Electronic Journal of Education, Social Economics and Technology
Vol. 6, No. 1, (2025), pp. 143-149
ISSN 2723-6250 (online)
DOI: https://doi.org/10.33122/ejeset.v6i1.470

SAINTIS publishing

Research Article

Cyber Security Paradox in MSMEs: Imbalance of Awareness and Implementation in the Digital Era

Haryanto*

Department of Accounting, Faculty of Economics and Business, Universitas Bina Insani, Jawa Barat, Indonesia
*Corresponding Author: haryanto@binainsani.ac.id

ABSTRACT

Cybersecurity is vital in ensuring the sustainability of micro, small, and medium enterprises (MSMEs) in today's digital landscape. While awareness of cybersecurity threats is rising, implementing effective mitigation measures among MSMEs remains relatively low. This study seeks to analyze the discrepancy between awareness and actual implementation of cybersecurity practices in MSMEs and investigate how management accounting approaches can help address these challenges. This study reviews pertinent academic literature and industry reports using narrative review and conceptual analysis methods. The findings reveal that the primary obstacles to implementing cybersecurity within MSMEs include limited financial resources, a shortage of information technology experts, and a low understanding of the long-term benefits of investing in digital security. To navigate these challenges, management accounting techniques such as cost-benefit analysis, cost control, and risk assessment can assist MSMEs in allocating their resources more efficiently to bolster cybersecurity. This research enhances the existing literature by bridging the fields of cybersecurity and management accounting and offering policy recommendations to improve MSMEs' digital readiness. Further research is necessary to empirically validate the proposed model and investigate the impact of regulation on enhancing cybersecurity in the MSME sector.

Keywords: Cyber Security; Digital Security Investment; Management Accounting; MSMEs; Risk Management

1. INTRODUCTION

In today's digital age, micro, small, and medium enterprises (MSMEs) are increasingly dependent on information technology to enhance operational efficiency and competitiveness. Embracing digitalization enables MSMEs to broaden their market reach, boost productivity, and streamline their financial systems and overall business management (Hendrawan et al., 2024). However, behind the benefits offered, digitalization also carries significant risks, one of which is cybersecurity threats (Safitra et al., 2023). MSMEs are often the main targets of cyber-attacks because their protection systems tend to be weaker than large companies that have more sophisticated digital security resources (Yudhiyati et al., 2021; Institute, 2023).

While the recognition of the significance of cybersecurity is growing, numerous MSMEs continue to encounter a disparity between understanding and executing digital protection measures. Strengthening internal controls and enhancing self-efficacy can improve employee productivity, mainly when employees are working remotely and accessing databases securely (Haryanto & Setiawan, 2022). Although the majority of MSMEs recognize the cyber threats that may jeopardize the continuity of their operations, only a tiny number have put protective strategies like firewalls, two-factor authentication, and data encryption into action. This discrepancy is referred to as the cybersecurity paradox, highlighting a lack of alignment between awareness of digital risks and the application of effective mitigation techniques (Schinagl et al., 2022; Carter, 2023).

Some of the main factors causing low implementation of cybersecurity in MSMEs are limited financial resources, lack of experts in the field of digital security, and low understanding of security investment as a long-term protection strategy (WEF, 2024). Many MSMEs consider investing in cybersecurity to be an additional cost that is not urgent without realizing that cyber threats can cause operational disruptions, manipulation of financial reports, and loss of customer trust (Pandey et al., 2020)4). Therefore, an approach is needed to help MSMEs manage their resources more effectively and improve digital protection.

In this context, management accounting plays a strategic role in optimizing cyber risk management. Management accounting-based approaches, such as cost-benefit analysis, cost control, and risk evaluation, can be used to help MSMEs allocate cybersecurity budgets more efficiently (Jain et al., 2025). With this approach, MSMEs can better understand how investing in digital security can improve operational efficiency and minimize potential losses due to cyberattacks. The contribution of MSMEs to regional economic growth is evident, so keeping them healthy and growing will benefit all stakeholders (Haryanto et al., 2024).

Despite the extensive literature on cybersecurity in MSMEs, research connecting digital security to management accounting is limited. This study aims to analyze the gap between cybersecurity awareness and implementation in MSMEs and explore how a management accounting approach can address these challenges. Using narrative review and conceptual analysis, it will examine relevant academic literature and industry reports to identify key challenges and mitigation strategies for the MSME sector.

