Journal of Information Systems and Informatics
Vol. 7, No. 3, September 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i3.1248 Published By DRPM-UBD

Building Digital Trust in Jakarta's Micro and Small Enterprises: From Awareness to Adaptation

Marcel[1*], Katherin Monica[2]

[12]Information System Department, Krida Wacana Christian University, Jakarta, Indonesia
[12]Sustainable Eco-Smart Digital Infrastructure Center (SESDIC)
Email: [1]marcel@ukrida.ac.id, [2]katherin.422023011@civitas.ukrida.ac.id

Abstract

Digital transformation opens many opportunities for micro, small, and medium enterprises (MSMEs) while also creating new challenges in security and trust. This study examines how MSMEs in Jakarta build digital trust through basic information security practices using a mixed-method approach. A survey involving 30 MSMEs showed that 70 percent of respondents understood the importance of strong passwords and 80 percent were aware of phishing risks. However, only 40 percent used two-factor authentication and 20 percent followed formal security guidelines. Interviews with ten business owners revealed that awareness often develops after personal experiences with fraud, while adaptive strategies such as self-learning, small internal training sessions, and the use of built-in security tools help them cope with limited knowledge and resources. The integration of quantitative and qualitative findings resulted in a conceptual model of incremental digital trust adaptation that progresses through awareness, practical adaptation, and gradual governance. Theoretically, the model explains digital trust as a continuous and context-based process within MSMEs. Practically, it provides guidance for governments, business associations, and digital platforms in creating simple, scalable, and realistic programs to strengthen the digital resilience of small enterprises.

Keywords: Digital trust, Cybersecurity awareness, Conceptual Model, Micro and small enterprises (MSMEs), Adaptive strategies

1. INTRODUCTION

Digital transformation has opened vast opportunities for micro, small, and medium enterprises (MSMEs) in Indonesia, from expanding market reach to improving operational efficiency. Yet, this rapid connectivity also introduces new challenges, especially in ensuring security and maintaining digital trust. The ISACA report [1] reveals that many organizations remain uncertain about their level of digital trust, while Thales [2] identifies trust as a decisive factor influencing consumer loyalty. Similarly, Arroyabe, Arranz, De Arroyabe, and De Arroyabe [3] emphasize that cybersecurity holds not only technical value but also significant economic importance for small enterprises. Moreover, consumer behavior studies

show that users are quick to abandon transactions when their personal data feels insecure [4]. These findings indicate that establishing digital trust is not merely a trend but an essential foundation for MSMEs striving to survive and grow in the digital marketplace.

Previous studies have examined digital transformation within large corporations that possess robust infrastructure and specialized IT divisions, the realities for MSMEs are markedly different. Research by Wardana and Suryani [5] and Slamet, Ikhlash, and Wulandari [6] demonstrates that only a small portion of MSMEs can meet the minimum information security standards defined by the national Information Security Self-Assessment (PAMAN KAMI) framework. Other studies [7], [8] confirm that MSME owners' awareness of digital security remains low, hindered by limited literacy, financial resources, and access to experts. Saeed, Altamimi, Alkayyal, Alshehri, and Alabbad [9] further warn that digital transformation in any business sector will inevitably bring security risks that, if unmanaged, may weaken resilience. Despite various government initiatives, ranging from regulatory frameworks to capacity-building workshops [10], [11], [12], [13], implementation at the MSME level remains inconsistent. Many small businesses struggle to sustain even the most basic protection measures, suggesting deeper structural and behavioral challenges that must be explored in context.

This gap is amplified by the limited research capturing the lived experiences of MSMEs in developing countries like Indonesia. Most global cybersecurity frameworks, such as the European SME cybersecurity guidelines [14] or the governance adaptation model from Portugal [15], were designed for environments with higher digital maturity and may not align with the everyday constraints of Indonesian MSMEs. Purnomo, Nurmalitasari, and Nurchim [16] highlight that digitalization among local MSMEs still faces significant obstacles, from uneven digital literacy to low technological readiness. Given these conditions, MSMEs urgently require a digital trust model that is simple, affordable, and aligned with their real-world capabilities.

This study aims to understand how Indonesian MSMEs cultivate digital trust through basic information security practices. It uses a mixed-method approach that combines descriptive quantitative surveys to map the level of awareness and compliance with qualitative interviews that explore the experiences and adaptive strategies of business owners. By integrating these two perspectives, the study develops a contextual and practical conceptual model of digital trust that reflects the real conditions faced by MSMEs rather than the assumptions of large corporations. The novelty of this research lies in its integration of descriptive data and qualitative insights to build a grounded framework that can serve as a practical reference for MSMEs, policymakers, and digital platform providers in designing realistic and scalable security interventions. In the long term, this study contributes

theoretically by enriching the discussion on digital trust with a contextual understanding of MSMEs and practically by offering actionable strategies that can help small businesses enhance their competitiveness in Indonesia's growing digital economy. The following are research questions that are the scope of this paper:

1) How do Indonesian MSMEs build digital trust through their everyday information security practices?
2) How can their experiences and adaptive responses be transformed into a model that reflects the practical realities of MSMEs?

2. METHODS

This study uses a mixed-method approach with a descriptive orientation. The main objective of the study is to gain a more comprehensive understanding of how MSMEs build digital trust. Quantitative data is used to provide an overview of the level of awareness and compliance of business actors with information security practices. Meanwhile, qualitative data provides a deeper understanding of their perceptions, experiences, and adaptive strategies.

The research focused on MSMEs operating in the Jakarta area, especially small home-based businesses that actively utilize digital channels, either fully or semi-online. Jakarta was chosen because it is the center of digital economic activity with a large number of MSME players, particularly in the culinary, fashion, and creative services sectors. Given these conditions, Jakarta is a relevant representation for observing the dynamics of digital trust among MSMEs.

In this study, 30 MSMEs took part in the quantitative survey. The participants were chosen purposively with several conditions: their businesses had been running for at least a year, they actively used digital platforms to carry out transactions, and the owners were directly engaged in managing daily operations. From this group, 10 business owners were later invited for in-depth interviews. The selection was made to represent different types of sectors and business scales, ensuring that the findings reflected a broader and more varied perspective.

The total of 30 MSME respondents was considered adequate for a descriptive exploratory study aimed at mapping basic awareness and compliance patterns rather than producing inferential generalizations. This size aligns with previous small-scale MSME studies on information security [6], [7], [8], which also involved limited samples to explore awareness and adaptation patterns in practical contexts. Meanwhile, 10 interview participants were sufficient to reach data saturation, as repetitive themes began to appear after the eighth interview.

A purposive sampling strategy was used to ensure that the selected MSMEs represented sectors that are both digitally active and highly exposed to online

transactions, namely culinary, fashion, and creative services. These sectors were chosen because they dominate the digital MSME landscape in Jakarta and involve frequent online interactions with customers. In practice, several additional respondents from handicrafts and other small service sectors were also included, as they met the same selection criteria and actively conducted online transactions.

