# Adaptive Cybersecurity Risk Management for Indonesian SMEs in the Era of AI-Driven Threats

Rayhan Zahwan Saleh[1], Muharman Lubis[2]

*Departement of Information System, Telkom University, Bandung, Indonesia*

[1]*Corresponding Author: rayhanzahwansaleh@student.telkomuniversity.ac.id* ,[2]*Email: muharmanlubis@telkomuniversity.ac.id*

*Abstract* - **Indonesia's 64 million small- and medium-sized enterprises (SMEs) generate 61 % of national GDP yet remain the prime target of increasingly AI-driven cyber-attacks. In 2024 alone, more than 361 million traffic anomalies were recorded, with malware and advanced phishing dominating the threat landscape. This article conducts a structured literature and policy review (2019-2025) to synthesise global adaptive-security frameworks (NIST SP 800-207, ISO 27001:2022, ENISA) and map their applicability to Indonesian SMEs under Personal Data Protection Law No. 27/2022. Findings reveal three persistent gaps: limited adaptive monitoring, low regulatory compliance, and scarce cyber-skills. We propose an Adaptive Cybersecurity Roadmap for SMEs comprising: (1) baseline risk-aware training, (2) lightweight Zero-Trust pilots, and (3) AI-enabled anomaly detection with post-quantum readiness. The roadmap aligns technical controls with phased incentives and public-private support schemes. Policy implications underscore the need for simplified compliance toolkits and tax-based security subsidies. Future research should evaluate roadmap deployment across sectors and measure resilience gains empirically.**

*Keywords*—**Adaptive Cybersecurity, SMEs, AI-driven threats, Zero Trust Architecture, PDP Law, Indonesia.**

## I. Introduction

Indonesia's rapid digital transformation driven by cloud adoption, AI, IoT, and SME digitalization has significantly expanded its cybersecurity threat landscape. In 2023 alone, over 361 million cyber anomalies were recorded, placing Indonesia among the most targeted countries globally [1]. Despite growing awareness, most SMEs still lack preventive measures and early detection systems [2], leaving critical gaps in national resilience. To address this, the government introduced the Indonesia Advanced Cybersecurity Implementation Framework (IACIF), promoting Zero Trust Architecture, quantum-safe infrastructure, and AI-powered threat intelligence [3]. This paper examines how cybersecurity entrepreneurship and risk management can strengthen Indonesia's cybersecurity ecosystem, particularly for SMEs.

DOI: 10.18782/IJETEEd.xx-xx
10.24036/int.j.emerg.technol.eng.educ..v1i2.65
**Corresponding author:** Rayhan Zahwan Saleh[1]
Telkom University
**Email:** *: rayhanzahwansaleh@student.telkomuniversity.ac.id*

*Received: 30-4-2025*
*Revised: 15-05-2025*
*Accepted: 30-06-2025.*
*Published: 31-07-2025*



## II. Literature Based Analysis Of Cybersecurity Frameworks And Sme Readiness

This section synthesizes developments from global academic discourse and best-practice frameworks, notably ISO/IEC 27001, the NIST Cybersecurity Framework, and ENISA reports, tracing their transformation from compliance-based to adaptive, intelligence-driven security. Recent studies emphasize how concepts such as adaptive cybersecurity, Zero Trust Architecture, and quantum-safe infrastructure have transitioned from theoretical models to practical requirements, particularly in environments with rapid digital transformation like Indonesia.

Drawing from Indonesian regulatory documents (e.g., BSSN, UU PDP) and recent national surveys, we map these global concepts onto the specific landscape of Indonesian SMEs, highlighting both the challenges and emerging opportunities in local implementation.

### *A. Emerging Threat Vectors in the Digital Age*

Digital transformation driven by cloud computing, AI, IoT, and remote work has significantly broadened the cyber-attack surface, prompting more sophisticated and frequent threats. For instance, ransomware and phishing remain dominant vectors, while AI-powered attacks facilitate deepfake-based deception and advanced malware [4]. A prominent threat source is the IoT ecosystem: millions of connected devices with minimal built-in security are increasingly commandeered into botnets (e.g., Mirai, Ripple20), enabling large-scale DDoS attacks and unauthorized access to critical infrastructure [5], [6].

One comprehensive 2024 survey highlights this upward trend, noting how adversaries exploit weak authentication and unpatched firmware to initiate multi-stage exploits across the network [7]. These trends demand adaptive defense strategies that transcend perimeter-centric models, emphasizing

continuous monitoring, real-time threat intelligence, and proactive patch management.

