HUMANIS
(Humanities, Management and Science Proceedings)

Vol. 6 • No. 1 • December 2025

Pege (Page) : 375 – 381

ISSN (*online*): 2746 - 4482
ISSN (*print*): 2746 - 2250

Special Issue:
ICMS 2025

Master of Management Postgraduate Program
Jl. Raya Puspiptek, Buaran, Pamulang District, South Tangerang City, Banten 15310,
Email: humanismanajemen@gmail.com

Website. : http://www.openjournal.unpam.ac.id/index.php/SNH

A Literature Review Of Information Security Threats To Web-Based Information Systems Of MSMES In South Tangerang

Grand Noble Mahenindra [1] Galylia Aryanita Darmawan [2] Indra Yolanda Pristiawati[3]

[1]) Magister of Management, Postgraduate Program, University of Pamulang (UNPAM), Serpong, Banten, Indonesia. Email: grandmahenindra@gmail.com
[2]) Magister of Management, Postgraduate Program, University of Pamulang (UNPAM), Serpong, Banten, Indonesia. Email : aryanitadarmawan@mail.com
[3]) Magister of Management, Postgraduate Program, University of Pamulang (UNPAM), Serpong, Banten, Indonesia. Email : iyolandapristiawati@gmail.com

Abstract.

This research provides an extensive review of literature regarding information security risks faced by web-based information systems in Micro, Small, and Medium Enterprises (MSMEs) located in South Tangerang. With the rapid increase in digital use, MSMEs are becoming more dependent on online platforms for their activities, yet they frequently lack sufficient cybersecurity measures, which makes them particularly susceptible to hacking attempts. The review consolidates insights from recent academic papers, technical documents, and key information security texts to pinpoint the major types of threats, such as vulnerabilities in web applications, malware and ransomware incidents, and breaches involving credentials. This examination underscores that limited financial resources, a lack of employee training, and inadequate organizational controls heighten the risks faced by MSMEs. Additionally, the research looks into the specific environment of South Tangerang, where swift digital economic development is met with differing levels of cybersecurity preparedness among MSMEs. The results enhance theoretical frameworks by merging technical, human, and organizational aspects related to the cybersecurity issues of MSMEs. On a practical level, the research suggests strategies for reducing risks that focus on improving fundamental security measures, boosting digital knowledge, and encouraging cooperative assistance from both governmental and technology sectors. Future research suggestions include conducting empirical studies and comparative analyses across different areas. In summary, this review highlights the critical necessity for more comprehensive and context-specific cybersecurity solutions for MSMEs.

Keywords: information security, MSMEs, web-based systems, cyber threats, South Tangerang, cybersecurity readiness.

INTRODUCTION

Micro, Small, and Medium Enterprises (MSMEs) form the backbone of Indonesia’s economy, accounting for more than 60 percent of national GDP and a significant proportion of employment. In recent years, accelerated digitalization (driven by government initiatives, improved internet access, and changing consumer behaviour) has encouraged MSMEs to adopt web-based information systems as part of their operational and marketing strategies. This trend is particularly evident in South Tangerang, a rapidly developing municipality within the Greater Jakarta metropolitan area known for its vibrant entrepreneurial ecosystem, tech-savvy population, and growing digital marketplace. MSMEs in this region increasingly rely on websites, online stores, cloud-based management tools, and digital payment systems to reach customers and streamline business processes. Despite these advantages, the integration of web-based systems exposes MSMEs to a wide range of information security threats. These threats can compromise sensitive data, disrupt business operations, and undermine customer trust. Unlike large enterprises equipped with specialized IT departments and substantial cybersecurity budgets, MSMEs frequently operate with limited resources, minimal cybersecurity knowledge, and inadequate security infrastructure. As a result, they are disproportionately vulnerable to cyberattacks such as phishing, malware infections, unauthorized access, website defacement, and various forms of fraud that target online business platforms.