2.1. Data Collection

In gathering the data, two instruments were used. One of them was a questionnaire that covered three areas: the general profile of the business, the extent of the owner's awareness of digital security, and their habits in following security practices. The questionnaire itself was not taken directly from existing templates but was developed by referring to the Information Security Self-Assessment Framework (PAMAN KAMI) from BSSN, and then adjusted to better match the realities faced by MSMEs. To ensure responses were more representative, the survey was distributed in both online format and through direct visits, so that owners who were less active digitally could still take part.

The second part of data collection was carried out through interviews with ten business owners. In these sessions, the conversations revolved around their daily encounters with digital risks, how they judged the seriousness of potential threats, and the kinds of steps they usually took to keep their businesses safe. Each interview lasted about 45 to 60 minutes. This format gave the owners enough space to share stories and reflections, while also allowing the researcher to observe how MSMEs adjust and develop their own ways of dealing with challenges in the digital sphere.

2.2. Data Analysis

The survey results were processed using descriptive statistics. Simple calculations of frequency and percentage were considered sufficient to map the main tendencies in the data. The outcomes were then arranged in several tables (Tables 2–6), which present the background of the respondents together with their level of awareness and the way they complied with information security practices.

The interview material was handled differently. Each transcript was read several times to capture important points and nuances. Passages that stood out were marked, coded, and gradually brought together into broader categories. From these categories, themes were developed to describe common patterns that appeared across the accounts of business owners.

Through this step-by-step reading, four themes emerged with some consistency. Many respondents showed only limited awareness of digital security, while a

number of obstacles and resource constraints held them back from improving. In several cases, specific incidents became eye-openers that pushed owners to act. Alongside these challenges, there was also a strong call for practical and adaptive solutions. A summary of these themes is provided in Table 7.

This study was limited to MSMEs operating within the Jakarta area and used a cross-sectional design. Therefore, the results represent a contextual snapshot of MSME conditions at the time of data collection and may not fully capture longitudinal changes or regional variations across Indonesia. In general, the research steps can be described as follows in Table 1.

Table 1. Research Methodology Flow.

Research Stage	Main Activities	Output / Results
Instrument Design	Developing survey questionnaires and interview guides based on PAMAN KAMI and related literature	Validated survey instrument and interview guide
Respondent Recruitment	Engaging Jakarta SMEs through business communities, associations, and local networks	30 survey respondents and 10 interview participants selected
Quantitative Data Collection	Conducting surveys on business profiles, awareness, and compliance with information security	Quantitative dataset (profile, awareness, compliance)
Qualitative Data Collection	Semi-structured interviews (45–60 minutes) with SME owners	Interview transcripts capturing perceptions, experiences, and adaptive strategies
Quantitative Data Analysis	Descriptive statistics: frequency, percentage, and tabulation	Tables 2–6 (profile, awareness, compliance)
Qualitative Data Analysis	Manual thematic analysis: reading, coding, categorizing, identifying themes	Tables 7–8 (perceptions & adaptive strategies)
Synthesis of Findings	Integrating quantitative and qualitative data	Conceptual model of adaptive digital trust for SMEs (Table 9)
Discussion & Implications	Linking findings to global literature and formulating practical recommendations	Discussion and interpretation, theoretical and practical implications

Figure 1 presents the sequential stages of the research process, which include instrument design, respondent recruitment, data collection and analysis for both quantitative and qualitative phases, synthesis of findings, and formulation of discussion and implications.

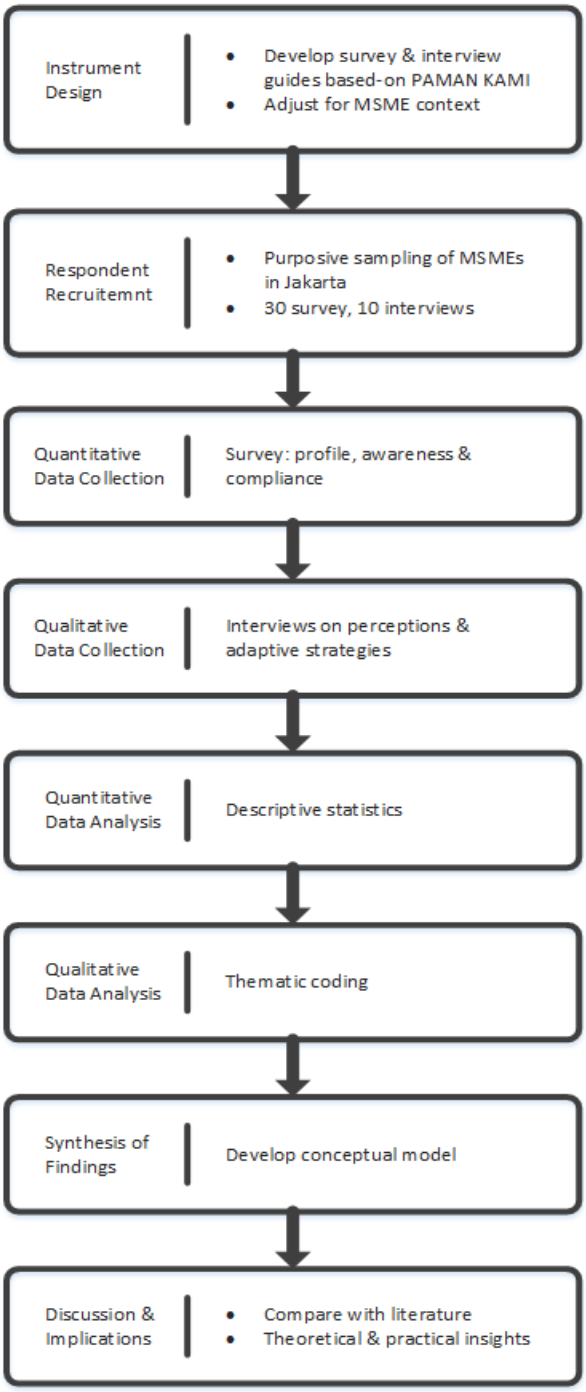

Figure 1. Research steps.

3. RESULTS AND DISCUSSION

3.1. Profile of MSME Respondents

This study involved 30 local MSMEs in the Jakarta area engaged in the culinary, fashion, creative services, handicrafts, and other businesses (Table 2, Figure 2). Respondents were selected using purposive sampling based on the main criteria: businesses actively using digital channels in their operations, either fully or semi-online, and the majority still operating on a home-based scale (Tables 3 and 4, Figure 3 and 4). This description provides important context about the real conditions of MSMEs, which are the backbone of the local economy but are also vulnerable to digital security issues. These findings are in line with the study by Tambunan and Busnetti [17], which shows that digitalization in MSMEs in Indonesia is indeed progressing rapidly, especially in sectors with broad market access, but also leaves gaps in infrastructure readiness and literacy.

Table 2. Types of Business Among Respondents.