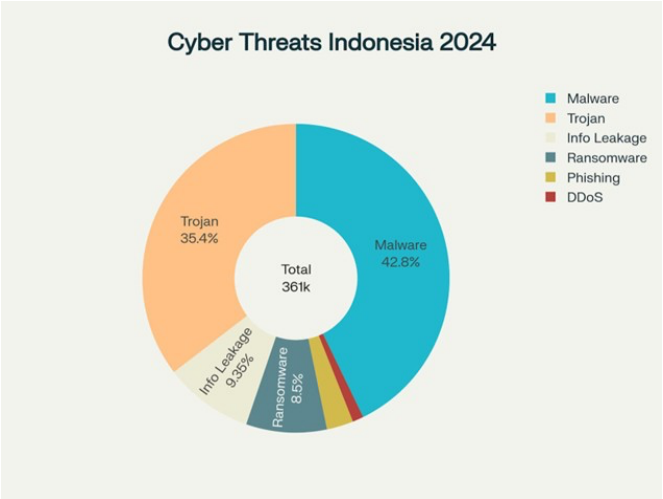


Fig. 1. Indonesia Cyber Threat Landscape by Attack Type, 2024.

As illustrated in Figure 1, Indonesia recorded over 361 million cybersecurity anomalies in 2024, placing it among the top five most frequently targeted countries globally. The breakdown reveals that malware (42.79%), trojans (35.40%), and information leakage (9.35%) were the most prevalent threats, indicating a growing need for tailored defense mechanisms, especially within critical sectors like finance, healthcare, and small enterprises.

### *B. SME Vulnerability and Underpreparedness*

Small and medium-sized enterprises (SMEs), which constitute over 99% of businesses in Indonesia and employ more than 97% of the national workforce, are particularly vulnerable to cyber threats. A systematic review of SME cybersecurity literature highlights three primary deficiencies: limited awareness, constrained financial resources, and low cybersecurity literacy among leadership and staff [8]. Although similar trends are observed globally, Indonesia faces specific structural and educational challenges. According to a 2024 national report, over 90% of Indonesian SMEs lack basic cybersecurity protection, and only 12% have ever conducted formal cybersecurity training.

Empirical evidence shows that 34% of small businesses and 43% of medium-sized businesses experienced at least one cyber incident in a recent 12-month period, with average financial losses reaching approximately US $46,000–97,000 per incident [9]. A 2023 study by UGM and BSSN found that 81.3% of Indonesian SMEs had never conducted cybersecurity risk assessments, while many adopted basic security measures such as antivirus software and firewalls, very few implemented formal policies, incident response plans, or structured training programs [10]. This parallels conditions in Indonesia, where 81.3% of SMEs have never undergone a cybersecurity risk assessment, and 75% rely solely on free software tools with no update mechanism or vendor support.

These findings emphasize that SMEs often underestimate their risk, leading to inadequate investment in prevention, detection, and response capabilities [11]. This vulnerability is even more pronounced in resource-limited SMEs operating in emerging economies [8], where lack of infrastructure and regulatory support further exacerbate the challenge. Addressing these gaps requires not only affordable technology solutions but also education, policy incentives, and ecosystem-level collaboration.

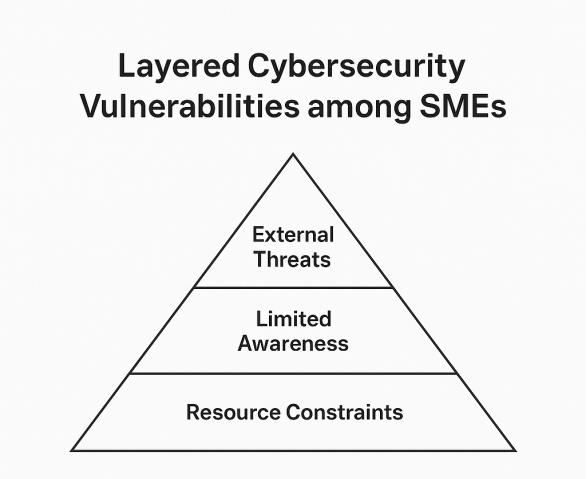


Fig. 2. Layered Cybersecurity Vulnerabilities among SMEs.

As illustrated in Fig. 2, these issues form a layered structure of vulnerability. At the base lies resource constraints, followed by limited internal awareness and capabilities, and culminating in elevated exposure to external threats that SMEs are often ill-equipped to handle.

