International Journal of Sustainable Applied Sciences (IJSAS)
Vol. 4, No. 7, 2026: 669-678

Literature Review: Cybersecurity Threat Trends in Micro, Small, and Medium Enterprises (MSMEs) in the Digital Era

Herwan Triason[1]*, Bisyron Wahyudi[2], Frado Sibarani[3]
Cyber Defense Engineering Study Program, Faculty of Defense Engineering and Technology, Indonesian Defense University
Corresponding Author: Herwan Triason herwan.triason@tp.idu.ac.id

ARTICLE INFO
Keywords: Cyber Security, MSMEs, Digital Transformation, Phishing, Digital Literacy

Received : 20, May
Revised : 26, June
Accepted: 28, July

ABSTRACT
Digital transformation provides operational convenience and market expansion for Micro, Small, and Medium Enterprises (MSMEs), but at the same time triggers an increase in exposure to cyber security threats. This study aims to map the cyber security threat trends in the MSME ecosystem, identify fundamental factors driving vulnerability, and formulate applicable mitigation strategies. Using a descriptive qualitative literature review approach, this study synthesizes various journal articles from academic databases to evaluate the current digital threat landscape. The analysis results show that social engineering (phishing) and data-hijacking software (ransomware) are the most dominant attack vectors in this sector. Architecturally, the main vulnerability of MSMEs is not purely caused by technological factors, but rather triggered by limited financial resources, the absence of information technology (IT) expert personnel, and the low level of digital literacy (cyber hygiene) among workers. The impact of cyber security incidents is proven to not only cause instant material losses, but also potentially paralyze operations totally and destroy brand reputation. Therefore, this study recommends a paradigm shift in cyber defense at the MSME level, moving from expensive hardware infrastructure investments to the implementation of behavior-based mitigation, such as the adoption of Two-Factor Authentication (2FA) and data backup routines.

DOI: https://doi.org/10.59890/ijsas.v4i7.25
ISSN-E: 3025-5597
http://ijsasjournal.my.id/index.php/ijsas

INTRODUCTION

The development of information and communication technology in the digital era has brought massive changes in various aspects of human life, including in the economic and business sectors. Digital transformation is no longer seen as merely an optional trend, but as a necessity for every business entity to survive and compete in an increasingly dynamic market. Increasingly even internet access, coupled with the sharply soaring adoption of smart devices, has created a new business ecosystem that is fast-paced, efficient, and borderless. Adaptation to this technology allows business processes to run more effectively, ranging from operational management, promotion, marketing, to financial transactions (Agit et al., 2024).

In Indonesia, Micro, Small, and Medium Enterprises (MSMEs) play a very crucial role as the backbone of the national economy. The contribution of MSMEs to the Gross Domestic Product (GDP) as well as their ability to absorb labor makes it the most massive economic driving sector. Recognizing the importance of this matter, the government together with various stakeholders continue to encourage MSME actors to immediately carry out digital transformation or *go digital* to expand their market reach. It is recorded that millions of MSMEs have now integrated their business wheels with e-commerce platforms, social media, and financial technology services to facilitate interactions with consumers (Utami et al., 2025).

Although digitalization offers various golden opportunities for the progress and efficiency of MSMEs, this transition actually also brings a dark side that cannot simply be ignored. When business activities increasingly depend on computer networks and cyberspace, the risk of digital security threats also increases exponentially. Cyberspace, which is virtual and without physical boundaries, has become a new arena for cybercriminals to launch their actions. Ironically, the euphoria of digital technology adoption by small business actors is often not balanced with an adequate understanding of the importance of data protection and information system security (Tangkelangi & Utamajaya, 2024).

Based on data from relevant agencies such as the National Cyber and Crypto Agency (BSSN), the cyber threat landscape in Indonesia continues to show a worrying upward trend every year. In recent years, up to billions of traffic anomalies identified as cyber attacks have been recorded, indicating that Indonesia's digital space is on high alert. These cyber attacks are actually no longer only targeting critical infrastructure belonging to state institutions or giant multinational corporations. The target network of hackers is now expanding, preying on anyone connected to the internet, regardless of the size of the business scale (Zulkarnain & Sutabri, 2023).

In this context, MSMEs often become one of the most vulnerable groups to cybercrime attacks in the digital realm. Unlike large companies that generally already have multi-layered data protection systems and established technology infrastructures, MSMEs are often considered by hackers as easy targets (*low-hanging fruit*). Cybercriminals realize that many small business actors manage and store important data—such as customer personal data, order information, to

financial data—but have very fragile digital defense fortresses to penetrate (Yusnanto et al., 2023).