Type of Business	Number	Percentage (%)
Culinary	12	40.0
Fashion	7	23.3
Creative Services	5	16.7
Handicrafts	3	10.0
Others	3	10.0

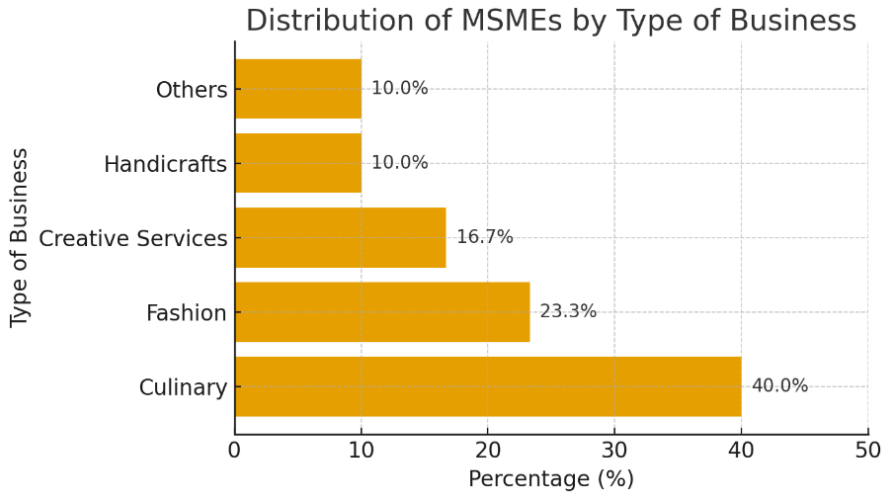

Figure 2. Types of Business Among Respondents (Bar chart).

1) Fully online MSMEs: all sales take place on digital platforms such as marketplaces, social media, or websites. These businesses seldom maintain physical outlets and depend heavily on electronic payments and delivery services.
2) Semi-online MSMEs: businesses still run through physical outlets or small workshops, yet part of their sales is handled online, often via WhatsApp, Instagram, or marketplaces. This model is widespread in Jakarta where internet access and digital tools are easily available.
3) Home-based MSMEs: small ventures operated from home with limited capital and family or local labor support. Despite their size, they actively use digital platforms to reach wider markets.

Most respondents in this study turned out to be working in culinary and fashion. This outcome is actually consistent with national findings from the Ministry of Cooperatives and SMEs, which note that both sectors have been quick to move into digital channels for selling products [5].

Table 3. Years in Operation.

Years in Operation	Number	Percentage (%)
Less than 2 years	8	26.7
2–5 years	14	46.7
More than 5 years	8	26.7

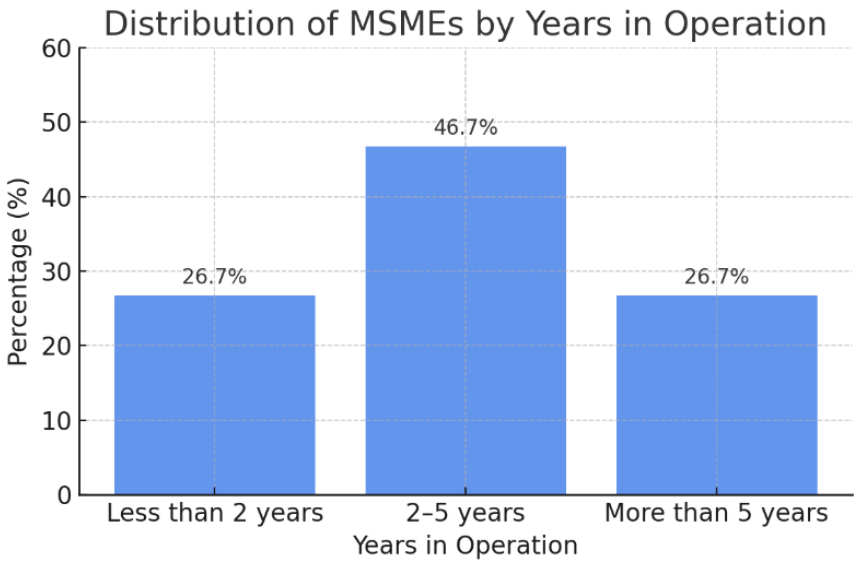

Figure 3. Years in Operation (Bar chart).

Almost half of the respondents had been operating their businesses for about two to five years. This indicates that many MSMEs are still navigating the early phase of growth, where efforts are directed mainly toward sustaining operations and reaching wider markets. At such a stage, digital security rarely becomes the main concern. Owners usually place greater attention on activities related to sales, marketing, and production. A similar pattern was reported by Suartana et al. [8], who found that MSMEs often postpone adopting formal security practices during the formative years of their business.

Table 4. Number of Employees.

Number of Employees	Number	Percentage (%)
1–5 people (micro)	18	60.0
6–19 people (small)	10	33.3
20–99 people (medium)	2	6.7

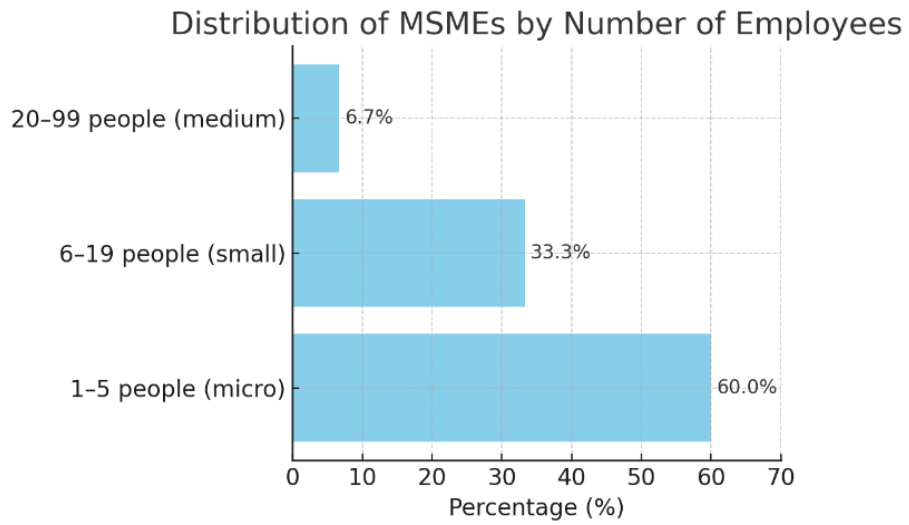

Figure 4. Number of Employees (Bar chart).

Most of the MSMEs in this study were micro businesses employing only one to five people. Such a small workforce is common in Jakarta, where business owners usually juggle multiple responsibilities at once, ranging from production and marketing to managing digital transactions. Under these circumstances, digital security often receives little attention because there are no staff members dedicated to this function. Similar observations were reported by Slamet et al. [6], who noted that limited human resource capacity remains one of the main reasons why security standards are rarely implemented among MSMEs in Indonesia.

The respondents did not only differ by sector, age, or size of their workforce, but also in the way they carried out daily operations. A number of businesses had shifted completely online, selling only through marketplaces, social media, or websites. Others still kept a physical presence such as a kiosk or small workshop while also using digital platforms for part of their sales. There were also many small ventures run from home with very modest resources and help from family members, yet these enterprises were surprisingly active in using online channels to reach customers outside their immediate neighborhood.