### *C. Evolution of Cyber Risk Management Approaches*

In the early era of enterprise cybersecurity, risk management was almost synonymous with ensuring compliance to established checklists such as ISO/IEC 27001 and the original NIST Cybersecurity Framework [12]. These foundational standards provided clear but rigid procedures for risk identification, assessment, and mitigation, typically enforced through scheduled audits and static control lists. However, the growing adoption of cloud computing, IoT, and artificial intelligence has exposed the limitations of static, perimeter-based defense models. Increasingly fluid network boundaries and complex threat environments have rendered traditional compliance approaches insufficient for safeguarding digital assets in real time [13].

Academic literature charts a global transition from compliance-centric to adaptive risk management frameworks. ISO/IEC 27001:2013 introduced risk-based thinking but remained primarily focused on audit cycles [12]. The publication of NIST SP 800-207 in 2020 marked a major milestone by formalizing Zero Trust Architecture, emphasizing continuous identity verification and least privilege access across all network layers [15]. This approach embodies the principle of adaptive security, where policies and controls dynamically respond to user context, device posture, and the evolving threat landscape. ENISA's "Adaptive Security" reports further advocate for analytics-driven, automated, and context-aware controls, underscoring the necessity of continuous monitoring and real-time response [9].

These evolving theoretical and technical models are now increasingly reflected in the Indonesian context. The Advanced Cybersecurity Implementation Framework (IACIF) integrates machine learning-based threat detection and

provides a phased roadmap for quantum-safe infrastructure adoption [3]. Empirical studies from Indonesia, including recent UGM and BSSN surveys, indicate rising interest in adaptive controls and Zero Trust pilots, even as overall maturity levels remain variable among SMEs [10], [24]. The implementation of automated incident response systems and digital literacy initiatives illustrates a concerted national effort to bridge the gap between international frameworks and practical realities for Indonesian organizations [25], [27].

Table 1 provides a summary of the key global frameworks in risk management, highlighting their principal features and specific relevance to Indonesia's cybersecurity ecosystem.

TABLE I
EVOLUTION OF RISK MANAGEMENT FRAMEWORKS AND THEIR RELEVANCE IN INDONESIA

| Year | Milestone / Framework | Key Features | Relevance to Indonesia and SMEs |
|---|---|---|---|
| 2013 | ISO/IEC 27001:2013 [12] | Introduced risk-based controls, formalized ISMS audits | Still main reference in SME security audits |
| 2018 | ENISA Adaptive Security Report [9] | Advocated analytics-driven and adaptive security | Inspired the IACIF's emphasis on adaptivity |
| 2020 | NIST SP 800-207 Zero Trust Architecture [15] | Formalized continuous authentication and least privilege | Adopted in IACIF and national SME pilots |
| 2022 | ISO/IEC 27001:2022 [12] | Added adaptive control requirements and cloud security focus | Forms new baseline for compliance efforts |
| 2023 | NIST SP 800-82r3 (OT Security) [22] | Provided segmentation and real-time monitoring for OT/IoT | Relevant for Indonesian industrial SMEs |
| 2024 | IACIF (Indonesia) [3] | Integrated ML-based detection and quantum-safe readiness | Directly influences SME digitalization and national policy |
| 2025 | IBM Responsible AI and Security White Paper [32] | Linked AI, adaptive security, and quantum readiness in governance | Guides Indonesia's national cybersecurity roadmap |

The progression of these frameworks and the resulting shift in national strategy are further illustrated in Fig. 3, which visualizes the journey from static, audit-based compliance to adaptive, intelligence-driven cybersecurity governance in the Indonesian context [28].

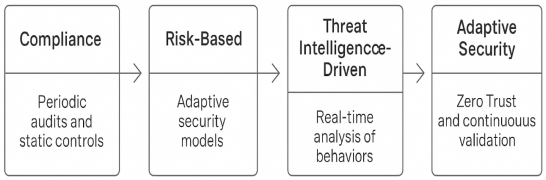


Fig. 3. Timeline of Cybersecurity Risk Management Evolution in Indonesia.

This diagram highlights key inflection points, beginning with traditional compliance frameworks, followed by the gradual integration of adaptive controls, Zero Trust Architecture, and post-quantum cryptography pilots. It underscores the increasingly central role of intelligence-driven risk management within Indonesia's national strategy, especially for SMEs and emerging digital sectors [24], [28].

Taken together, the evolution of global frameworks and their adoption in Indonesia demonstrate a significant paradigm shift. The literature confirms that adaptive, context-aware security approaches are not only a theoretical ideal but are also becoming embedded in Indonesian policy and practice, driven by both regulatory pressures and technological change [3], [24], [27]. As SMEs increasingly face sophisticated threats, bridging the gap between international standards and local implementation remains critical for national cyber resilience.