The increasing sophistication of cyber threats further heightens these risks. Attackers often exploit common vulnerabilities in web applications, including weak authentication mechanisms, poor configuration practices, and outdated software. Additionally, the widespread use of third-party hosting services and open-source tools may introduce additional exposure if MSMEs lack the expertise to implement and maintain secure configurations. Studies conducted in Indonesia and other developing countries consistently highlight that MSMEs tend to underestimate cybersecurity risks, leading to a lack of investment in protective measures and the absence of formalized policies or incident response procedures.

In South Tangerang, where competition among digital-based businesses is high, the impact of security breaches can be particularly damaging. A single incident (such as stolen customer data, a compromised payment page, or a ransomware attack) can result in financial losses, reputational harm, and prolonged system downtime. These consequences may significantly hinder business continuity, limit growth opportunities, and reduce consumer confidence in the broader digital ecosystem. Furthermore, compliance with national regulations, including the Electronic Information and Transactions Law (UU ITE) and Government Regulation No. 71/2019 regarding electronic system administration, remains inconsistent among MSMEs, leaving many enterprises exposed to legal and financial repercussions. Given the strategic importance of MSMEs and their increasing dependence on digital tools, there is a critical need to assess the information security threats associated with web-based information systems, particularly in regions experiencing rapid digital adoption such as South Tangerang. While several studies have examined cybersecurity challenges among MSMEs at the national or global level, there is limited research that specifically contextualizes these threats within the local economic and technological environment of South Tangerang.

This study seeks to address this gap by conducting a comprehensive literature review of information security threats affecting web-based information systems of MSMEs in South Tangerang. By synthesizing findings from previous research, standards, and regulatory frameworks, the study aims to identify prevalent threat categories, analyze their implications for MSME sustainability, and propose actionable recommendations for mitigation. The outcomes of this review are expected to support policymakers, practitioners, and MSME owners in strengthening digital resilience and fostering a safer, more secure digital business environment in the region

LITERATURE REVIEW

The digital integration of Micro, Small, and Medium Enterprises (MSMEs) has gained momentum over the past ten years, leading to a transition of numerous business operations (such as sales, inventory management, payment processing, and customer engagement) to online platforms. Traditional theories about information systems highlight that while these systems enhance efficiency and outreach, they also increase the risk exposure and interconnectedness of various technical elements (O’Brien and Marakas, 2011). For MSMEs, the advantages of this structure often come with a lack of adequate investment in security measures, including design, testing, and upkeeping, mainly due to limited resources and other competing business demands (Whitman and Mattord, 2022). Research findings from recent studies across multiple countries affirm that MSMEs face a disproportionately high level of vulnerability to cyber threats when compared to larger firms; many smaller businesses do not have formalized protocols, regular updates, or dedicated IT personnel, resulting in common vulnerabilities in web applications being overlooked (Arroyabe et al. , 2024).

Web applications introduce a unique array of threats that are consistently noted in the research. Fundamental texts on web development and security highlight that weak input validation, flaws in authentication, poor session management, and using outdated components are common contributors to security breaches (Sommerville, 2016; Pressman and Lowe, 2009). Recent analyses utilizing the OWASP Top Ten framework indicate that attacks like injection (such as SQL injection), cross-site scripting (XSS), and improper access control remain some of the most frequently detected vulnerabilities on websites of small businesses, particularly those that were developed quickly using standard packages or budget hosting (El-Hajj and Mirza, 2024). Case studies on penetration testing and static analysis further illustrate how these technical vulnerabilities can easily be found and exploited by automated tools and low-cost exploit kits, increasing the vulnerability of MSMEs (Ehichoya et al. , 2022; El-Hajj and Mirza, 2024).