From the profile of respondents, several important points can be noted. MSMEs in Jakarta appear eager and relatively quick in taking advantage of digital platforms, yet this speed is not matched by adequate resources, leaving many of them vulnerable to security risks. The data also show that a large share of the businesses are micro-scale and home-based. This suggests that digital trust cannot be fostered only through the enforcement of formal rules. It needs to grow through approaches that fit the everyday realities of small enterprises. Keeping this in mind provides a clearer background for the next section, which explores the awareness, compliance, and experiences of business owners.

3.2. Level of Information Security Awareness

MSME players' awareness of information security is a key factor in building digital trust. Although the majority of respondents already use digital platforms for daily transactions, their understanding of security varies. Survey data shows a gap between basic knowledge and the application of technical practices (Table 5, Figure 5).

Table 5. Level of Security Awareness Among SMEs.

Awareness Aspect	Yes (%)	No (%)
Use of unique and strong passwords	70	30
Activation of two-factor authentication	40	60
Regularly updating applications/platforms	65	35
Awareness of phishing and online scams	80	20
Participation in cybersecurity training	25	75

The results of the study show that most respondents already have a basic awareness of the importance of strong passwords (70%) and vigilance against phishing (80%). The high level of vigilance against phishing is reasonable, as this threat is often experienced firsthand by businesses that conduct transactions through social media and marketplaces. However, awareness of more advanced technical security practices, such as the use of two-factor authentication (40%) or participation in digital security training (25%), remains low.

This shows that MSMEs tend to prioritize security measures that are easy to understand and directly related to everyday experiences, while technical aspects that require more in-depth understanding or additional learning time are still rarely implemented.

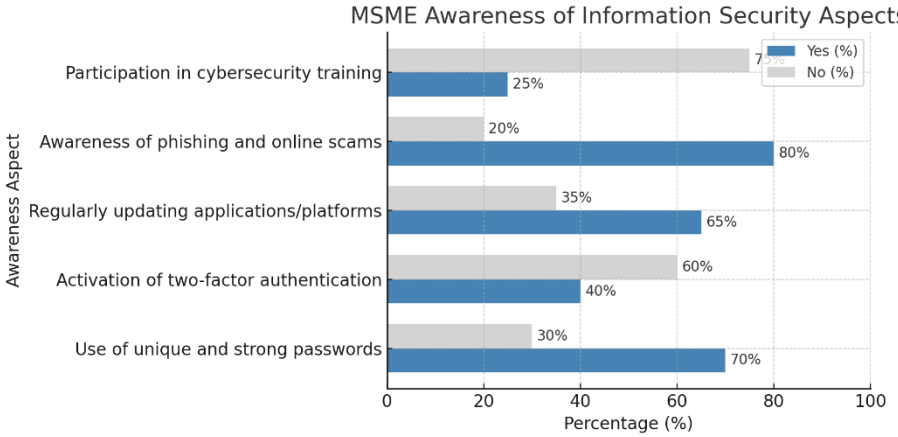

Figure 5. Level of Security Awareness Among SMEs (Bar chart).

The results of this study are consistent with the work of Ajhari, Manaon, and Dimas [7], who observed that MSMEs generally recognize only broad information security threats, while overlooking more technical measures such as multi-factor authentication. Similarly, research by Suartana et al. [8] points out that formal awareness of digital security among Indonesian MSMEs remains low, largely because digital literacy and education have not been evenly distributed. In another study, Nugraha, Setiawan, Nathan, and Fekete-Farkas [18] emphasize that decisions to adopt digital innovation are shaped not only by technical capacity but also by business owners' perceptions of tangible benefits, ease of use, and the sense of security in conducting transactions.

In a global context, this pattern is similar to the findings of Papathanasiou et al. [14], which confirm that small businesses are more sensitive to the practical threats they experience directly, compared to formal security protocols that are considered complicated. In other words, SME awareness tends to be reactive, only strengthening when there is direct experience or real cases.

This partial awareness indicates that there is fundamental potential that can be developed. MSME players already understand certain risks, but they need a more practical and relevant educational approach. Efforts to build digital trust for MSMEs are not enough to simply introduce technical concepts, but must be accompanied by communication strategies that are simple, based on real cases, and

tailored to their capacities. If this aspect is not addressed, the gap between awareness and implementation will continue to exist, leaving the potential for security risks high.

3.3. Compliance with Security Practices

In addition to awareness, compliance is an important indicator in assessing the extent to which MSMEs actually implement information security practices in their daily activities. Survey data shows that most MSMEs still rely on simple practices, while the implementation of formal standards is relatively minimal. The survey results show that relatively easy practices, such as using legal antivirus software (55%) or performing regular data backups (45%), tend to be more widely implemented by MSMEs. However, more systematic and formal practices, such as following the PAMAN KAMI guidelines (20%) or having internal digital security SOPs (25%), are still rarely implemented. The separation of personal and business devices is also not yet common (40%), indicating that the majority of business owners still mix personal needs with business operations (Table 6, Figure 6).

Table 6. SME Compliance with Information Security Practices.

Security Practice	Yes (%)	No (%)
Performing regular data backups	45	55
Using licensed/legitimate antivirus software	55	45
Separating personal and business devices	40	60
Following the PAMAN KAMI guidelines (BSSN)	20	80
Having a simple internal SOP for cybersecurity	25	75

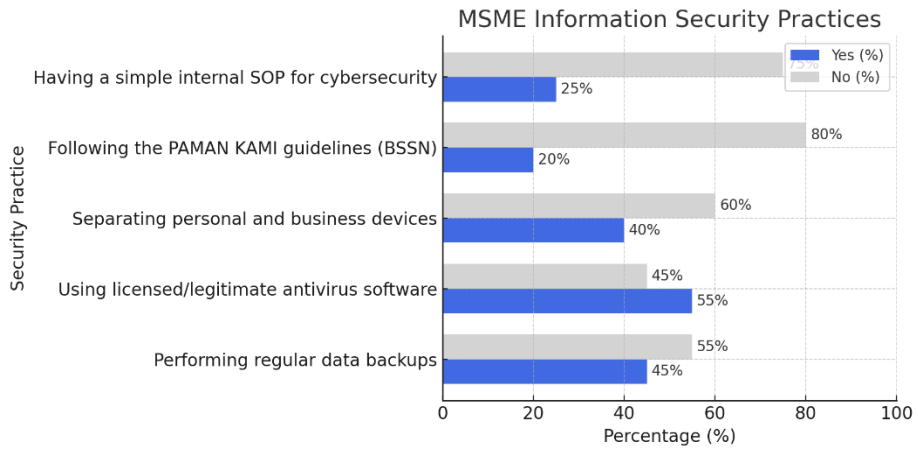

Figure 6. SME Compliance with Information Security Practices (Bar chart).