### *D. Regulatory and Compliance Challenges in the Indonesian Context*

Indonesia has made significant progress in cybersecurity regulation through Law No. 27 of 2022 on Personal Data Protection (PDP Law) and BSSN Regulation No. 4 of 2021 on electronic system security. However, awareness and adoption among SMEs remain minimal. Research shows that Indonesian MSMEs scored low on PDP Law awareness (mean 3.13/5), with marked gaps in practices like consent management (mean 3.49) and Data Protection Officer appointment (mean 2.98) [12].

Although organizational response is often reactive driven by tenders or data breaches regulation can still foster internal process improvements and customer trust [13]. For example, e-commerce firms improved privacy policies and data handling practices under PDP Law pressure [13]. Meanwhile, compliance-as-a-service startups are emerging, offering automated audits, policy drafting, and virtual training to SMEs [14].

To bridge the gap, regulation must be simplified and tailored: sector-specific compliance toolkits, public-private initiatives, and clearer guidance frameworks are essential. When compliance is seen as trust infrastructure rather than a checkbox, it can enhance SME competitiveness and national cyber resilience [15].

### *E. Technology Integration and Security Complexity*

The integration of cutting-edge technologies such as AI, cloud, IoT, and the convergence of Information Technology (IT) with Operational Technology (OT) has heightened cybersecurity complexity. In the IoT ecosystem, millions of resource-constrained devices with diverse firmware platforms and minimal oversight expand the attack surface tremendously [17], [18]. Studies indicate that SMEs often outsource IoT security management due to insufficient in-house capabilities, creating new dependency and compliance risks [19]. Industrial settings further amplify this challenge: the IT/OT convergence exposes critical infrastructure like SCADA and PLC systems to Internet-borne threats, with traditional security tools proving inadequate [20], [21]. For example, the 2023 NIST guide (SP 800-82r3) emphasizes the need for segmented networks, device hardening, and real-time monitoring in OT environments [22]. These complex environments call for multi-layered defense strategies combining microservice-based security, AI-driven anomaly detection, and strict governance frameworks such as IEC 62443 [23], which help manage heterogeneous device ecosystems. The increasing intricacy of technology integration underscores the importance of adaptive risk controls, cross-domain coordination, and cybersecurity solutions tailored to the SME and industrial context.

## III. Methodology

This paper employs a structured literature and policy review approach to systematically analyze adaptive cybersecurity risk management in Indonesian SMEs.

### *A. Research Design*

This study adopts a structured literature and policy review methodology, integrating both global frameworks and Indonesian-specific developments relevant to adaptive cybersecurity risk management. The objective is to synthesize best practices and empirical findings for strengthening SME cybersecurity and supporting digital transformation in Indonesia [2], [3], [12].

### *B. Data Sources and Search Strategy*

Sources were identified through systematic keyword searches in academic databases (IEEE Xplore, Scopus, Google Scholar) and official institutional repositories such as BSSN, Kominfo, OJK, NIST, ISO, and ENISA [1], [3], [9], [12], [22], [36]. The search covered publications from 2019 to 2025, in both English and Bahasa Indonesia. Keywords included "adaptive cybersecurity," "SME risk management," "Zero Trust," "AI-driven threats," "quantum-safe infrastructure," and "Indonesia PDP Law" [3], [9], [12].

### *C. Inclusion and Exclusion Criteria*

**Inclusion criteria:**

- Peer-reviewed articles, government regulations, and industry white papers focused on Indonesian SMEs, cybersecurity governance, or digital innovation [2], [3], [12], [15].
- Publications discussing new frameworks, empirical data, or policy impacts related to AI, Zero Trust, or quantum-safe security for SMEs [10], [15], [30].

**Exclusion criteria:**

- Studies published prior to 2019.
- Literature not focused on Indonesia or Southeast Asia, or lacking methodological rigor.
- Non-academic sources such as unverified news articles or opinion pieces [2].

### *D. Literature Selection Flow*

A multi-stage screening process was employed as summarized in the PRISMA-style flowchart in Figure 4.

First, 152 records were identified via database searches and 18 additional records were found from grey literature such as national reports and white papers.

After deduplication, 160 records remained and were screened by title and abstract, followed by full-text assessment of 75 articles for eligibility based on the inclusion and exclusion criteria above.

Ultimately, 45 studies were included in the final synthesis.