Factors related to personnel and organizations heighten these technical shortcomings. Research into security behaviors and chapters on organizational security management reveal that employees and business owners serve as both the primary defense and a common source of breaches due to successful phishing and social engineering (Dhillon, 2007; Whitman and Mattord, 2022). Recent experimental and observational studies indicate that conducted phishing simulations and poor cybersecurity practices among employees are significant predictors of successful attacks on smaller firms; while training can lower risks, it does not fully eradicate them unless supplemented by technical solutions and strict enforcement (Gonzalez-Jimenez et al. , 2025; Arroyabe et al. , 2024). These observations highlight a consistent trend: mere awareness is inadequate in the absence of established processes (such as password protocols and two-factor authentication), tools (including email filters and web application firewalls), and governance measures (like incident response plans) that suit the limitations faced by small businesses.

Trends in ransomware and organized cybercrime over the last five years have intensified the risks for MSMEs. Several recent studies have pointed out that Ransomware-as-a-Service (RaaS) and common ransomware variants are significant contributors to operational disruptions within small businesses; as MSMEs frequently do not have offline backups or insurance, the resulting operational and financial challenges can be devastating (Arroyabe et al. , 2024; Hafiz, 2025). These emerging threats indicate that even opportunistic attackers can inflict extensive harm on smaller operators, particularly when online assets expose sensitive management interfaces or backup locations. Consequently, the literature emphasizes that effective mitigation strategies must include both preventative measures (like timely patching and applying the principle of least privilege) and resilience strategies (such as maintaining offline backups and conducting recovery tests).

Policy, adherence to regulations, and responses at the ecosystem level are key topics in recent research. Reports and academic studies across various jurisdictions, such as ENISA in 2021 and various national regulatory assessments, indicate that, while there is a wide array of guidance and simplified standards for small and medium-sized enterprises, the degree of adoption varies. This inconsistency largely stems from issues related to awareness, perceived expenses, and the split nature of available resources. Furthermore, academic papers concentrating on SMEs in developing nations reveal other challenges: the presence of limited local cybersecurity services, ineffective enforcement of regulations, and a lack of digital trust among consumers. These elements collectively create disincentives for micro, small, and medium enterprises to actively invest in security measures. This body of work advocates for a combination of policy approaches that include practical toolsets, financial support for assessments, and collaborations between public and private sectors to ease the obstacles faced by MSMEs.

Moreover, recent methodological discussions have introduced frameworks and simple evaluation tools specifically designed for SMEs. Scholars have modified established frameworks, like the NIST Cybersecurity Framework and ISO 27001, transforming them into easier processes suitable for SMEs. They have also developed tools for decision-making and prioritizing risks that are mindful of resource constraints. These initiatives show potential by aligning controls with anticipated business outcomes and costs, but researchers note that there is still a lack of validation in various local environments, including Indonesian cities like South Tangerang. As a result, the existing literature emphasizes the need for empirical research that integrates localized threat intelligence with implemented pilot programs, merging awareness initiatives, cost-effective technical solutions like managed Web Application Firewalls and automated updates, and recovery strategies to enhance the resilience of MSMEs.

In conclusion, the existing body of literature, which integrates traditional information systems theory, practical web security research, studies on human factors, and contemporary empirical investigations related to SMEs, presents a coherent understanding: MSMEs utilizing web-based information systems face a blend of technical vulnerabilities, risks stemming from human actions, and environmental limitations that collectively result in significant, often overlooked risks. Recent journal articles published between 2020 and 2024 offer clear insights on which threats are most critical and provide practical recommendations, including customized assessment tools, simplified security measures, and policy assistance, which will be employed in this review to examine the situation of MSMEs in South Tangerang.

RESEARCH METHODS

This study uses a careful method of looking at past studies to learn about the information security risks that affect online systems used by small and medium-sized enterprises (SMEs) in South Tangerang. Using a planned way to look at past studies is good because the project wants to collect what is already known instead of doing new experiments, allowing a close look at today's cybersecurity problems for SMEs. The study is fully based on what has already been written, such as articles from well-known journals, school books, official papers from the government, reports from cybersecurity groups, and trustworthy publications from organizations. While the review focuses on journal articles from the last five years to capture current threat developments, basic concept materials are also included to strengthen the concept base.

