1]. Cybercriminals increasingly target SMEs since they are perceived to have the weakest defences. Additionally, SMEs do not seem to implement all the advisable security measures to help them resist such attacks [11]. According to [3], cybercrimes include theft, embezzlement, data hacking, and destruction. Approximately 10.5 trillion dollars will be spent each year on cybercrime by 2025. In terms of year-over-year growth, cyber-attacks are growing at 15 per cent. There are always costs associated with cyber-attacks, whether monetary or non-monetary.[3]

For [12], SMEs lack of knowledge, vulnerability, economic impact, insufficient risk awareness, and inadequate security measures highlight the need for SMEs to prioritise Cybersecurity and implement adequate security measures to protect their businesses from cyber risks.

Like most SMEs worldwide, Mozambican SMEs undergoing DT may face common cybersecurity challenges, such as limited cybersecurity awareness among employees and budget constraints for implementing strong cybersecurity measures.

© 2024 ITMA. All rights reserved.

Cyberattacks can result in significant financial losses and operational disruptions, damaging the trust of customers and patterners. There are global cybersecurity Frameworks available, like the NIST Cybersecurity Framework (CSF), which the National Standards and Technology developed in the U.S. This framework provides guidelines on how to identify, protect, detect, respond, and recover from cyber incidents[13]. The framework is designed to define security standards and policies applicable to all critical infrastructure sectors, provide a flexible and repeatable approach, and prioritize activities[14].

There is CIS Control v8 that provides a solution that complies with globally recognized standards and is one of the best ways to protect information technology systems and data from cyberattacks[15]. It focuses on operational best practices, not system management. There is also ISO/ISEC 27001, an international standard for managing information security, and it provides a set of standardised requirements for an Information Security Management System [13]. ISO 27001 is part of the ISO 27000 family, which is a comprehensive security management framework and is therefore much larger than CIS Control.

Due to a limited budget, its implementation can be recourse-intensive, which may be challenging for SMEs. On the other hand, different countries and regions may have their cybersecurity frameworks tailored to local needs and legal requirements. In the Mozambican context, a Cybersecurity framework that meets the SMEs matur lacking. The reason why a proposed Cybersecurity Framework that combines the existing national cybersecurity policies, local needs, and globally well-established Cybersecurity framework could result in customisation and scalability framework, enabling businesses to focus on the most relevant aspects without being overwhelmed by clear and practical instructions that can be comprehended and applied without requiring advanced cybersecurity knowledge, elements for employee training and awareness, as well as adherence to legal and regulatory obligations.

3. Research Methodology

Given the objective of the thesis, the Design Science Research (DSR) methodology is proposed. The DSR methodology, as outlined in [16], is a comprehensive approach for conducting research in information systems. Through a systematic process, a DSR allows the creation and rigorous evaluation of the artefact, ensuring its efficiency and validity. DSR also provides interaction with all involved in the process, guaranteeing quality.

© 2024 ITMA. All rights reserved.

Table 1 describes the activities of DSR methodology according to [16].

Table 1: DSR Methodology

Activity	Description
Problem Identification and Motivation	The initial phase focuses on identifying the specific problem that the research intends to address. [1]For Mozambican SMEs, the problem is the lack of a cybersecurity framework that caters to their needs during DT. Interviews, surveys, and secondary data analysis will be conducted to confirm and detail the problem scope.
Objectives of a Solution	The subsequent step is to articulate the objectives of the solution, which, in this case, is the cybersecurity framework. The requirements of SMEs, the technical feasibility, and the potential for impact will guide the objectives. This will involve setting clear, measurable goals for the framework.
Design and Development	The artefact (the cybersecurity framework) will be created during this stage. The previously defined objectives will inform the design and follow an iterative process, incorporating stakeholder feedback. Prototyping and other design methodologies will be utilised to develop a preliminary framework model.
Demonstration	The demonstration phase involves using the artefact in a real-world scenario to show how it can solve the identified problem. The framework will be implemented in a controlled environment within selected SMEs to illustrate its practical application and to gather preliminary performance data.
Evaluation	Evaluation is crucial to assess the effectiveness of the artefact. This research will employ qualitative and quantitative methods to evaluate the cybersecurity framework's functionality, completeness, and usability, among other criteria. The results will be compared against the objectives defined in the second stage.
Communication	Finally, the research findings and knowledge generated throughout the DSR process will be shared with academic and practitioner audiences. Scholarly articles, conference presentations, and workshops for SMEs will be used as platforms for dissemination.