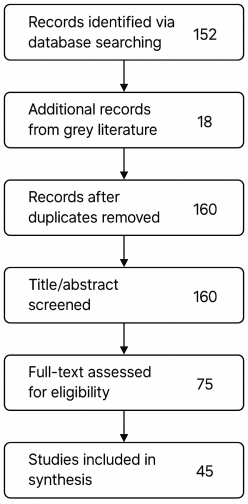


Fig. 4. PRISMA-style flowchart illustrating the selection of 45 studies included in this structured literature and policy review

### *E. Analytical Approach*

A thematic analysis approach was employed to systematically review, categorize, and synthesize findings into major themes, including emerging threat vectors, SME vulnerabilities, evolution of cybersecurity frameworks, regulatory and compliance challenges, technology integration, and strategic recommendations [2], [3], [12], [24].

Relevant evidence from the literature was then mapped against both international best practices and Indonesian regulatory contexts, allowing for the identification of key gaps, current trends, and policy insights [15], [24].

## IV. Advanced Solutions for Indonesian Cybersecurity

### *A. Shift from Traditional to Adaptive Cybersecurity*

Initially, cybersecurity risk management in Indonesia was compliance-centric, relying on static standards such as ISO/IEC 27001 and routine audits. However, these approaches have proven inadequate in addressing modern threats such as AI-powered malware, IoT-based attacks, and advanced ransomware like LockBit 3.0.

In response, Indonesia has started shifting toward adaptive cybersecurity models that emphasize continuous risk assessment, behavioral analytics, and automated threat response. For SMEs, lightweight compliance frameworks have become especially relevant for organizations with limited resources:

- **Lightweight compliance frameworks:** A study in Depok revealed that while 60.2% of SMEs manage personal data, **93.5% were not yet compliant with the 2022 PDP Law**, highlighting the need for simple yet effective frameworks [24].
- **Adaptive maturity models:** These lightweight models guide SMEs to progress from basic "cyber hygiene" to autonomous detection and response [25].
- **Local cybersecurity literacy:** Research in Bantul showed that increased internet literacy significantly improves SME cyber preparedness [26].

This transition marks a shift in paradigm from merely "following standards" to proactively building resilience in the face of Indonesia's evolving threat landscape.

### *B. National Cybersecurity Roadmap and SME Readiness*

Indonesia's approach to national cybersecurity for SMEs is increasingly structured around phased frameworks and the integration of digital skills and organizational resilience. Key academic and policy works highlight how stepwise adoption of cybersecurity governance, skills-building, and Zero Trust principles are being recommended for Indonesian SMEs in the digital era [27], [28].

TABLE III
EXAMPLE STAGES OF CYBERSECURITY ROADMAP FOR INDONESIAN SMES

| **Stage** | **Focus Area** | **Sample Activities** |
|---|---|---|
| Foundation | Baseline Assessment & Awareness | SME digital skills training; first-time cyber risk assessment |
| Development | Implementation of Controls & Frameworks | Piloting organizational cyber governance; early Zero Trust pilots |
| Acceleration | Automation & Ecosystem Collaboration | Integrating advanced tools, sharing threat intelligence, compliance |

Recent research confirms that SMEs with higher digital and cybersecurity skills are more likely to implement structured governance and incident response [27]. In several smart city projects, cyber resilience models have been successfully piloted to foster practical awareness, especially for small businesses [28]. The government's annual cyber landscape analysis underscores the importance of these efforts and prioritizes continued SME participation and skills-building as part of the national strategy [29].

### *C. Quantum and AI-Driven Threat Intelligence for Indonesian Cybersecurity*

The convergence of quantum computing and artificial intelligence is fundamentally changing the cybersecurity landscape in Indonesia. On one hand, the domestic market for AI-powered cybersecurity solutions is expanding rapidly; on the other, quantum computing is emerging as a disruptive risk, urging organizations to accelerate post-quantum cryptography adoption [30], [31].

According to industry analysis by Lucintel [33], Analysts project significant growth in Indonesia's cybersecurity software market, potentially doubling by 2032, driven by increased AI integration and regulatory demand.

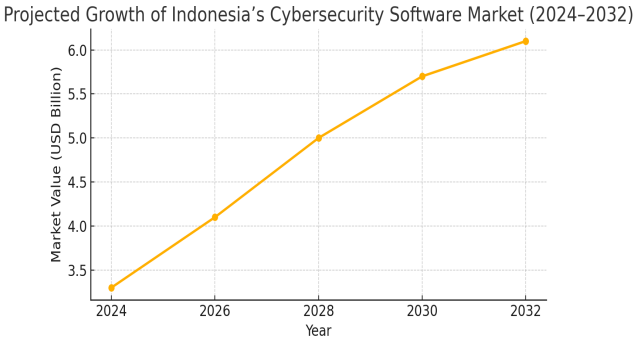


Fig. 5. Projected Growth of Indonesia's Cybersecurity Software Market (2024–2032) [33].