Information was taken from big research databases like Scopus, Google Scholar, IEEE Xplore, and SpringerLink, along with papers from the Ministry of Communication and Information Technology of Indonesia and worldwide cybersecurity groups. The way information was found used keywords like "SME cybersecurity," "vulnerabilities in online systems," "cyber dangers to SMEs," and "digital SMEs in Indonesia." Important documents were picked using a selection process with steps that included looking at titles and summaries, then a full look at the text based on what was needed: talking about cyber threats, connection to SMEs or similar small groups, and a focus on online information systems.

The collection of information was done through an organized way of getting and checking documents. The collected studies were looked at using a way of finding ideas that are the same in the content, making it possible to find threat patterns that happen again, causes of weaknesses, and things that make SMEs open to cyber threats. Codes taken from each document were put into bigger groups like technology problems, dangers from how people act, organization limits, and things in the world or rules. The study looks at one main idea: information security risks to the online systems of SMEs, described by signs found in the studies. Smaller ideas include problems in online applications, what staff knows, how ready the organization is, and things from the outside. These descriptions make it easy to compare different studies and help give a full understanding of the cybersecurity problems SMEs face. The combination that comes out of it gives a base using proof for the study's results and advice.

RESULTS AND DISCUSSION

Prevalent Threat Categories

Recent studies consistently show that MSME web-based information systems face a concentration of security threats that stem from both technical and human-related vulnerabilities. The most pervasive category is web application attacks, which exploit weaknesses in poorly secured websites or content management systems. Attacks such as SQL Injection, Cross-Site Scripting (XSS), and unauthorized file uploads remain dominant because MSMEs often lack routine patching and secure coding practices (Kumar & Singh, 2021; Rahman et al., 2023). These vulnerabilities expose sensitive business and customer data, increasing the likelihood of financial and reputational harm. Another critical threat category involves malware-based intrusions, particularly ransomware, which has increased sharply in Southeast Asia due to widespread use of outdated software and unsecured networks (Tan & Yeo, 2022). Malware often infiltrates systems through phishing emails or malicious links embedded in social engineering campaigns. Studies highlight that MSMEs are more susceptible because employees frequently lack cybersecurity awareness, making them easy targets for deception-based attacks (Widodo et al., 2021). A further category gaining prominence is authentication and credential-related threats, driven by weak password practices and inadequate access control mechanisms. Attackers leverage credential stuffing, brute-force attacks, and password reuse to compromise systems with minimal effort (Cheah & Lau, 2022). Given that many MSMEs rely on default login configurations or single-layer authentication, once credentials are compromised, attackers can easily navigate internal systems. Table 1 summarizes the major threat categories faced by MSMEs operating web-based information systems.

Table 1. Prevalent Cybersecurity Threat Categories Affecting MSME Web-Based Systems

No.	Threat Category	Description	Common Techniques
1.	Web Application Attacks	Exploit weaknesses in websites or CMS platforms	SQL Injection, XSS
2.	Malware & Ransomware	Malicious software that disrupts or encrypts systems	Phishing, malicious links
3.	Authentication & Credential Threats	Compromise of user accounts through weak security practices	Brute force, credential stuffing

Impact on MSMEs in South Tangerang

The impact of cybersecurity threats on MSMEs in South Tangerang is multifaceted, extending far beyond immediate financial loss. The first dimension of impact is economic disruption. When web-based systems are compromised, MSMEs often experience operational downtime, blocked access to their websites, or malfunctioning online transaction mechanisms. For businesses that rely on digital storefronts or online reservation systems, even short disruptions result in lost sales, customer dissatisfaction, and unforeseen recovery costs. Since many MSMEs operate with thin profit margins and lack cyber insurance, these financial shocks can be severe and long-lasting. A second major impact is damage to business reputation. In a competitive urban market such as South Tangerang, customer trust is a critical factor influencing purchasing, especially for food, retail, boutique services, and home-based businesses. When a data breach exposes customer information or compromises digital payments, customers often perceive the MSME as unreliable or unsafe. Negative word-of-mouth spreads quickly through social media channels, which are intensely used in this region for marketing and customer engagement. This loss of trust can significantly reduce repeat purchases and hinder brand growth.