The vulnerability of MSMEs to cyber threats is fundamentally triggered by several primary constraints frequently faced by small entrepreneurs. The main factor is limited operational budgets, where investments for cyber security software such as licensed antiviruses or firewalls are often considered as additional cost burdens instead of essential security investments. In addition, the limited human resources with specific expertise in the field of information technology make the management of security systems at the MSME level very minimal, or even non-existent (Octiva et al., 2024).

Besides budget and technical expert factors, low digital literacy regarding cyber security practices also exacerbates the vulnerability level. The majority of micro and small business actors often still mix the use of personal devices (such as smartphones or laptops) with devices specifically designated for business matters. The habits of downloading unofficial applications, using weak passwords, or using public Wi-Fi networks without protection make sensitive business data very easy to hack, intercept, or steal by irresponsible parties (Karim et al., 2024).

The impact of a cyber attack on an MSME can be very fatal and is often far more destructive compared to its impact on large companies. When a customer data leak or operational system paralysis occurs due to hacking, MSMEs are not only faced with direct financial losses to restore their operational systems. They also risk losing reputation and trust from their customers. For startups or small businesses, consumer trust is the most valuable asset that is very difficult to rebuild once destroyed by a cyber security incident (Munawar, 2018).

Furthermore, current cyber threat trends are increasingly sophisticated, such as the massive spread of malware, ransomware (data hostage for ransom), and phishing (social engineering to steal passwords). Although the urgency of protection for MSMEs is very clear amidst this rampant crime trend, there are still gaps in existing literature and academic research. The majority of studies on cyber security currently tend to focus their analysis more on banking, large-scale enterprises, or high-tech architectures, so tactical references and guidelines that are friendly to MSME capabilities are still relatively limited.

Based on this background, this literature review article is compiled to examine in-depth the cyber security threat trends that specifically target the MSME sector in the digital era. The main objective of this study is to map the types of cyber attacks that occur most frequently, identify the primary factors causing their vulnerability, and review their impact on MSME business continuity. Through the collection and analysis of previous literature, this article is expected to present a comprehensive summary that can serve as a foundation in formulating practical, easy-to-implement, and low-cost cyber security defense strategies for MSME actors.

LITERATURE REVIEW

Cyber Security Concepts in MSMEs

Cyber security refers to efforts, practices, and technologies designed to protect networks, devices, programs, and data from attacks, damage, or

unauthorized access. In the context of Micro, Small, and Medium Enterprises (MSMEs), various literatures emphasize that cyber security does not always revolve around complex server infrastructures, but rather on the protection of basic digital assets. This includes securing business social media accounts, protecting customer transaction data, and securing smartphone or laptop devices used for daily operations. Previous research agrees that protecting these digital assets is just as important as securing physical store assets.

Main Threat Trends in the MSME Sector Based on studies of various information security journals, there are three types of cyber threats that consistently become the biggest threats to MSME actors in the digital era:

- Phishing: Social engineering attacks where the perpetrator poses as a trusted party (such as a bank or e-commerce platform) via email or text messages (SMS/WhatsApp). The goal is to manipulate victims into handing over sensitive information, such as PINs, One-Time Passwords (OTPs), or passwords.
- Malware and Ransomware: Malicious software that infiltrates systems because users download unofficial applications or click on random links. Specifically, for Ransomware, this program will lock (encrypt) all business data on the MSME's device, and hackers will demand a ransom for the data to be accessed again.
- Account Hijacking: The forced takeover of business accounts due to the use of weak passwords or the lack of Two-Factor Authentication (2FA) features. Hijacked accounts are often used to scam the customers of the MSME.

Drivers of MSME Vulnerability

Various previous empirical studies have identified why MSMEs are far more vulnerable to the attacks above compared to large companies. The literature summarizes this vulnerability into two main factors:

- Resource Factors (Financial and Technical): MSMEs operate with tight profit margins, so allocating funds to purchase security software (such as paid antiviruses) is often sidelined. In addition, the lack of dedicated staff in the Information Technology (IT) field makes operational systems run without standard security supervision.
- Human Awareness Factors (Human Error): The majority of cyber security incidents in MSMEs stem from the lack of digital literacy among their workers. The use of the same password for various accounts, the habit of using public Wi-Fi networks without a VPN for business transactions, and mixing the use of personal devices and business devices are the main loopholes most often exploited by hackers.