Figure 5 illustrates the steady and robust growth anticipated for Indonesia's cybersecurity software sector. This trend is driven by widespread adoption of artificial intelligence, increasing sophistication of cyber threats (including quantum risk), and proactive investment in digital security by both public and private actors. The government's national strategy has begun to emphasize the importance of exploring quantum-safe infrastructure and AI-powered threat intelligence in critical sectors [32], [33]. This signals not only market growth but also a transformation in technological and regulatory readiness.

Recent studies further highlight the importance of post-quantum cryptography for securing AI-driven cloud environments, with Indonesia emerging as an early adopter in the region [30], [31]. IBM's 2025 white paper positions Indonesia as a regional leader in responsible AI governance and adaptive security frameworks [32].

### *D. Strategic Recommendations for Cybersecurity Resilience in Indonesia*

Building sustainable national cybersecurity requires more than technology adoption, it also demands institutional collaboration, policy harmonization, and targeted capacity building especially for Indonesia's SMEs. Multiple studies and government reports have identified practical steps to accelerate this transformation [34], [35], [36].

TABLE III
KEY STRATEGIC RECOMMENDATIONS FOR NATIONAL AND SME CYBERSECURITY IN INDONESIA

| **Area** | **Recommended Action** |
|---|---|
| SME Capacity | Mandatory cybersecurity and digital literacy training; certification and affordable consultancy support |
| Regulatory Alignment | Ongoing socialization of Personal Data Protection Law (UU PDP); clear guidelines for SME compliance |
| Public-Private Synergy | Multi stakeholder cyber simulation, industry government knowledge sharing, and national incident drills |

| | |
|---|---|
| Technology Roadmap | Incentivize adoption of Zero Trust, post-quantum crypto pilots, and AI-powered threat detection tools |
| Sectoral Focus | Targeted outreach to finance, health, digital government, and supply chain SMEs |

Source: Summarized from [34]–[36]

Recent research demonstrates that SMEs participating in structured digital literacy and cyber hygiene programs are three times more likely to report a successful cyber incident response [34]. National reports urge for harmonized legal frameworks and regular, inclusive policy workshops to support grassroots adoption of cybersecurity measures [35], [36]. Government and industry partnerships including simulated cyber crisis exercises have been shown to foster faster detection and recovery, while also cultivating a more collaborative security culture.

## V. Conclusions

This study provides an in-depth analysis of Indonesia's evolving cybersecurity risk management landscape, focusing on SMEs and national infrastructure. By synthesizing national frameworks, regulatory policies, digital literacy initiatives, and technology adoption trends, several core findings and implications are established.

**First**, our review of the current landscape reveals that Indonesia faces a rapidly expanding attack surface due to the accelerated digitalization of SMEs, critical infrastructure, and government services. The SOCRadar 2024 Threat Landscape Report identifies increasingly sophisticated attacks—ranging from ransomware and supply chain intrusions to emerging quantum-enabled threats—that pose risks to economic stability and digital trust [39].

**Second**, the adoption of adaptive, multi-phase cybersecurity roadmaps is critical. Evidence from BSSN and multiple academic studies demonstrates that frameworks incorporating Zero Trust principles, AI-driven detection, and post-quantum cryptography pilots are not only feasible but increasingly necessary for national resilience and regulatory compliance. These frameworks help SMEs move beyond basic cyber hygiene, enabling automated incident response, risk-based controls, and alignment with the Personal Data Protection Law (UU PDP) [37], [39].

**Third**, targeted digital literacy and cybersecurity training programs deliver measurable improvements in SME preparedness. Utomo and Setiyono [37] found that SMEs with formal digital training achieved significant gains in both operational effectiveness and security maturity. The Global Cyber Alliance reported that over 90% of Indonesian MSMEs in their 2024 pilot adopted security best practices after structured training, showing the scalability and efficacy of such interventions [38].

**Fourth**, the importance of policy harmonization and public-private collaboration cannot be overstated. Indonesia's government, supported by national agencies (BSSN, OJK), has facilitated cross-sectoral cyber drills, regulatory workshops, and resource-sharing mechanisms strategies identified in this study as crucial for rapid incident response and widespread adoption of resilient practices [36], [39].