2. LITERATURE REVIEW

2.1 Cybersecurity in MSMEs: Challenges and Paradoxes of Awareness

Cybersecurity is a fundamental aspect of business sustainability in the digital era. Cyber-attacks on MSMEs have continued to increase in recent years, with increasingly complex modes, such as phishing, ransomware, and financial data manipulation. A Ponemon Institute (2023) study found that cyberattacks can cause significant financial losses for MSMEs, with an average recovery cost of USD 100,000. This cost includes system repairs, data recovery, and reputational impacts due to loss of customer trust.

On the other hand, research by the Ministry of Communication and Information (2023) shows that although most MSMEs know cybersecurity risks, only a few allocate resources to invest in digital protection technology. This leads to a cybersecurity paradox, where business owners understand the importance of digital security but do not take adequate precautions. One of the leading causes of this phenomenon is ignorance of the long-term benefits of cybersecurity investments and the assumption that digital threats only target large companies (Carter, 2023).

2.2 The Role of Management Accounting in Cyber Risk Management

In financial and operational management, management accounting strategically assesses cybersecurity investments' costs, benefits, and risks. Management accounting-based approach can help MSMEs optimally allocate budgets for digital security by considering efficiency and cost control. (Jiang, 2024). The cost-benefit analysis allows MSMEs to assess the extent to which investments in cybersecurity can reduce the risk of losses due to digital attacks. Thus, MSMEs can make more informed decisions regarding spending priorities, such as investing in firewalls, encryption systems, or employee training on cybersecurity.

Cost control and operational efficiency are also important parts of this strategy. MSMEs need to optimize the use of limited resources by adjusting cybersecurity policies that are appropriate to the scale of their business. With better cost management, MSMEs can reduce the potential for waste in digital security investments that are irrelevant to their business needs (Triwahyono et al., 2023). In addition, risk evaluation is also needed to identify the main threats that can disrupt the financial stability of MSMEs due to cyber-attacks. Developing risk management-based mitigation strategies, such as regular security audits, data backup policies, and cyber incident response procedures, is important to maintaining business continuity. Ensuring strong cybersecurity measures is crucial as employees increasingly work from home. This is particularly important for professionals like accountants conducting analytical data audits, as they must manage sensitive information securely while maintaining their productivity (Setiawan et al., 2023). The management accounting-based approach focuses on digital protection, business sustainability, and financial stability. A study by Better Accounting (2024) found that MSMEs that apply management accounting principles in their cybersecurity strategies can increase operational efficiency by 30% and reduce the risk of losing financial data by up to 40%.

2.3 Literature Gaps and Contributions of This Study

Although various studies have discussed the importance of cybersecurity for MSMEs, most still focus on technical and regulatory aspects without considering how a management accounting approach can help manage resources for digital security. Therefore, this study fills the gap in the literature by linking cybersecurity aspects with financial risk management in MSMEs.

Adopting a narrative review-based conceptual approach, this study aims to identify key challenges in implementing cybersecurity in MSMEs and propose mitigation strategies based on management accounting principles. The primary contribution of this research is the creation of a conceptual framework that can help MSMEs enhance their digital readiness more effectively and sustainably. Consequently, this study delivers more profound academic insights into the cybersecurity dilemma MSMEs face. It presents practical solutions for stakeholders to bolster the digital resilience of MSMEs through a strategy focused on financial efficiency and risk management.

3. RESEARCH METHOD

3.1 Research Approach

This study uses a qualitative approach based on narrative review and conceptual analysis, which aims to explore the gap between cybersecurity awareness and implementation in MSMEs and analyze how management accounting can help mitigate cyber risks. The narrative review approach was chosen because it allows for in-depth analysis of existing literature without using statistical data processing (Snyder, 2019). Narrative review allows researchers to identify patterns, trends, and gaps in previous research and develop a more comprehensive understanding of the issues being studied (Baumeister & Leary, 1997). In addition, this study also adopts conceptual analysis to build a theoretical framework that connects cybersecurity with the management accounting approach in the context of MSMEs. This approach is used to develop a conceptual model that can assist in formulating risk mitigation strategies based on financial management. Conceptual analysis is often used in research that aims to clarify concepts that are not well structured or build new relationships between existing theories (Jaakkola, 2020).