METHODOLOGY

This study uses a qualitative method with a Literature Review approach. This approach was chosen because researchers did not conduct primary data collection in the field, but rather explored, summarized, and analyzed the cyber security threat trends in the MSME sector based on findings from relevant

previous studies. The implementation of this research includes three main stages, namely literature search strategy, criteria-based selection, and data analysis.

1. Literature Search Strategy Secondary data collection was conducted online through credible academic databases that can be accessed openly (*open access*). The main databases relied upon in this search include Google Scholar, Portal Garuda (Garba Rujukan Digital), and DOAJ (*Directory of Open Access Journals*). To obtain highly specific and relevant literature, searches were conducted using a combination of keywords in Indonesian and English, such as: "keamanan siber UMKM", "ancaman siber usaha kecil", "literasi digital UMKM", "cybersecurity SME", and "cyber threats small business".
2. Inclusion and Exclusion Criteria To ensure the literature reviewed remains relevant, accurate, and up-to-date, researchers set limitations on the selection of reading materials based on the following criteria:
   - **Inclusion Criteria:**
     - Scientific journal articles that have gone through a peer-review process.
     - Published within the last five years (2021–2026) to guarantee data novelty, considering digital technology trends and cybercrimes change very rapidly.
     - Have a focus of discussion on aspects of digital threats, cyber security literacy, or system vulnerabilities at the Micro, Small, and Medium Enterprise (MSME) level.
   - **Exclusion Criteria:**
     - Articles in the form of popular opinions, personal blog posts, or news from online portals that do not include a valid secondary data foundation.
     - Research that purely discusses the cyber security architecture of giant-scale companies (*enterprises*) or banking infrastructure that is not relevant to the technical capacity of MSMEs.
3. Data Analysis Techniques All literature that passed the selection criteria was then analyzed using content analysis techniques. This process began by summarizing the main points of each journal (data reduction), grouping the most frequently reported patterns of cyber-attacks, and mapping the root causes of their vulnerabilities. Furthermore, the grouped data was synthesized and presented descriptively to formulate practical conclusions and recommendations for MSME actors.

RESULTS AND DISCUSSION

The literature search and extraction yielded a number of comprehensive findings regarding the cyber threat landscape in Micro, Small, and Medium Enterprises (MSMEs) in the digital era. Analysis of the selected journal articles shows a consistent pattern regarding structural vulnerabilities and the types of attacks that most often target this sector. In general, the findings of this literature review are classified into three main discussion pillars, namely: identifying dominant cyber threats, analyzing fundamental factors driving vulnerability, and evaluating the impact of incidents on business organizational resilience.

In the first pillar regarding threat identification, the literature synthesis confirms that the digital threat ecosystem for MSMEs is very different from large corporations. The cyber threats that most often prey on MSMEs do not center on complex advanced attacks like Advanced Persistent Threats (APT). Instead, the Digital Threat Interaction Theory is proven empirically where hackers tend to exploit psychological loopholes of users and basic security weaknesses. This makes social engineering methods and malicious software (malware) infections the main weapons most frequently reported in various MSME security case studies.

Specifically, phishing ranks highest as the most successful attack vector penetrating MSME defenses. Through psychological manipulation, cybercriminals disguise themselves as authoritative parties (such as e-commerce platforms, banks, or logistics couriers) to deceive business owners and employees. This tactic is very effective because it often manages to manipulate targets into handing over login credentials, credit card numbers, or One-Time Passwords (OTPs) voluntarily. The high success rate of phishing proves that the weakest point in an MSME's cyber security architecture is not its computer systems, but its human users.

Besides phishing, ransomware (data hostage software) infections are identified as the second biggest nightmare threatening the survival of MSMEs. When operational hardware or digital cashier systems (Point of Sale) are infected due to users downloading suspicious files, all important business data will be encrypted by hackers. Literature studies show that most MSMEs do not have data backup systems isolated from the main network. This condition often forces business owners to pay large amounts of ransom to restore their operational access, even though there is no guarantee the data will be returned.