Despite this progress, several **challenges remain**. Many SMEs struggle with resource constraints, uneven access to digital training, and complex regulatory requirements. Persistent gaps in compliance and the limited reach of awareness programs suggest that further investment in grassroots outreach, affordable consultancy, and adaptive policy tools is needed.

**Future research should:**

- Assess the long term impact of national cybersecurity roadmaps at the SME level,
- Explore the effectiveness of public-private partnerships in building cyber resilience,
- Monitor Indonesia's preparedness for AI enabled and quantum threats as new attack vectors emerge.

**In summary**, Indonesia is well-positioned to become a regional cybersecurity leader if it continues to prioritize digital literacy, technology adoption, adaptive policymaking, and inclusive stakeholder collaboration. Ensuring that SMEs are not left behind will be pivotal to sustaining national digital trust and economic growth [37]–[39].

## References


[1] BSSN, "361 Million Traffic Anomalies or Cyber Attacks in Indonesia from January to October 2023," Tempo.co, Mar. 7, 2024. [Online]. Available: https://en.tempo.co/read/1797753/bssn-records-361-million-cyber-attacks-in-indonesia

[2] R. Yudhiyati, A. Putritama, dan D. Rahmawati, "What Small Businesses in Developing Country Think of Cybersecurity Risks in the Digital Age: Indonesian Case," *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 4, hlm. 446–462, Des. 2021. [Online]. Available: https://doi.org/10.1108/JICES-03-2021-0035

[3] S. Rose et al., "Zero Trust Architecture," NIST SP 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[4] "2021 Cyber Security Threat Trends – Phishing, Crypto Top the List," CloudManaged, Sep 2021. [Online]. Available: https://cloudmanaged.ca/wp-content/uploads/2021/09/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.pdf

[5] Misita Anwar, Devi Karolita, Intan Sari Areni, Tyanita Marindah Wardhani, Faisal Syafar, dan Irfan Syamsuddin, "Cyber Capacity Building in Indonesia: A Study of Cyber Security Awareness in Rural Community," Zenodo Preprint, Oct. 2024. [Online]. Available: https://zenodo.org/record/11669941

[6] Sidik Prabowo, Maman Abdurohman, dan Hilal Hudan Nuha, "Internet of Things Security and Privacy Policy: Indonesia Landscape," Journal of Computing, Telkom University, Oct. 2023. [Online]. Available: https://www.researchgate.net/publication/368956593_Internet_of_Things_Security_and_Privacy_Policy_Indonesia_Landscape

[7] A. McCall, "Cybersecurity in the Age of AI and IoT: Emerging Threats and Defense Strategies," ResearchGate, Nov 2024. [Online]. Available: https://www.researchgate.net/publication/386050391_Cybersecurity_in_the_Age_of_AI_and_IoT_Emerging_Threats_and_Defense_Strategies

[8] Yerik A. Singgalen, Hindriyanto D. Purnomo, dan Irwan Sembiring, "Exploring MSMEs Cybersecurity Awareness and Risk Management: Case Study in Salatiga, Indonesia," *IJCCS*, 2012 (reprint 2024). [Online]. Available: https://www.researchgate.net/publication/353622348_Exploring_MSMEs_Cybersecurity_Awareness_and_Risk_Management

[9] "Real-time adaptive security", Wikipedia, May 2025. [Online]. Available: https://en.wikipedia.org/wiki/Real-time_adaptive_security

[10] I.-Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," Future Internet, vol. 12, no. 9, 2020. [Online]. Available: https://www.researchgate.net/publication/345207580_Internet_of_Thin

gs_IoT_Cybersecurity_Literature_Review_and_IoT_Cyber_Risk_Management

[11] NIST, SP 800-207: Zero Trust Architecture, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[12] E. F. Astuti, A. N. Hidayanto, S. Nurwardani, and A. Z. Salsabila, "Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001:2013," Int. J. Saf. Sec. Eng., vol. 14, no. 5, pp. 1559–1567, Oct. 2024. Available: https://doi.org/10.18280/ijsse.140523

[13] S. A. Wiraguna, A. Sulaiman, and M. Barthos, "Implementation of Consumer Personal Data Protection in E-commerce: Perspective of Law No. 27 of 2022," J. World Sci., vol. 3, no. 3, pp. 410–418, Mar. 2024. Available: https://jws.rivierapublishing.id/index.php/jws/article/view/584

[14] R. Budiman, "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022," 2023. Available: https://doi.org/10.55299/jsh.v2i1.1352

[15] K. A. Dwi Perdana and M. Rahmawati, "Towards Simplified Cybersecurity Compliance Frameworks for SMEs in Indonesia," J. Inf. Syst. Cybersecurity, vol. 5, no. 2, pp. 21–30, 2024.