3.2 Data Sources and Literature Selection Criteria

The data used in this study come from secondary sources, consisting of academic journals, industry reports, and policy documents related to cybersecurity and MSMEs. To ensure the quality and relevance of the literature used, this study sets several selection criteria as follows: When conducting a literature review, it is essential to focus on academic journals, official industry, and policy reports from reputable organizations such as the World Economic Forum (WEF), the Ponemon Institute, and the Association of International Certified Professional Accountants (AICPA & CIMA). The review specifically highlights studies addressing cybersecurity within MSMEs, financial risk management, and the role of management accounting in overseeing digital technology investments. Furthermore, it is crucial to include literature that contributes to developing conceptual frameworks encompassing cybersecurity theories, cost-benefit-based decision-making theories, and management accounting approaches tailored for cyber risk management.

3.3 Data Analysis Strategy

This study employs three primary analysis stages: thematic analysis, comparative analysis, and developing a conceptual framework. The thematic analysis identifies key patterns in the literature, focusing on themes such as cybersecurity awareness and implementation among MSMEs, barriers to digital security adoption, and the role of management accounting in reducing cyber risks. This approach follows established qualitative research methods to uncover themes across various data sources (Braun & Clarke, 2006). The study uses comparative analysis alongside thematic analysis to enhance its findings. By comparing various studies and policies on cybersecurity in MSMEs across different countries, it examines how differences in regulation, infrastructure, and digital literacy affect the implementation of cybersecurity measures. A conceptual framework is also developed that connects cybersecurity approaches with management accounting strategies for managing cyber risk in MSMEs. It highlights how tools like cost-benefit analysis and risk evaluation can help overcome barriers to implementing digital security measures.

3.4 Methodological Limitations

This study has several limitations as a narrative review and conceptual analysis-based study. First, this study did not collect primary data, so the results obtained depend on findings from published literature. Second, this study did not use statistical methods or quantitative modeling, so the relationship between variables cannot be tested numerically. Third, this study focuses more on financial management and accounting, so other factors, such as behavioral psychology in cybersecurity decision-making or technical aspects of information security, have not been discussed in depth. Nevertheless,

with an approach based on narrative review and conceptual analysis, this study still provides important academic contributions by identifying gaps in the literature and developing a theoretical framework that can be the basis for further research using an empirical approach.

4. RESULTS AND DISCUSSION

4.1 The gap between Cybersecurity Awareness and Implementation in MSMEs

The analysis results show that cybersecurity awareness among MSMEs is relatively high, but the implementation of mitigation measures is still minimal. While MSMEs are aware of cyber threats, only a tiny portion implement protective strategies such as firewalls, two-factor authentication, and data encryption. This imbalance is known as the cybersecurity paradox, where business owners understand digital risks but do not take adequate mitigation measures. This situation also frequently comes from older employees who are not as familiar with new technologies as compared to the new generations (Setiawan et al., 2021).

Some of the main factors causing the low implementation of cybersecurity in MSMEs include limited financial resources, lack of experts in the field of digital security, and low understanding of cybersecurity as a long-term investment (Institute, 2023). Many MSMEs consider investing in cybersecurity to be an additional, non-urgent cost without realizing that cyber threats can cause significant financial losses, operational disruptions, financial report manipulation, and loss of customer trust (Accounting, 2024). Table 1 shows the gap between the percentage of MSMEs aware of cybersecurity's importance and the percentage that implement digital security measures.

Table 1. The Gap between Cybersecurity Awareness and Implementation in MSMEs

Cybersecurity Factors	Awareness (%)	Implementation (%)
Cyber Risk Awareness	75	30
Use of Firewalls	60	25
Implementation of Two-Factor Authentication	55	20
Data Encryption	50	15
Employee Cybersecurity Training	40	10

(Source: Research Processed data, Ponemon Institute, 2023)

The **Table 1**, shown that although 60% of MSMEs understand the importance of firewalls, only 25% use them. The same happens with two-factor authentication, where awareness reaches 55%, but implementation is only 20%. Thus, the main challenge is not a lack of awareness but rather the difficulty in allocating resources and understanding the long-term benefits of cybersecurity.

4.2 Impact of Cyber Attacks on MSME Accounting Systems

Cyber-attacks have a significant impact on MSME accounting and financial management systems. A study by the Ponemon Institute (2023) found that recovering from a cyber-attack on MSMEs can reach USD 100,000, including system recovery costs, loss of financial data, and negative impacts on business reputation. As a result, disruptions in accounting systems can lead to inaccurate financial reports, manipulation of transaction data, and difficulties in tax reporting and financial audits. Table 2 summarizes the types of cyber-attacks that frequently target MSMEs, the potential financial losses they cause, and their impact on business confidence.