Table 1. Synthesis of Findings on the MSME Cyber Security Landscape

Analysis CategoryDominant Findings in LiteratureRecommended Mitigation ApproachesThreat Vectors	**Analysis CategoryDominant Findings in LiteratureRecommended Mitigation ApproachesThreat Vectors**	**Analysis CategoryDominant Findings in LiteratureRecommended Mitigation ApproachesThreat Vectors**
Phishing, Ransomware, Account Hijacking (Weak Credentials).	Phishing, Ransomware, Account Hijacking (Weak Credentials).	Phishing, Ransomware, Account Hijacking (Weak Credentials).
Implementation of Two-Factor Authentication (2FA) and email/message filtering.	Implementation of Two-Factor Authentication (2FA) and email/message filtering.	Implementation of Two-Factor Authentication (2FA) and email/message filtering.
Root of Vulnerability	Root of Vulnerability	Root of Vulnerability
Limited IT budget, lack of technical experts, low security literacy.	Limited IT budget, lack of technical experts, low security literacy.	Limited IT budget, lack of technical experts, low security literacy.

Moving to the second pillar, the literature uniformly concludes that limited financial resources are the main root cause of the high vulnerability of MSMEs. Unlike large-scale companies that have specific budget allocations for Information Technology (IT) security, MSMEs operate with very tight profit margins. The majority of business actors prioritize all their capital for production, marketing, and market expansion. As a result, investments in premium licensed antivirus software, firewalls, or system security audits are often seen as non-essential cost burdens that can be ignored.

These financial limitations directly impact the absence of qualified human resources in the IT field within the organizational structure of MSMEs. The management of digital infrastructure—ranging from social media to customer databases—is generally done concurrently by business owners who do not have a background in cyber security. This low digital literacy triggers a series of bad habits that enlarge vulnerability points, such as using identical passwords for personal and business accounts, using hardware interchangeably (shared devices), to the habit of accessing transaction data using unencrypted public Wi-Fi networks.

Entering the third pillar regarding the impact of incidents, the Organizational Resilience Theory finds its relevance when MSMEs face the post-cyber-attack phase. When hackers successfully penetrate defenses and steal data, the material impact experienced by MSMEs is instant and often fatal. This direct loss includes the disappearance of funds in business accounts, emergency costs for system recovery, and the cessation of sales activities while the system experiences downtime. For micro-scale businesses with daily cash turnover highly dependent on smooth transactions, system paralysis in just a matter of days can lead to total bankruptcy.

Beyond just material losses, the most destructive unseen impact in the long run is the destruction of brand reputation and the loss of customer trust. In the contemporary digital business ecosystem, consumer trust is the foundation that maintains market loyalty. If customers find out that their personal data (such as addresses, phone numbers, or transaction histories) leaked due to MSME system negligence, a negative stigma will immediately form. Restoring market reputation post-data leak requires time, energy, and marketing costs that far exceed the initial financial losses.

As a form of synthesis and recommendation, the literature emphasizes the need for a shift in cyber security mitigation approaches for MSMEs to focus more on behavior-based resilience. Given the budget constraints, MSMEs are not required to build corporate-level security architectures. Business actors are advised to focus on implementing basic cyber hygiene principles that are low-cost but highly effective. These tactical steps include routine operating system updates, activating built-in security features like 2FA across all platforms, and physically or virtually separating devices for personal entertainment and business operations.

Ultimately, the results of this literature review affirm that the cyber security challenges in the MSME sector are not merely technical infrastructure problems, but rather issues of managerial awareness and digital literacy. Massive

digital transformation must be balanced with a paradigm shift, where data security is no longer positioned as an optional addition (afterthought), but adopted as a vital operational culture. To realize a resilient digital economy ecosystem, strong synergy is needed between the government as policymakers, digital platform providers, and MSME actors themselves in sustainably increasing security literacy capacity.

CONCLUSIONS AND RECOMMENDATIONS

This literature review study has mapped the global literature evolution regarding cyber security threat trends in Micro, Small, and Medium Enterprises (MSMEs) in the digital era. Evaluations of various studies consistently confirm a surge in vulnerability directly proportional to the massive digital transformation in the small business sector. The scientific mapping in this domain is driven by three main thematic pillars: first, the identification of social engineering tactics (phishing) and data hostage software (ransomware) as the most dominant attack vectors; second, the confirmation that limited financial resources and minimal digital literacy of workers are the roots of system vulnerability; and third, the reality that operational paralysis and the destruction of business reputation due to data leaks are fatal threats to the organization's long-term resilience.

Although the urgency of data protection is increasingly recognized, the literature synthesis reveals that cyber security implementation at the MSME level is still faced with structural barriers. Capital limitations and the absence of dedicated Information Technology (IT) personnel make corporate-standard security architecture solutions (*enterprise*) irrelevant and unaffordable. Therefore, mitigation approaches must immediately shift from expensive hardware investments to tactical digital behavioral improvements. This study recommends MSME actors to rigorously adopt basic cyber hygiene principles, which include activating Two-Factor Authentication (2FA) across all platforms, separating work and personal devices, and establishing data backup routines isolated from the main business network.

