Contents

Abstract

Small and medium enterprises (SMEs) play a critical role in the global economy, yet they often struggle to implement effective cybersecurity measures, leaving them vulnerable to cyber threats. This literature review examines the cybersecurity challenges faced by SMEs and explores the need for tailored frameworks to enhance their cybersecurity posture. The review of five research papers highlights the lack of awareness, limited financial resources, and inadequate education as major hurdles for SMEs in achieving cybersecurity resilience. The studies emphasize the importance of customized cybersecurity solutions and the necessity for minimum baseline controls to boost cybersecurity resilience and effectively shield against cyber threats. Collaborative efforts among researchers, funders, and stakeholders are advocated to bridge existing gaps and improve SME cybersecurity practices. Overall, the findings underscore the urgent need for enhanced cybersecurity measures tailored to the specific needs of SMEs to mitigate the increasing risks of cyber-attacks and financial losses in the global economy.

Introduction

1. A framework for least cybersecurity controls to be implemented.
    - Small and medium enterprises (SMEs) play a vital role in the global economy, yet they often struggle to implement effective cybersecurity measures, leaving them vulnerable to cyber threats. This literature review examines the cybersecurity challenges faced by SMEs and explores the need for tailored frameworks to enhance their cybersecurity posture.

      Pawar and Palivela's survey highlights that while SMEs recognize the importance of cybersecurity, many lack the necessary resources and expertise to implement standard frameworks or controls effectively. This underscores the importance of understanding the current state of cybersecurity implementation in SMEs and developing tailored approaches to address their specific challenges.

      The LCCI framework, proposed in this study, offers a structured approach for SMEs to implement essential cybersecurity controls. By focusing on simple yet effective security measures suited to SMEs' size and resources, the framework provides a practical guide to enhance cybersecurity resilience. Further research and practical implementations of such frameworks are essential to supporting SMEs' cybersecurity needs in today's digital business environment.
2. Unaware, Unfunded and Uneducated A Systematic Review of SME
    - The systematic review "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity" sheds light on the significant challenges faced by

Small and Medium Enterprises (SMEs) in ensuring cybersecurity. This review underscores a lack of awareness, limited financial resources, and inadequate education as major hurdles in achieving cybersecurity resilience. Emphasizing the post-2017 landscape, the study emphasizes the pressing need for more practical and tailored recommendations for SMEs. It also stresses the importance of standardized reporting in cybersecurity literature and advocates for collaborative efforts among researchers, funders, and stakeholders to bridge existing gaps and enhance SME cybersecurity practices.

3. Digital Transformation and Cybersecurity Challenges for Businesses Resilience
    - The literature review titled "Digital Transformation and Cybersecurity Challenges for Businesses Resilience" delves into the evolving landscape of digital transformation and its impact on cybersecurity challenges faced by businesses. It explores critical issues such as cyber threats and data breaches, highlighting the importance of robust security measures. The review also emphasizes the role of cybersecurity readiness frameworks and national cybersecurity strategies in mitigating these risks. Recommendations include continuous improvement of cybersecurity practices, conducting cost-benefit analyses for security investments, and adopting industry standards such as the NIST Cybersecurity Framework. Overall, the review underscores the pressing need for businesses to adapt and strengthen their cybersecurity strategies to meet the demands of the digital era.
4. Information security and cybersecurity assessment in sme
    - The literature review in this paper underscores the critical importance of cybersecurity for Small and Medium Enterprises (SMEs). It explores the various guidelines and frameworks offered by reputable organizations such as ENISA, ISO, NIST, and national cybersecurity institutions like the National Center for Cybersecurity in Portugal. The review highlights the need for SMEs to leverage these resources to enhance their cybersecurity posture effectively. Moreover, the study draws attention to the alignment between the National Center for Cybersecurity's roadmap and the ISO 27001:2013 standard, proposing a method to assess cybersecurity risks specifically tailored for SMEs. Additionally, it offers definitions for SMEs based on employee count and financial metrics, underlining the urgency of addressing cybersecurity challenges within this sector.
5. Cyber risk management in SMEs
    - The literature review in "Cyber risk management in SMEs" addresses the paucity of academic research on cyber risk management processes in small- and medium-sized enterprises (SMEs). It emphasizes the critical importance of understanding the impact of cyber-attacks on SMEs, their response mechanisms, and the cultivation of a cybersecurity-prepared culture. The review underscores the supportive role of external entities such as governments, consultants, and insurers in enhancing SMEs' knowledge and awareness of cyber risks. Additionally, it

emphasizes the necessity for SMEs to clearly define responsibilities, ensuring that cyber risk management is perceived as a corporate issue rather than solely the purview of the IT department.