Table 2. Impact of Cyber-Attacks on MSME Accounting Systems

Types of Cyber Attacks	Potential Financial Losses (USD)	Impact on Business Confidence
Phishing	50,000	Medium
Malware/Ransomware	100,000	High
Financial Data Peninsulas	75,000	High
Financial Report Manipulation	85,000	Very High
Accounting Operational Disruption	60,000	Medium

(Source: Research Processed data, Ponemon Institute, 2023; Better Accounting, 2024; AICPA & CIMA, 2024)

The **Table 2**, shown that malware and ransomware are the biggest threats to MSME accounting systems, with potential losses reaching USD 100,000. These attacks have a high impact on business trust, as they can lead to theft of customer data, loss of important financial documents, and operational delays that result in the loss of clients or business partners. In addition, phishing attacks are also dangerous, with an average loss of USD 50,000, because they often trick business owners into disclosing sensitive login information.

4.3 Cybersecurity Strengthening Strategy in MSMEs Based on Management Accounting

A management accounting-based approach can be used as a strategic solution to bridge the gap between awareness and implementation of cybersecurity in MSMEs. This approach not only focuses on the technical aspects of cybersecurity but also considers cost control, risk management, and optimization of financial resources. Table 3 shows the main strategies MSMEs can implement to improve cybersecurity and the effectiveness and readiness of implementation in the MSME sector.

Table 3. Cybersecurity Strengthening Strategy in MSMEs Based on Management Accounting

Cyber Security Strategy	Level of Effectiveness (1-5)	Readiness for Implementation in MSMEs (%)
Cost-Benefit Analysis for Cyber Investment	5	40
Security Integration into Internal Control	4	30
Regular Employee Training	4	25
Periodic Data Backup Policy	5	50
Financial System Security Audit	5	35

(Source: Research Processed data, Better Accounting, 2024; Ponemon Institute, 2023)

Based on the **Table 3**, the cost-benefit analysis strategy for cybersecurity investment, periodic data backup policies, and financial system security audits are the most effective (5 out of 5). However, only 40% of MSMEs are ready to implement cost-benefit analysis, while data backup is 50% implementation-ready, making it the most straightforward strategy to implement. On the other hand, security integration in internal control is quite effective (4 out of 5), but the level of implementation readiness in MSMEs is still low (30%). This shows that many MSMEs need policy support, education, and incentives from the government and technology service providers to implement digital security measures more widely.

4.4 Implications

The findings of this study confirm that although MSMEs are aware of cybersecurity risks, the implementation of protection strategies is still minimal due to limited resources and a lack of understanding of digital security investments. By implementing management accounting principles, MSMEs can optimize their budget allocation, reduce costs due to cyber-attacks, and increase their business resilience in the digital era. Moving forward, the government, financial regulators, and the private sector need bold intervention to increase MSMEs' awareness and readiness for adopting cybersecurity. The interventions can be tax incentives for digital security investments, education programs, and the provision of more affordable cybersecurity infrastructure. The education sector should also begin an early program by educating students or the new generations (Z) about the importance of risk management (Setiawan & Haryanto, 2024).

5. CONCLUSION

This study highlights the cybersecurity paradox in MSMEs, where high awareness of cyber risks is met with low implementation of protective measures like firewalls and data encryption. Major obstacles include budget constraints, a lack of digital security expertise, and a limited understanding of cybersecurity's long-term benefits. Consequently, MSMEs remain vulnerable to cyberattacks, jeopardizing their accounting systems, financial statements, and overall stability. This study found that cyberattacks, including phishing and ransomware, can lead to significant financial losses and erode trust among customers and partners. A systematic strategy incorporating management accounting is essential to enhance digital security in MSMEs. The study highlights that management accounting tools, such as cost-benefit analysis and risk evaluation, can help MSMEs allocate resources effectively for cybersecurity. Implementing financial system security audits and regular data backups has proven effective, but readiness remains low due to limited understanding and lack of policy support. Thus, this study enriches the literature by linking cybersecurity and management accounting aspects and providing recommendations for stakeholders, including the government, financial sector, and technology providers.

Further support in the form of fiscal incentives, cybersecurity education, and the provision of more affordable security infrastructure is needed to help MSMEs strengthen their digital resilience. Although this study provides in-depth conceptual insights, further studies using an empirical approach are needed to test the effectiveness of the proposed model in various business contexts. Future research can explore how cybersecurity regulations and managerial behavioral factors influence decision-making in digital security investment. With a more holistic approach, it is hoped that MSMEs can be better prepared to face cyber threats and maintain their financial stability in the digital economy era.