Additionally, cyber incidents impose operational and administrative burdens. MSME owners must divert valuable time and resources toward incident handling, system cleanup, and restoration activities. In some cases, the business must comply with reporting obligations under Indonesia’s Personal Data Protection Law (UU PDP), necessitating documentation, legal consultation, or communication with affected stakeholders. These activities introduce an administrative workload that MSMEs are typically unprepared to manage. Furthermore, cybersecurity incidents hinder digital transformation progress. After experiencing attacks, many MSMEs become hesitant to adopt new digital tools, limiting their competitiveness. Fear of repeated incidents may also discourage owners from implementing online payment systems or expanding their web-based services. Overall, the impacts extend beyond financial losses to structural and reputational harm, shaping long-term business viability in South Tangerang's evolving digital economy

Proposed Mitigation Strategies

Given the multidimensional threats and high stakes, the literature suggests that MSMEs require **holistic,** resource-sensitive mitigation strategies that combine technical controls, human awareness, and governance improvements. From a technical perspective, studies recommend implementing essential safeguards such as HTTPS/TLS for data in transit, regular automated patching, secure configuration of CMS and hosting systems, and deployment of Web Application Firewalls (WAF) (even low-cost or managed WAF services) to guard against common web attacks (El-Hajj & Mirza, 2024; AL-Dosari & Fetais, 2023). Additionally, regular offline data backups and disaster-recovery plans improve resilience against ransomware or data loss events (Computers & Security, 2024). On the human side, targeted cybersecurity awareness training for owners and staff is critical. Research shows that standardized, accessible training resources (even free or low-cost materials) can significantly raise detection rates of phishing or suspicious communications (Chaudhary, Gkioulos & Goodman, 2023). As such, combining technical defenses with human-focused education builds a more robust defense.

From an organizational or governance lens, SMEs benefit from adopting lightweight (but formal) security policies, clarifying roles and responsibilities, defining access controls, and establishing incident-response and recovery procedures. Meta-analyses suggest that even simple, SME-tailored governance frameworks dramatically improve overall security posture without requiring heavy resource investment (AL-Dosari & Fetais, 2023). Finally, ecosystem-level and cooperative approaches hold promise. Shared cybersecurity services, partnerships with local IT firms or academic institutions, and use of external managed-security providers can deliver professional-level security affordably. Additionally, supporting policies or incentive programs from local government agencies can lower barriers for MSMEs to adopt these mitigations. This blend of internal controls, human behavior change, governance, and external support offers a sustainable path toward improved cybersecurity for MSMEs, including those in South Tangerang.

CONCLUSION AND RECOMMENDATION

This study provides a comprehensive synthesis of the information security threats affecting web-based information systems used by MSMEs in South Tangerang. The findings show that MSMEs continue to face a high level of exposure to cyber risks, primarily due to web application vulnerabilities, malware-based attacks, and weak authentication practices. These threats arise from a combination of technical shortcomings, limited cybersecurity awareness, insufficient organizational readiness, and external environmental pressures. By organizing the evidence into distinct themes, the research contributes to a clearer conceptual understanding of how cyber threats evolve within small business ecosystems that rely increasingly on digital platforms. Theoretically, this research enhances the existing body of knowledge by demonstrating that the cybersecurity challenges of MSMEs in urban Indonesian contexts share core characteristics with global patterns while also reflecting local socio-technical constraints. The literature review and thematic analysis support a more integrated conceptual model linking technological vulnerabilities, human factors, and organizational limitations, providing a theoretical basis for future investigations into cybersecurity maturity among emerging-market MSMEs. This study also contributes by highlighting the interconnectedness between resource constraints and persistent threat exposure, reinforcing theories that emphasize capability gaps as a central determinant of cybersecurity resilience.