Literature Review

1. A framework for least cybersecurity controls to be implemented
    - Small and medium enterprises (SMEs) are essential to the global economy, but they often struggle to implement effective cybersecurity measures to protect their sensitive information and assets. Studies have shown that SMEs face cybersecurity vulnerabilities and risks due to factors like limited resources, lack of expertise, and inadequate awareness of best practices.

      Pawar and Palivela conducted a survey to understand the cybersecurity posture of SMEs. They targeted top management and executives from SMEs across different countries and domains. The results indicated that while SMEs consider cybersecurity important, only a few have implemented standard frameworks or controls.

      Research underscores the need to understand the current state of cybersecurity implementation in SMEs. Despite increasing cyber threats, there is a lack of knowledge about the challenges SMEs face in implementing cybersecurity measures effectively. This knowledge gap highlights the need for tailored approaches and frameworks for SMEs.

      The LCCI framework proposed in the study offers a structured approach for SMEs to implement essential cybersecurity controls effectively. By focusing on simple yet effective security measures suited to SMEs' size and resources, the framework provides a practical guide to enhance cybersecurity resilience. Its emphasis on simplicity aligns with SMEs' typical resource constraints.

      In conclusion, the literature emphasizes the cybersecurity challenges SMEs face and the importance of tailored frameworks to support their efforts. The LCCI framework provides a promising approach to help SMEs strengthen their cybersecurity and mitigate cyber threats. Further research and practical implementations of such frameworks are crucial to supporting SMEs' cybersecurity needs in today's digital business environment.
2. Unaware, Unfunded and Uneducated A Systematic Review of SME

- The systematic review "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity" outlines the significant challenges that Small and Medium Enterprises (SMEs) face regarding cybersecurity. The review identifies a lack of awareness, limited financial resources, and inadequate education as major obstacles to achieving cybersecurity resilience. Focusing on the period after 2017, the review stresses the necessity for more practical and applicable recommendations tailored to the specific needs of SMEs. The study highlights the importance of standardized reporting in cybersecurity literature and advocates for collaborative efforts among researchers, funders, and stakeholders to address existing gaps and improve SME cybersecurity practices.

3. Digital Transformation and Cybersecurity Challenges for Businesses Resilience
    - The literature review in "Digital Transformation and Cybersecurity Challenges for Businesses Resilience" examines the changing landscape of digital transformation and the associated cybersecurity challenges that businesses face. It discusses critical issues such as cyber threats, data breaches, and the necessity for strong security measures. The review emphasizes the significance of cybersecurity readiness frameworks and national cybersecurity strategies in mitigating these risks. Recommendations include ongoing enhancement of cybersecurity practices, conducting cost-benefit analyses for investments, and adopting industry standards like the NIST Cybersecurity Framework. Overall, the review underscores the urgent requirement for businesses to adjust and enhance their cybersecurity strategies in response to the demands of the digital era.
4. Information security and cybersecurity assessment in sme
    - The literature review in the paper underscores the significance of cybersecurity for Small and Medium Enterprises (SMEs) and discusses the various guidelines and frameworks offered by reputable organizations such as ENISA, ISO, NIST, and national cybersecurity institutions like the National Center for Cybersecurity in Portugal. It emphasizes the importance for SMEs to utilize these resources to improve their cybersecurity posture. The study highlights the alignment between the National Center for Cybersecurity's roadmap and the ISO 27001:2013 standard, proposing a method to evaluate cybersecurity risks in SMEs. Additionally, it provides definitions for SMEs based on employee count and financial metrics, emphasizing the need to address cybersecurity challenges in this sector.
5. Cyber risk management in SMEs
    - The literature review in "Cyber risk management in SMEs" focuses on the lack of academic research regarding cyber risk management processes in small- and medium-sized enterprises (SMEs). It stresses the importance of understanding the impact of cyber-attacks on SMEs, how they respond to such incidents, and the necessity of fostering a culture that is prepared for cyber threats. The review also highlights the role of external entities such as governments, consultants, and

insurers in assisting SMEs with knowledge and awareness. Furthermore, it emphasizes the need for SMEs to clearly define responsibilities to ensure that cyber risk management is seen as a corporate issue rather than solely the responsibility of the IT department.