This situation reflects that most MSMEs choose security measures that are practical, quick, and do not add to their financial burden, while formal standards are considered complicated and difficult to implement. This phenomenon of low compliance is consistent with the research by Slamet, Ikhlash, and Wulandari [6], which found that only a small proportion of MSMEs were able to meet minimum security standards through the PAMAN KAMI instrument. Wardana and Suryani [5] also confirm that most MSMEs find it difficult to maintain consistency in the implementation of security regulations, either due to limited resources or low priority given to security issues. In the global literature, Bottarelli et al. [19] highlight that security standards designed for large organizations are often difficult for small businesses to adapt, so their compliance is more dependent on simple solutions that are relevant to their internal capacity. This shows a gap between top-down imposed security models and the operational reality in the field.

Low compliance with formal standards indicates that security strategies for MSMEs cannot rely solely on uniform regulations. A more flexible, simple, and affordable approach is needed so that MSMEs can internalize security practices without feeling burdened. This is in line with the efforts of BSSN [10], [11], which has begun to develop capacity-based coaching programs, although their implementation still needs to be expanded. By understanding these compliance patterns, it can be concluded that building digital trust in MSMEs must begin with simple, familiar practices, then gradually move towards more systematic standards. This gradual approach will be more realistic in encouraging compliance, while reducing the digital risks that threaten the sustainability of small businesses.

3.4. Perceptions and Experiences of MSME Players

Qualitative analysis through in-depth interviews produced findings that enriched the survey data. MSME players in Jakarta are aware of the importance of digital security, but the actual practices they implement are still simple and tend to be limited to practical steps that can be taken without additional costs. One of the owners of an online culinary business explained: "I understand that data security matters, but in practice all I can do is rely on passwords and change them from time to time. I don't have the resources to invest in special systems or applications. Most of my attention goes to boosting sales and serving customers."

The response shows that digital security has not yet been placed at the center of business priorities. What matters most for many owners is keeping the business alive from day to day. Cash flow must keep moving, orders have to be delivered, and customers need attention. Under such pressure, putting money or effort into security, something that rarely gives instant results, naturally falls behind other concerns. In another case, the owner of a semi-online fashion business shared their experience with the risk of fraudulent transactions: "I was almost scammed once

by a fake buyer who used a fake transfer receipt. Luckily, I double-checked with the bank. After that, I became more vigilant, but I'm still confused about how to stay safe."

This quote illustrates that bad experiences are an important trigger for increased security awareness. However, limited technical knowledge means that businesses are still confused about what preventive measures to take next. A home-based creative services entrepreneur mentioned: "I do want training, especially the short ones. But, you know, most of them are too technical, too complicated. I end up not understanding much. What we need is training that's simple, straight to the point, and can actually help us in our work right away."

What emerges here is the need for training that speaks the language of small business owners. Complex technical concepts rarely stick, while practical tips that fit daily routines are much easier for them to adopt and sustain. Based on the manual coding process, four main themes were identified (Table 7).

Table 7. Summary of Thematic Analysis of SME Perceptions.

Main Theme	Sub-Codes	Example Quote
Awareness exists but limited	"Strong password," "App updates"	"I know the importance of data security, but I only rely on changing passwords."
Constraints and limitations	"High costs," "Operational focus"	"Honestly, I can't afford it yet, my focus is still on sales."
Experience as a trigger	"Fraud," "Fake transfers"	"I almost fell for a scam once, luckily I double-checked with the bank."
Need for adaptive solutions	"Practical guidance," "Simple training"	"If there were short, easy-to-understand trainings, I'd definitely join."

These results reinforce previous quantitative data showing that although 70% of respondents already use strong passwords and 80% are aware of the risks of digital fraud, compliance with systematic practices such as following the PAMAN KAMI guidelines is still very low (20%). This gap can be explained by two factors: limited resources and low access to guidelines that are truly tailored to the needs of MSMEs. Conceptually, this pattern is consistent with global findings. A study by Papathanasiou et al. [14] emphasizes that MSMEs tend to need simpler, tailored guidelines compared to the standard guidelines commonly used by corporations. Azinheira et al. [15] also highlight the importance of remapping security standards so that they can be applied to small businesses with limited capacity. In Indonesia, this context is even more relevant given that the majority of MSMEs still operate from home or semi-online, with owners wearing many hats.

3.5. Adaptive Strategies and Practices Implemented by MSMEs

Despite resource constraints being a major obstacle, some MSMEs in Jakarta continue to show adaptive initiatives in facing digital risks. The strategies they implement tend to be simple, accessible, and in line with their capacities. The interview results show several consistent patterns. First, some business owners choose to educate themselves by utilizing open sources on the internet, such as digital security articles, YouTube tutorials, or short webinars. An owner of a semi-online fashion business said: "If I have a problem or am confused, I usually search on YouTube or read online articles. From there, I learn small things, such as how to identify fake emails or how to change passwords more securely". Second, some respondents conduct internal training within their small businesses. These practices are simple, such as teaching employees not to open suspicious links or to always double-check transfer receipts before sending goods. Third, many MSMEs lean on no-cost security options that come with the tools they already use. Free antivirus programs, marketplace protections, and one-time password (OTP) authentication are common choices, mainly because they do not add financial pressure yet still offer a layer of safety. As a culinary entrepreneur explained: "I don't spend on special software. I just make use of the marketplace's security features. With payment protection already provided, I feel safer."

From the business side, such adaptive strategies are viewed as sufficient for day-to-day operations. Learning on their own helps owners build awareness, even though their knowledge often remains basic. Short and simple training inside the business is useful to avoid common mistakes, while security features already embedded in applications give them extra confidence when carrying out transactions. However, some respondents also recognize its limitations. This strategy does not fully protect against more complex attacks, such as account hacking or digital identity theft. In other words, the effectiveness of the adaptive strategy lies more in basic prevention rather than comprehensive protection (Table 8).

Table 8. Adaptive Strategies Adopted by SMEs.

Strategy Type	Example from Respondents	Perceived Effectiveness
Self-zlearning (online resources)	Learning from YouTube tutorials or online articles on detecting phishing and password management.	Increases basic awareness but limited in depth.
Internal informal training	Owners reminding staff to double-check transfer receipts or avoid suspicious links.	Effective in preventing simple mistakes.
Free security applications	Using free antivirus, OTP features, or built-in protections from e-commerce platforms.	Provides reassurance for daily transactions but limited against advanced threats.

This adaptive practice of MSMEs in Jakarta is relevant to the findings of Papathanasiou et al. [14], which emphasize the importance of providing simple and practical guidance for small businesses. Similar to Europe, MSMEs in Indonesia find it easier to adopt strategies that can be implemented immediately without significant investment. Azinheira et al. [15] also emphasized that mapping security standards into simple governance guidelines is key to enabling small businesses to improve their digital resilience. These findings are also in line with Benjamin, Adegbola, Amajuoyi, Adegbola, and Adeusi [20], who emphasize that cyber risks in MSMEs can be minimized through practical and capacity-appropriate mitigation strategies, rather than through complex standards. Furthermore, Sudirman, Astuty, and Aryanto [21] assert that the successful adoption of digital technology in MSMEs is greatly influenced by sustainable resilience strategies and entrepreneurial orientation, which in turn strengthen the ability to adapt to digital risks.