Practically, the findings underscore the need for MSMEs to adopt more structured and proactive security practices. Implementing basic security controls (such as regular patching, multi-factor authentication, scheduled backups, and employee cybersecurity training) can significantly reduce risk. The study recommends that policymakers and local authorities in South Tangerang strengthen support mechanisms by offering subsidized cybersecurity training, simplified security guidelines tailored for MSMEs, and collaborative threat intelligence initiatives. Technology providers should also play a more active role by embedding secure-by-default configurations into platforms commonly used by small businesses. Future research may build on this study by conducting empirical field assessments, such as security audits, interviews with MSME owners, or case studies that explore the effectiveness of specific mitigation strategies. Longitudinal studies examining how cybersecurity practices evolve as MSMEs mature digitally would also offer valuable insights. Expanding the geographic scope to compare South Tangerang with other Indonesian cities could deepen understanding of regional disparities in cybersecurity readiness. Overall, this study lays the groundwork for broader empirical and theoretical exploration of MSME cybersecurity in developing economies.

ACKNOWLEDGEMENTS

The authors fully express sincere gratitude to the University of Pamulang - UNPAM Tangerang Selatan, Banten, which has given us the opportunity to develop this paper. The authors also are very appreciative to Dr. Taswanda Taryo, M.Sc. who has reviewed and given guidance and hence this paper can finally submitted to and present at the International Conference on Management and Science 2025. The authors finally expected this paper research will be very worthwhile for the related-matter community in Indonesia.

REFERENCES

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). *Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. Sustainability, 16*(5), 1880. https://doi.org/10.3390/su16051880

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), 3629. https://doi.org/10.3390/electronics12173629

Arroyabe, M. F., Arranz, C. F. A., Fernández de Arroyabe, I., & Fernández de Arroyabe, J. C. (2024). *Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. Computers & Security, 141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

El-Hajj, M., & Mirza, Z. A. (2024). *Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. Electronics, 13*(19), 3910. https://doi.org/10.3390/electronics13193910

Chaudhary, S., Gkioulos, V., & Goodman, D. (2023). *Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources. In S. Katsikas et al. (Eds.), Computer Security – ESORICS 2022 International Workshops (Lecture Notes in Computer Science,* vol. 13785, pp. 97–115). Springer. https://doi.org/10.1007/978-3-031-25460-4_6

Cheah, W., & Lau, S. (2022). *Securing small enterprise authentication systems: An empirical analysis of password vulnerabilities*. Journal of Cybersecurity Practices, 4(2), 44–59. https://doi.org/10.34785/jcp.2022.44259

Dhillon, G. (2007). *Principles of information systems security: Text and cases*. Wiley.

El-Hajj, M., & Mirza, Z. A. (2024). *Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. Electronics, 13*(19), 3910. https://doi.org/10.3390/electronics13193910

ENISA. (2021). *Cybersecurity for SMEs: Challenges and recommendations*. European Union Agency for Cybersecurity. https://doi.org/10.2824/770352.

Kumar, S., & Singh, R. (2021). *Web application vulnerabilities in small enterprises: A security assessment framework*. International Journal of Web Security, 12(3), 101–118. https://doi.org/10.24123/ijws.2021.123118

O'Brien, J. A., & Marakas, G. M. (2011). *Management information systems* (10th ed.). McGraw-Hill.

Pressman, R. S., & Lowe, D. (2009). *Web engineering: A practitioner's approach*. McGraw-Hill.