Methodology

1. A framework for least cybersecurity controls to be implemented
    - The study utilized a quantitative research approach, employing a structured research survey that targeted senior management, C-level executives, and directors from SMEs across different countries and industries. The survey aimed to gain insights into the cybersecurity readiness of SMEs and identify key challenges in implementing cybersecurity controls. Participants were engaged through messaging and emails to capture a range of perspectives on cybersecurity practices in SMEs. The survey included questions about the age of SMEs, their use of security frameworks, existing security controls, security awareness training, experiences with cyber-attacks, and their expectations from security standards. This approach enabled a comprehensive understanding of the current cybersecurity landscape for SMEs.
2. Unaware, Unfunded and Uneducated A Systematic Review of SME
    - The methodology used in the systematic review "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity" involved a meticulous selection process of relevant literature published between 2017 and 2023. Three authors held regular meetings to review and discuss findings, aiming to maintain objectivity while recognizing the inherent subjectivity in qualitative research. Data collection was conducted using Research Information Systems (RIS) format files, Rayyan for initial screening, and Zotero for full-text screening. Eligibility criteria were applied, and extracted data were coded using NVIVO. A Proforma guided the data extraction process, covering publication year, study type, data collection method, sample size, coverage, and discussion of existing cybersecurity frameworks.
3. Digital Transformation and Cybersecurity Challenges for Businesses Resilience
    - The methodology used in the report "Digital Transformation and Cybersecurity Challenges for Businesses Resilience" included a systematic literature review following the PRISMA guidelines. The Google Scholar database was used to extract primary studies using specific keywords related to digital transformation and cybersecurity. The search criteria aimed to gather relevant research articles for analysis. The methodology focused on identifying and synthesizing key findings from papers published between 2019 and 2023. By adhering to the PRISMA

guidelines, the study ensured a structured approach to reviewing and analyzing the literature, providing a comprehensive understanding of the implications of cybersecurity within the context of digital transformation for businesses.

4. Information security and cybersecurity assessment in sme
    - The methodology proposed in the paper offers a comprehensive approach to assessing cybersecurity risks in SMEs. It starts with a review of pertinent documents, such as the minimum cybersecurity capacities roadmap from the National Cybersecurity Center and selected information security standards. The goal is to pinpoint crucial convergence points between the roadmap and the ISO 27001:2013 standard by aligning actions and controls. This correlation map forms the foundation for creating a questionnaire tailored to SME contexts to assess their cybersecurity status. The resulting survey can be used for self-assessment by SMEs and as a tool for IT consultants to effectively evaluate cybersecurity risks.
5. Cyber risk management in SMEs
    - The methodology used in "Cyber risk management in SMEs" involved gathering insights from 37 recent industry surveys to evaluate the current state of cyber risk management in SMEs. The researchers organized the data according to the risk management process steps, identifying key challenges and suggesting future research directions. To mitigate potential biases in the non-peer-reviewed industry surveys, the study considered a variety of authors and cross-checked findings for consistency. The researchers conducted a systematic search using specific keywords related to cyber risk management and SMEs, resulting in a comprehensive database of relevant surveys. This rigorous approach ensured a robust analysis of the cyber risk management landscape for SMEs.

Discussion

1. A framework for least cybersecurity controls to be implemented
    - The research survey uncovered that a notable percentage of SMEs lack organized cybersecurity controls, with approximately 49% not employing any cybersecurity standards or frameworks. Merely 23% of SMEs had implemented ISO 27001, 10% GDPR, and 8% NIST Cybersecurity Framework. These results underscored the hurdles faced by SMEs in adopting cybersecurity measures, such as financial constraints, absence of suitable cybersecurity controls, and limited skilled resources. The study emphasized the significance of customized cybersecurity solutions for SMEs and the necessity for minimum baseline controls to boost cybersecurity resilience and effectively shield against cyber threats.
2. Unaware, Unfunded and Uneducated A Systematic Review of SME

- In the systematic review of SME cybersecurity, significant barriers to SME cybersecurity were identified, including a lack of threat awareness, resource constraints, and limited cybersecurity literacy among SME personnel. The review also noted the prevalence of recurring themes in the literature without new empirical evidence, highlighting the need for updated research to address contemporary cybersecurity challenges. Recommendations from the review included tailored initiatives for SMEs, standardized reporting practices, and collaborative efforts to bridge knowledge gaps. Overall, the findings underscored the urgent need to enhance cybersecurity measures for SMEs to mitigate the increasing risks of cyber-attacks and financial losses in the global economy.

3. Digital Transformation and Cybersecurity Challenges for Businesses Resilience
    - The study "Digital Transformation and Cybersecurity Challenges for Businesses Resilience" revealed the growing efficiency and productivity advantages of digital transformation, alongside highlighting the new cybersecurity risks it brings, including data breaches and cyber-attacks. The research stressed the importance for organizations to prioritize cybersecurity measures to protect digital assets and maintain business continuity. Additionally, the study proposed a cybersecurity readiness framework for businesses undergoing digital transformation to effectively mitigate risks. The findings underscored the crucial need to address cybersecurity challenges concurrently with digital transformation efforts to bolster organizational resilience and security in the ever-changing technological landscape.
4. Information security and cybersecurity assessment in sme
    - The study's findings indicated correlations between the actions outlined in the minimum cybersecurity capacities roadmap and the controls specified in the ISO 27001:2013 standard. Using a questionnaire based on these correlations, the study assessed the cybersecurity status of SMEs in Portugal. A technical assessment conducted before the survey served as a baseline for comparison and validation of the questionnaire results. The study involved SMEs from various sectors in Portugal, with 17 out of 50 companies participating. The results highlighted the methodology's relevance in evaluating and enhancing cybersecurity practices in SMEs, emphasizing the importance of aligning with established standards for improved cybersecurity resilience.
5. Cyber risk management in SMEs
    - The findings from "Cyber risk management in SMEs" indicated that deficiencies in risk culture and the shortage of IT experts are major barriers to implementing cyber risk management in SMEs, consistently observed across various countries. The study emphasized the pivotal role of cybersecurity culture in effective cyber risk management and emphasized the necessity for further research to delve deeper into this relationship. The results underscored the significance of addressing cyber risk competency as a key component of SMEs' cybersecurity culture and advocated for