3.6. Conceptual Model of Digital Trust Adaptation for MSMEs

The synthesis of quantitative and qualitative findings reveals a clear connection between what MSMEs know and what they actually do. The survey data show that awareness of basic digital security practices is relatively high, while compliance remains low. The interviews then explain why this gap exists, highlighting cost limitations, lack of expertise, and the dominance of informal learning. When combined, these two perspectives demonstrate that MSMEs' digital trust is not merely a function of technical knowledge but an outcome of continuous adaptation shaped by real experiences. This integrated view serves as the foundation of the proposed conceptual model.

The quantitative and qualitative findings in this study lead to one main conclusion: MSMEs in Jakarta have a basic awareness of digital security, but the implementation of security practices is still low and sporadic. High awareness of directly experienced threats (e.g., phishing and fraud) does not automatically correlate with compliance with formal standards such as PAMAN KAMI. This is reinforced by in-depth interviews showing that bad experiences are often the main trigger for awareness, while resource constraints mean that MSMEs are only able to adopt simple adaptive strategies.

The conceptual model developed in this study seeks to explain how digital trust takes shape within MSMEs through adaptive behaviors that grow from real experiences and limitations. Instead of acting as a rigid framework, the model serves as a way to understand the ongoing connection between awareness, practical adaptation, and governance. Its main goal is to help researchers and practitioners grasp how digital trust evolves step by step within small enterprises.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Based on data synthesis, the conceptual model offered in this study emphasizes three main pillars of digital trust adaptation in MSMEs:

1) Awareness Foundation: Basic awareness born from real experiences (e.g., having been scammed) or self-learning is the gateway to implementing security practices. Survey data supports this, with 80% of respondents stating that they understand the risks of phishing, even though only 40% use two-factor authentication.
2) Practical Adaptation: Because of limited resources, most security efforts are carried out through simple actions such as making manual backups (45%), using free antivirus programs (55%), or applying informal internal procedures (25%). This finding supports the qualitative theme identified in the analysis, which highlights the "need for adaptive solutions."
3) Incremental Governance: This model explains that building digital trust is not something that happens all at once. Small businesses usually begin with simple habits, then move little by little toward more structured management. The process often starts when owners join short awareness sessions, learn through practice, and gradually prepare themselves to use formal tools like PAMAN KAMI. The focus is on progress that feels natural and realistic, not on forcing instant compliance with complex standards.

This study introduces a model that looks at how small businesses begin to build readiness before they can fully meet formal standards like PAMAN KAMI [10]. PAMAN KAMI is useful for assessing information security levels, but it works best for organizations that already have stable systems and enough technical knowledge. Many micro and small enterprises are still developing that capacity. The model described here shows how readiness can grow from simple awareness, everyday habits, and gradual improvements in management. It helps connect the real situations faced by MSMEs with the formal standards promoted by BSSN, creating a smoother and more realistic path toward stronger information security practices.

The Proposed Conceptual Model (Table 9 and Figure 7) consists of:

1) Input: MSME profile (micro, home-based, semi-online), partial awareness (Table 5), low compliance (Table 6).
2) Adaptation Process:
   a) Awareness is formed from direct experience (reactive awareness).
   b) Barriers include financial, technical, and human resource limitations.
   c) Simple adaptive strategies are implemented (Table 8).
3) Output: A phased model towards digital trust, based on practical, adaptive, and affordable solutions.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 9. Conceptual Model of Adaptive Digital Trust for SMEs.

Dimension	Key Elements	Description
Input	SME profile, partial awareness, low compliance	Most SMEs are micro-scale, operate semi-online, and have basic awareness but limited practice
Adaptive Process	Awareness from direct experiences, resource constraints, simple adaptive strategies	Trust-building emerges reactively from incidents (e.g., fraud), limited by financial/technical capacity, and supported by practical steps such as free apps or informal training
Output	Incremental digital trust	Digital trust is developed gradually, starting from basic practices toward more formal governance models

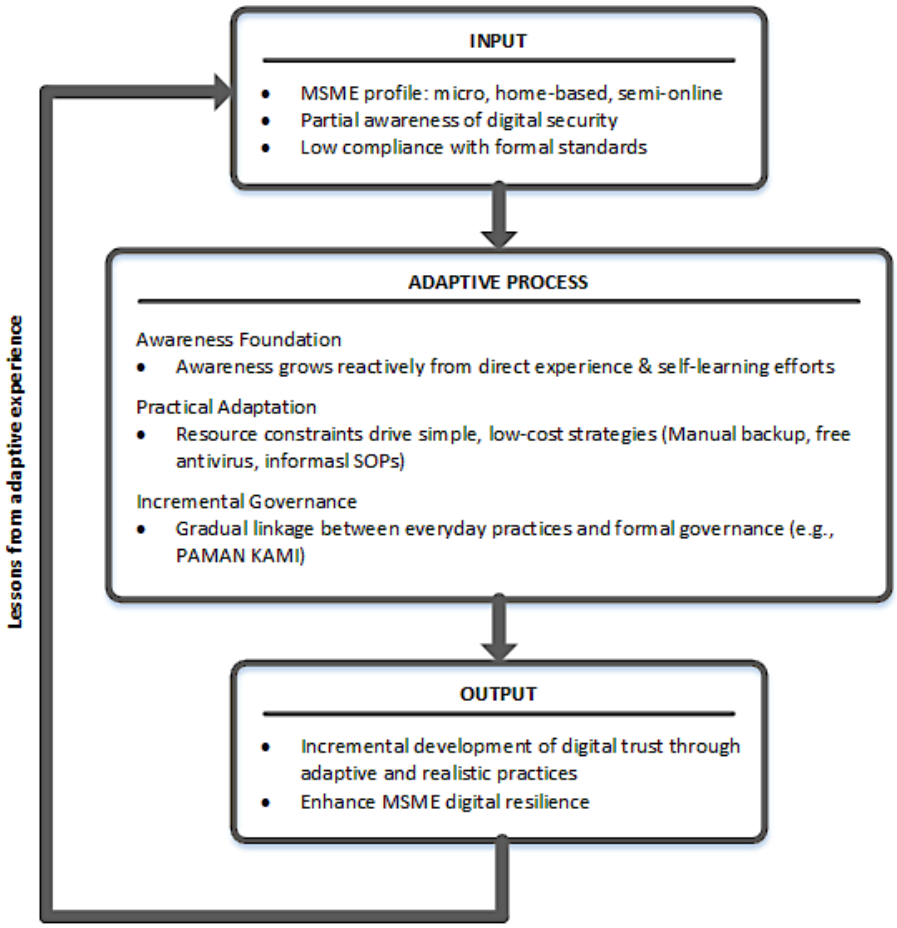

Figure 7. Conceptual Model of Adaptive Digital Trust for SMEs.

This model is in line with Papathanasiou et al. [14], who emphasize that small businesses need simpler, tailored guidelines compared to corporate standards. Azinheira et al. [15] similarly assert that the success of MSMEs in building digital resilience depends on remapping security standards to suit their capacities. Furthermore, Metin, Özhan, and Wynn [22] emphasize the need for an operational framework that integrates digitization with applicable security practices, so that strategies are not only conceptual but can also be applied in practice on a small business scale. Kahveci [23] also underlines that the digital transformation of MSMEs needs to be understood within the framework of enablers and interconnections that support sustainable competitive advantage, so that the digital trust adaptation model not only addresses protection needs but also strengthens long-term competitiveness.