Ultimately, the protection of cyberspace for the MSME sector can no longer be seen solely as the burden of individual business owners' responsibilities, but demands the presence of a holistic protection ecosystem. To build maximum cyber resilience, strategic synergy between technology practitioners and policymakers is highly recommended. Digital platform providers and security practitioners are required to develop intuitive, automatic, and low-cost (*plug-and-play*) security solutions specifically designed for MSME capacities. At the same time, the government needs to strengthen regulatory infrastructure and present massive data security literacy assistance programs to ensure this economic driving sector has adequate protective shields in facing future digital threat crises.

FURTHER RESEARCH

This literature review has several methodological limitations that need to be acknowledged academically. The process of extracting and collecting literature in this study was limited to open-access databases that were predetermined. This approach focusing on a single or limited database poses a

risk of excluding highly relevant scientific publications that may be indexed in other major databases. Additionally, screening criteria that restrict the review to journal articles with specific language criteria potentially ignore local cyber security mitigation case studies published in regional languages or alternative publication platforms.

To refine these findings, future research is recommended to expand the scope of literature searches across various multidisciplinary academic databases to capture a more comprehensive perspective. Researchers are also highly encouraged not to stop at the literature review stage, but to continue with empirical studies or field studies. Further research can be focused on detailed technical performance evaluations regarding the implementation of specific security algorithms or cyber mitigation frameworks when applied directly to MSME operational infrastructures. This methodological expansion is expected to produce digital security modules that are not only theoretically solid but also field-tested for reliability.

REFERENCES

Agit, A., Wildayanti, W., & Oktavianty, O. (2024). Efektivitas Penggunaan Transaksi Digital Dalam Menunjang Kinerja Bisnis. *JEMPER (Jurnal Ekonomi Manajemen Perbankan)*, *6*(2), 88–97. https://doi.org/10.32897/jemper.v6i2.3042

Eva Selvin Sura Tangkelangi, & Joy Nashar Utamajaya. (2024). Audit Sistem Informasi UMKM di Penajam Paser Utara Mengidentifikasi Kelemahan dan Meningkatkan Kepatuhan. *Saturnus : Jurnal Teknologi Dan Sistem Informasi*, *2*(3), 234–244. https://doi.org/10.61132/saturnus.v2i3.275

Karim, A., Umam, M. N., Fatahillah, M. L., & Hadi, Moh. A. F. (2024). the Identifikasi Kerentanan dan Upaya untuk Melindungi Data Pada Aplikasi Seluler. *JUSTIFY : Jurnal Sistem Informasi Ibrahimy*, *2*(2), 178–181. https://doi.org/10.35316/justify.v2i2.4159

Munawar, Z. (2018). KEAMANAN PADA E-COMMERCE USAHA KECIL DAN MENENGAH. *TEMATIK*, *5*(1), 1–16. https://doi.org/10.38204/tematik.v5i1.144

Octiva, C. S., Haes, P. E., Fajri, T. I., Eldo, H., & Hakim, M. L. (2024). Implementasi Teknologi Informasi pada UMKM: Tantangan dan Peluang. *Jurnal Minfo Polgan*, *13*(1), 815–821. https://doi.org/10.33395/jmp.v13i1.13823

Utami, Y., Riyanto Tri Wijaya, J., Wiyanti, S., & Murdiati, S. (2025). INTEGRASI PLATFORM ONLINE SHOP DAN DIGITAL FINANCE DALAM MENINGKATKAN KINERJA UMKM. *Jurnal Abdi Mandala*, *4*(2), 1–12. https://doi.org/10.52859/jam.v4i2.812

Yusnanto, T., Fatkhurrochman, F., Muin, M. A., & Waluyo, S. (2023). Pelatihan Dasar Keamanan Digital Untuk Mengurangi Pencurian Data Yang Berdampak Pada UMKM. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(9), 2022–

2029. https://doi.org/10.59837/jpmba.v1i9.458

Zulkarnain, Z., & Sutabri, T. (2023). ANALISIS KEJAHATAN CARDING PADA BNI 46. *Blantika: Multidisciplinary Journal*, *1*(2), 33–43. https://doi.org/10.57096/blantika.v1i2.10