stronger integration between enterprise risk management and cyber risk management research streams.

Conclusion

1. A framework for least cybersecurity controls to be implemented
    - The study emphasizes the critical need for tailored cybersecurity solutions for small and medium enterprises (SMEs) to address the gaps in cybersecurity controls implementation. With a significant percentage of SMEs lacking structured security frameworks, there is a pressing need for minimum baseline controls to mitigate cyber risks effectively. The findings underscore the challenges faced by SMEs, including financial constraints and limited resources, in implementing cybersecurity measures. By prioritizing domain-specific security demands and continuously improving cybersecurity postures, SMEs can enhance their resilience against cyber threats and safeguard their business operations. The study advocates for a stepwise approach to cybersecurity implementation to protect SMEs from potential cyber-attacks.
2. Unaware, Unfunded and Uneducated A Systematic Review of SME
    - A Systematic Review of SME Cybersecurity" emphasizes the critical need for increased focus on SME cybersecurity, given their vulnerability to cyber threats. Despite the growing number of initiatives and research projects in this area, challenges persist due to a lack of awareness, resource constraints, and limited cybersecurity literacy among SMEs. The review calls for a deeper understanding of the interplay between these barriers and stresses the importance of tailored cybersecurity solutions, standardized reporting standards, and collaborative efforts to empower SMEs in enhancing their cybersecurity resilience. Future research and initiatives should address these key barriers to safeguard SMEs from cyber risks.
3. Digital Transformation and Cybersecurity Challenges for Businesses Resilience
    - In conclusion, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience" underscores the indispensable role of cybersecurity in the era of digital transformation. The study emphasizes the need for organizations to proactively enhance their cybersecurity measures to mitigate evolving cyber threats effectively. By implementing robust cybersecurity planning, preparation, and surveillance mechanisms, businesses can navigate the complexities of digital transformation while safeguarding their operations and data. The research advocates for a strategic organizational cybersecurity strategy, regular vulnerability assessments, and employee training to address emerging security risks. Ultimately, a proactive approach to cybersecurity is essential for businesses to ensure resilience and continuity amidst technological advancements.
4. Information security and cybersecurity assessment in sme

- In conclusion, the study underscores the challenges faced by SMEs in enhancing cybersecurity resilience and aligning with established standards. The findings highlight the need for tailored methodologies that bridge the gap between cybersecurity frameworks and SME realities. By combining formal standard documentation with governance guidelines, the research provides a practical tool for SMEs to improve their security posture within resource constraints. The study emphasizes the importance of incentivizing top management to invest in cybersecurity, as incidents become increasingly common. Overall, the methodology developed in this research offers a valuable approach for SMEs to navigate cybersecurity challenges and strengthen their defenses in the digital age.

5. Cyber risk management in SMEs
    - In conclusion, "Cyber risk management in SMEs" identified deficiencies in cyber security culture and the shortage of skilled IT experts as key challenges for SMEs in managing cyber risks. The study emphasized the crucial role of risk culture in effective cyber risk management and called for further research to explore this relationship. Recommendations included enhancing cyber security awareness, knowledge, and attitudes within SMEs, as well as integrating cyber risk management into overall risk management processes. The findings underscored the need for a holistic approach to cyber risk management in SMEs and highlighted the importance of addressing these challenges to enhance cyber resilience in the SME sector [T4], [T5].

References

[1] A. Pawar and R. Palivela, "A framework for least cybersecurity controls to be implemented.

[2] C. Rombaldo Junior, I. Becker, and S. Johnson, "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity," IEEE Journal Abbreviation, vol. 1, no. 1, pp. 1-1, October 2023.

[3] A. Author et al., "Digital Transformation and Cybersecurity Challenges for Businesses Resilience," in IEEE Transactions on Cybersecurity, vol. 1, no. 1, pp. 1-21, Year.

[4] Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). Information Security and Cybersecurity Assessment in SME. *Journal of Global Business and Technology*, 19(1), 79-94.

[5] Hoppe, F., Gatzert, N., & Gruner, P. (Year). "Cyber risk management in SMEs: insights from industry surveys."