ACKNOWLEDGEMENTS

The author would like to thank all parties who supported this research in Indonesia.

REFERENCES

Accounting, B. (2024). *How Cybersecurity in Accounting Protects SMEs in 2025*. Better Accounting. https://betteraccounting.com/cybersecurity-in-accounting/

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology*, *1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Carter, W. J. (2023). *The crucial role of cybersecurity for accounting firms*. AICPA & CIMA. https://www.aicpa-cima.com/professional-insights/article/the-crucial-role-of-cybersecurity-for-accounting-firms

Haryanto & Setiawan, A. (2022). Pengaruh Pengendalian Intern dan Self-Efficacy terhadap Kinerja pada Masa Bekerja secara Online. *Jurnal Riset Akuntansi Dan Keuangan*, *10*(1), 151–164. https://doi.org/10.17509/jrak.v10i1.34184

Haryanto, H., Nurainie, N., Querelia, M., & Wijaya, Y. R. (2024). The Role of MSMEs in Driving the Economy of Singkawang: A Systematic Literature Review. *Jurnal Ilmiah Raflesia Akuntansi*, *10*(1), 427–434. https://doi.org/10.53494/jira.v10i1.486

Hendrawan, S. A., Chatra, A., Iman, N., Hidayatullah, S., & Suprayitno, D. (2024). Digital transformation in MSMEs: Challenges and opportunities in technology management. *Jurnal Informasi Dan Teknologi*, 141–149. https://doi.org/10.60083/jidt.v6i2.551

Institute, P. (2023). *The Impact of Cybersecurity Breaches on SMEs: Cost and Risk Factors*. Ponemon Institute. https://www.ponemon.org

Jaakkola, E. (2020). Designing conceptual articles: four approaches. *AMS Review*, *10*(1), 18–26. https://doi.org/10.1007/s13162-020-00161-0

Jain, A., Kakade, K. S., & Vispute, S. A. (2025). The Role of Artificial Intelligence (AI) in the Transformation of Small-and Medium-Sized Businesses: Challenges and Opportunities. *Artificial Intelligence-Enabled Businesses: How to Develop Strategies for Innovation*, 209–226. https://doi.org/10.1002/9781394234028.ch12

Jiang, J. (2024). A Study on the Digital Transformation Trends in Financial Management for Small and Micro Enterprises. *International Journal of Global Economics and Management*, *3*(1), 355–363. https://doi.org/10.62051/IJGEM.v3n1.42

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. In *Sustainability (Switzerland)* (Vol. 15, Issue 18). https://doi.org/10.3390/su151813369

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, *122*, 102903. https://doi.org/10.1016/j.cose.2022.102903

Setiawan, A., Djajadikerta, H., Haryanto, H., & Wirawan, S. (2021). Theory of Reasoned Action dan Literasi Teknologi terhadap Adaptasi Perubahan Teknologi. *Jurnal Sistem Informasi Bisnis*, *11*(1), 51–61. https://doi.org/10.21456/vol11iss1pp51-61

Setiawan, A., Djajadikerta, H., Wirawan, S., Faninda, S., & Haryanto, H. (2023). The Consequences of Work from Home Policy on the Productivity of Indonesian Accountants During the COVID-19 Outbreak. *International Journal of Economics, Finance and Management Sciences*, *September 2023*. https://doi.org/10.11648/j.ijefm.20231105.12

Setiawan, A., & Haryanto, H. (2024). Exploring the perspective of Generation Z on personal risk management. *Journal of Economics and Business (JECOMBI)*, *4*(02), 60–73. https://doi.org/10.21456/vol11iss1pp51-61

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(July), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Triwahyono, B., Rahayu, T., & Kraugusteeliana, K. (2023). Analysing the role of technological innovation in improving the operational efficiency of MSMEs. *Jurnal Minfo Polgan*, *12*(1), 1417–1426. https://doi.org/10.33395/jmp.v12i1.12791

WEF. (2024). *SMEs can turn cybersecurity risk into opportunity. Here's how*. World Economic Forum (WEF). https://www.weforum.org/stories/2024/07/smes-can-turn-cybersecurity-risk-into-opportunity-heres-how/

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, *19*(4), 446–462. https://doi.org/10.1108/JICES-03-2021-0035