The adaptation model presented in this study highlights not only the challenges faced by MSMEs but also the gradual and systematic way in which digital trust can be developed. Theoretically, the model introduces the idea of adaptive logic, showing that digital trust among MSMEs grows step by step rather than through immediate adoption. From a practical perspective, this model can guide governments and related institutions in creating more inclusive digital security programs through case-based training, practical guidelines, and the use of accessible built-in applications that support everyday business activities.

3.7. Theoretical and Practical Implications

This study shows that digital trust in MSMEs is not formed instantly through formal standards, but develops gradually through basic awareness, adaptive strategies, and simple practices. From an academic perspective, this enriches the literature by emphasizing that digital security in the small sector is more social and contextual in nature, rather than merely technical. These findings are also in line with the dynamic capability perspective offered by Saeedikiya, Salunke, and Kowalkiewicz [24], [25], where the ability of MSMEs to continuously adapt to technological changes is an important foundation for their digital transformation. Thus, this study adds a new dimension to the literature on digital trust, namely that social factors, real-world experience, and gradual adaptation are as important as technical aspects in strengthening the competitiveness of small businesses. Table 10 explains the theoretical and practical implications of this study.

Table 10. Theoretical and Practical Implications.

Dimension	Key Implications
Theoretical	- Enriches digital trust studies with a contextual model for SMEs.
	- Highlights security as both a social and managerial process, not only technical.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Dimension	Key Implications
Practical	- Training should be case-based and easy to digest.
	- Guidelines need to be modular: start simple, then move to formal standards.
	- Collaboration with digital platforms to offer affordable, SME-friendly security features.

The adaptive strategies identified in this study, including self-learning, informal internal training, and the use of built-in security features, can be scaled and formalized through gradual integration into MSME development programs. Local business associations and government agencies may transform these informal practices into short and modular training sessions as well as simple digital trust checklists that reflect the stages of awareness, adaptation, and governance described in the conceptual model. Over time, these scalable initiatives can be aligned with formal frameworks such as PAMAN KAMI, enabling MSMEs to institutionalize security practices while maintaining flexibility in accordance with their available resources and operational capacity.

From a practical standpoint, these findings encourage the creation of more inclusive interventions, ranging from practical training and modular guidelines to digital platform support that is friendly to MSMEs. Governments, business associations, and digital service providers can use this adaptation model as a reference for designing strategies that are relevant to the capacity of MSME actors. This approach not only strengthens basic protection from digital threats, but also provides space for MSMEs to build long-term resilience through simple, gradual, and affordable strategies.

3.8. Discussion

The study reveals that digital trust among MSMEs does not form instantly or merely through the adoption of formal information security frameworks. Instead, it evolves gradually through everyday experiences and ongoing adaptation. Many MSME owners already understand basic principles of digital safety, such as using strong passwords or avoiding suspicious links, but their actual practices often remain simple and inexpensive. This difference between knowledge and action shows that digital trust is not only a technical matter. It grows through experience, reflection, and the ability to turn awareness into small, consistent habits that suit their limited resources. Therefore, digital trust among MSMEs can be seen as a social process that matures over time.

Integrating the quantitative and qualitative results offers a clearer picture of how this process unfolds. Survey data indicate that while awareness of information

security is fairly high, compliance with formal standards remains limited. Interviews help explain this gap. Many business owners understand the importance of digital security but are constrained by cost, time, and a lack of expertise. When formal training feels too technical or expensive, they often seek alternatives by learning independently online, reminding each other within small teams, or relying on built-in protection features from digital platforms. These adaptive behaviors demonstrate how MSMEs respond creatively to their conditions and how digital trust can grow from practical, grounded actions rather than formal structures.

A key insight from this research is that adaptation itself serves as a foundation for resilience. Instead of describing MSMEs as lagging behind large companies, the findings reveal that many are already building trust through small and consistent efforts. These informal actions, such as independent learning, cautious communication, and basic verification of transactions, help reduce daily risks and maintain customer confidence. More importantly, they represent the initial stage of readiness for more formal security frameworks. Recognizing and supporting these early efforts can therefore become a practical entry point for strengthening MSME cybersecurity capacity.

The conceptual model developed in this study describes this gradual process of development. It is based on three interrelated pillars: awareness, adaptation, and governance. Awareness is often triggered by direct experiences, such as encountering online fraud or phishing. Adaptation follows when owners start implementing practical and affordable solutions to avoid similar problems. Over time, these small steps evolve into simple governance mechanisms, such as internal guidelines or checklists that reflect more formal structures. This progressive path provides a realistic description of how digital trust can emerge and mature in small businesses that operate with limited technical and financial capacity.

Viewed from a practical angle, this study shows that many MSMEs already have useful habits, such as learning on their own, sharing tips with coworkers, and using the security features that come with digital platforms. These habits can actually be developed further through MSME assistance programs. Business associations, digital platforms, and government agencies can turn such everyday practices into short learning sessions or simple checklists that follow three gradual steps: raising awareness, adapting behavior, and managing security more consistently. As these efforts continue, they can be aligned with the PAMAN KAMI framework so that MSMEs can build stronger information security routines while staying realistic about their resources and scale of business. This steady approach helps practical experience grow into formal skills, making digital trust a goal that small enterprises can reach step by step.

4. CONCLUSION

This study reveals that MSMEs in Jakarta face a dilemma in building digital trust. From a quantitative perspective, the majority of respondents (70%) already use strong passwords and 80% are aware of the risks of phishing, but only 40% implement two-factor authentication and 20% follow the formal PAMAN KAMI guidelines. These figures indicate a clear gap between awareness and compliance. From the qualitative findings, interviews revealed that business owners often become aware of security issues only after facing direct incidents, such as almost being deceived by fraud or receiving fake transfer proofs. The strategies they adopt in response are generally straightforward, looking up information online, giving brief informal instructions to staff, and depending on security features already available in marketplaces or free applications. For most of them, these measures are seen as adequate for everyday operations, even if they fall short of offering full protection. The synthesis of these two findings resulted in a conceptual model of digital trust adaptation in MSMEs, with three main pillars: (1) awareness foundation, which is basic awareness born from real experiences; (2) practical adaptation, in the form of simple strategies in line with resource constraints; and (3) incremental governance, which is a gradual path from basic practices to formal standards. This model emphasizes that building digital trust in MSMEs is an incremental process, not an instant adoption.

This study has some boundaries. The data were drawn from only 30 MSMEs, all located in Jakarta, so the picture that emerges is still very local and should not be assumed to represent other regions. The survey used here was descriptive, which means it helped show patterns but could not explain cause-and-effect relationships. The interviews were also relatively brief. They gave useful insights, but they were not long enough to uncover deeper elements such as organizational culture. Future studies may broaden the scope by including more respondents from different regions so the findings can better reflect conditions at the national level. Using inferential methods in quantitative research would also allow scholars to identify the factors that shape compliance more precisely. On the qualitative side, deeper exploration within particular sectors such as culinary or fashion could offer richer insights into the specific context and internal dynamics that influence how MSMEs build digital trust.