Therefore, the DSR will allow the development and evaluation of effective practical solutions to mitigate and resolve Cybersecurity risks in SMEs in Mozambique during the Digital Transformation.

4. Conclusions

The SMEs aspire to integrate emerging technologies to enhance operational efficiency and broaden their market reach. However, they often underestimate the potential cybersecurity risks that could jeopardise business continuity, compromise data reliability,

[1]https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research

© 2024 ITMA. All rights reserved.

and compromise customer privacy. The proposed framework aims to empower Mozambican SMEs to harness the potential of Digital Transformation while effectively managing the heightened cybersecurity risks accompanying this progress. This framework will be tailored to the specific needs and challenges SMEs face, drawing on the rigorous standards set by global benchmarks. By providing a structured approach to navigating the complexities of digital security, the framework will be a critical tool in facilitating a secure and efficient digital transition for SMEs in Mozambique. The successful implementation of this framework will contribute to protecting SMEs from cyber threats and ensure that they can confidently explore new avenues for growth, innovation, and connectivity in the digital era. Ultimately, this will foster a resilient and forward-looking digital economy within Mozambique and beyond.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638.

[2] INE, "Estatísticas do Ficheiro de Unidades Estatísticas 2022 - INE." Accessed: Nov. 14, 2023. [Online]. Available: https://t.ly/JSvwH

[3] S. Mishra and S. Gochhait, "Emerging Cybersecurity Attacks in the Era of Digital Transformation," in *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India: IEEE, May 2023, pp. 1442–1447. doi: 10.1109/ICICCS56967.2023.10142357.

[4] "View of Cybersecurity in Mozambique: Status and Challenges." Accessed: Sep. 16, 2023. [Online]. Available: https://papers.academic-conferences.org/index.php/eccws/article/view/1194/1203

[5] "Cybersecurity Survey | Deloitte Moçambique." Accessed: Sep. 16, 2023. [Online]. Available: https://www2.deloitte.com/pt/pt/mz/pages/risk-advisory/articles/cybersecurity-survey.html

[6] International Trade Administration, "Mozambique's Digital Transformation." Accessed: Nov. 14, 2023. [Online]. Available: https://www.trade.gov/market-intelligence/mozambiques-digital-transformation

© 2024 ITMA. All rights reserved.

[7] European Commission, “Fostering SMEs growth through digital transformation - Smart Specialisation Platform.” Accessed: Nov. 14, 2023. [Online]. Available: https://s3platform.jrc.ec.europa.eu/en/web/guest/w/fostering-smes-growth-through-digital-transformation

[8] The World Bank, “Individuals using the Internet (% of population) - Mozambique | Data.” Accessed: Nov. 14, 2023. [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&locations=MZ&most_recent_year_desc=false&start=1990&view=chart

[9] ITU, “Statistics.” Accessed: Nov. 14, 2023. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[10] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, “Systematic Approach to Cyber Resilience Operationalization in SMEs,” *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

[11] “Cybersecurity and the Unbearability of Uncertainty | IEEE Conference Publication | IEEE Xplore.” Accessed: Nov. 15, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7600224

[12] Andrei-Laurențiu Mitrofan, Elena-Veronica Cruceru, and Andreea Barbu, “Determining the Main Causes that Lead to Cybersecurity Risks in SMEs,” *Bus. Excell. Manag.*, vol. 10, no. 4, pp. 38–48, 2020.

[13] A. Chidukwani, S. Zander, and P. Koutsakis, “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations,” *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[14] “Cybersecurity Framework | NIST.” Accessed: Jul. 2, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[15] S. Gros, “A Critical View on CIS Controls,” in *2021 16th International Conference on Telecommunications (ConTEL)*, Zagreb, Croatia: IEEE, Jun. 2021, pp. 122–128. doi: 10.23919/ConTEL52528.2021.9495982.

[16] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

© 2024 ITMA. All rights reserved.