Future longitudinal studies would also be valuable to observe how MSMEs sustain and evolve their digital trust practices over time. The proposed conceptual model can further guide policymakers and training institutions in developing targeted capacity-building programs that align with the stages of awareness, adaptation, and governance. Through this approach, MSME training initiatives can transform informal security habits into structured, sustainable practices that strengthen digital trust and resilience across Indonesia's small enterprise sector.

REFERENCES

[1] ISACA, "What's The State of Digital Trust This Year?," ISACA, 2024. [Online]. Available: https://www.isaca.org/digital-trust/state-of-digital-trust

[2] D. de Vreeze, "The State of Digital Trust in 2025 - Consumers Still Shoulder the Responsibility," Thales Group, 2025.

[3] M. F. Arroyabe, C. F. A. Arranz, I. Fernandez De Arroyabe, and J. C. Fernandez De Arroyabe, "Exploring the economic role of cybersecurity in SMEs: A case study of the UK," *Technol. Soc.*, vol. 78, p. 102670, Sep. 2024, doi: 10.1016/j.techsoc.2024.102670.

[4] J. Boehm, L. Grennan, A. Singla, and K. Smaje, "Why Digital Trust Truly Matters," *McKinsey & Company*, 2022.

[5] A. A. Wardana and E. Suryani, "Evaluation of information security management in MSMEs using Penilaian Mandiri Keamanan Informasi (PAMAN KAMI)," *presented at the In Proceedings of the 6th International Conference on Management of Technology, Innovation, and Project (MOTIP 2023)*, 2023.

[6] M. R. Slamet, M. Ikhlash, and F. Wulandari, "Analisis Penilaian Keamanan Informasi dengan menggunakan Penilaian Mandiri keamanan Informasi (PAMAN KAMI)," *J. Appl. Bus. Adm.*, vol. 6, no. 1, pp. 41–50, Mar. 2022, doi: 10.30871/jaba.v6i2.3604.

[7] A. A. Ajhari, M. A. Manaon, and Dimas, "Security Awareness Framework untuk Usaha Mikro, Kecil dan Menenengah di Indonesia," *Info Kripto*, vol. 17, no. 3, pp. 85–91, Dec. 2023, doi: 10.56706/ik.v17i3.80.

[8] I. M. Suartana, R. Eka Putra, R. Bisma, and A. Prapanca, "Pengenalan Pentingnya Cyber Security Awareness pada UMKM," *J. Abadimas Adi Buana*, vol. 5, no. 02, pp. 197–204, Jan. 2022, doi: 10.36456/abadimas.v5.i02.a4560.

[9] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[10] BSSN, "Peraturan BSSN Nomor 4 Tahun 2024 tentang Penyelenggaraan Penilaian Mandiri Keamanan Informasi bagi UMKM," Badan Siber dan Sandi Negara, 2024.

[11] BSSN, "Workshop pembinaan kapasitas kematangan keamanan siber UMKM Go Digital," Badan Siber dan Sandi Negara, 2025.

[12] Cyberthreat.id, "BSSN luncurkan panduan mandiri keamanan informasi bagi pelaku UMKM.," Cyberthreat.id, 2020.

[13] Komite.id, "Kepala BSSN: Pengaturan keamanan siber dinilai mendesak," Komite.id, 2023.

[14] A. Papathanasiou, G. Liontos, A. Katsouras, V. Liagkou, and E. Glavas, "Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era," *J. Inf. Secur.*, vol. 16, no. 01, pp. 1–43, 2025, doi: 10.4236/jis.2025.161001.

[15] B. Azinheira, M. Antunes, M. Maximiano, and R. Gomes, "A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal," *Procedia Comput. Sci.*, vol. 219, pp. 121–128, 2023, doi: 10.1016/j.procs.2023.01.272.

[16] S. Purnomo, N. Nurmalitasari, and N. Nurchim, "Digital transformation of MSMEs in Indonesia: A systematic literature review," *J. Manag. Digit. Bus.*, vol. 4, no. 2, pp. 301–312, Aug. 2024, doi: 10.53088/jmdb.v4i2.1121.

[17] T. TH. Tambunan and I. Busnetti, "Recent Evidence on the Digitalization Process in Indonesia's Micro and Small Enterprises," *Int. J. Curr. Sci. Res. Rev.*, vol. 07, no. 08, Aug. 2024, doi: 10.47191/ijcsrr/V7-i8-18.

[18] D. P. Nugraha, B. Setiawan, R. J. Nathan, and M. Fekete-Farkas, "Fintech Adoption Drivers for Innovation for SMEs in Indonesia," *J. Open Innov. Technol. Mark. Complex.*, vol. 8, no. 4, p. 208, Dec. 2022, doi: 10.3390/joitmc8040208.

[19] M. Bottarelli, G. Epiphaniou, S. Mahmood, M. Hooper, and C. Maple, "Assessing the Trustworthiness of Electronic Identity Management Systems: Framework and Insights from Inception to Deployment," 2025, *arXiv*. doi: 10.48550/ARXIV.2502.10771.

[20] Lucky Bamidele Benjamin, Ayodeji Enoch Adegbola, Prisca Amajuoyi, Mayokun Daniel Adegbola, and Kudirat Bukola Adeusi, "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies," *Glob. J. Eng. Technol. Adv.*, vol. 19, no. 2, pp. 134–153, May 2024, doi: 10.30574/gjeta.2024.19.2.0084.

[21] I. D. Sudirman, E. Astuty, and R. Aryanto, "Enhancing Digital Technology Adoption in SMEs Through Sustainable Resilience Strategy: Examining the Role of Entrepreneurial Orientation and Competencies," *J. Small Bus. Strategy*, vol. 35, no. 1, Jan. 2025, doi: 10.53703/001c.124907.

[22] B. Metin, F. G. Özhan, and M. Wynn, "Digitalisation and Cybersecurity: Towards an Operational Framework," *Electronics*, vol. 13, no. 21, p. 4226, Oct. 2024, doi: 10.3390/electronics13214226.

[23] E. Kahveci, "Digital Transformation in SMEs: Enablers, Interconnections, and a Framework for Sustainable Competitive Advantage," *Adm. Sci.*, vol. 15, no. 3, p. 107, Mar. 2025, doi: 10.3390/admsci15030107.

[24] M. Saeedikiya, S. Salunke, and M. Kowalkiewicz, "Toward a dynamic capability perspective of digital transformation in SMEs: A study of the mobility sector," *J. Clean. Prod.*, vol. 439, p. 140718, Feb. 2024, doi: 10.1016/j.jclepro.2024.140718.

[25] S. Joyce, "Bridging the gaps to cyber resilience: The C-suite playbook. Findings from the 2025 Global Digital Trust Insights," *Pricewaterhouse Coopers*, 2025.