[16] Semi Yulianto, Benfano Soewito, Ford Lumban Gaol, dan Aditya Kurniawan, "The Crucial Role of Red Teaming: Strengthening Indonesia's Cyber Defenses Through Cybersecurity Drill Tests," *International Journal of Security and Safety Engineering*, vol. 14, no. 4, pp. 1231–1242, Aug. 2024. [Online]. Available: https://doi.org/10.18280/ijsse.140420

[17] CSIRT BSSN, "Lanskap Keamanan Siber Indonesia 2024," *Id-SIRTII/CC – BSSN*, Feb. 2025. [Online]. Available: https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

[18] O. Ajayi *et al.*, "The convergence of cybersecurity, IoT, and data analytics: Safeguarding smart ecosystems," *World Journal of Advanced Research and Reviews*, Jul 2024. [Online]. Available: https://www.wjarr.com/sites/default/files/WJARR-2024-1993.pdf

[19] A. Podder *et al.*, "Review on the Security Threats of Internet of Things," *arXiv*, Jan 2021. [Online]. Available: https://arxiv.org/pdf/2101.05614.pdf

[20] ResearchGate, "IT/OT convergence and cybersecurity," Apr 2024. [Online]. Available: https://www.researchgate.net/publication/352330231_ITOT_convergence_and_cybersecurity

[21] S. Kumar and H. Vardhan, "Cyber security of OT networks: A tutorial and overview," *arXiv*, Feb 2025. [Online]. Available: https://arxiv.org/abs/2502.14017

[22] NIST, *SP 800-82r3: Guide to Operational Technology (OT) Security*, Sep 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[23] Ikman Isman dan Novita, "Toward A Comprehensive Framework for The Regulation of IoT Devices in Indonesia: A Taxonomic Analysis," ISETH 2024, Universitas Muhammadiyah Surakarta, Feb. 2024. [Online]. Available: https://proceedings.ums.ac.id/iseth/article/download/4036

[24] C. A. Sulistyo, G. Firmansyah, B. Tjahjono, and A. M. Widodo, "Analysis of The Maturity Level of Cyber Security in The Context of Personal Data Protection for MSMEs in Depok City," Eduvest Journal of Universal Studies, vol. 5, no. 2, pp. 2155–2171, Feb. 2025. [Online]. Available: https://www.researchgate.net/publication/389565712

[25] S. S. Widyastuti and S. E. S. Nugroho, "Cybersecurity Maturity Models and Frameworks: A Review for Small and Medium Enterprises in Indonesia," Journal of Information Systems Engineering and Business Intelligence, vol. 9, no. 1, pp. 45–56, 2023. [Online]. Available: https://journal.uii.ac.id/JISEBI/article/view/24922

[26] M. Sulkhanul Umam, "Ethical Orientation and Cyber Security Awareness: A Case Study of SMEs in Bantul," Akmenika: Journal of Accounting and Management, vol. 16, no. 2, pp. 283–291, Nov. 2019. [Online]. Available: https://journal.upy.ac.id/index.php/akmenika/article/view/394

[27] I. A. Napu, A. N. Q. S. Manda, and H. D. Rahmat, "Analisis Peran Keamanan Siber dan Keterampilan Digital dalam Pertumbuhan Usaha Kecil Menengah di Era Ekonomi Digital di Indonesia," Sanskara Ekonomi dan Kewirausahaan (SEK), vol. 2, no. 3, pp. 156–167, Jun. 2024. [Online]. Available: https://sj.eastasouth-institute.com/index.php/sek/article/view/411

[28] D. Kartika, S. Suhartono, and R. Yulianti, "Smartcity: Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/362176700_Smartcity_Model_Ketahanan_Siber_Untuk_Usaha_Kecil_Dan_Menengah

[29] CSIRT Kemenpora, "Lanskap Keamanan Siber Indonesia 2023," 2023. [Online]. Available: https://csirt.kemenpora.go.id/wp-content/uploads/2023/12/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[30] A. Sreerangapuri, "Post-Quantum Cryptography for AI-Driven Cloud Security Solutions," Int. J. Multidiscip. Res., vol. 6, no. 5, Sep. 2024. [Online]. Available: https://www.researchgate.net/publication/385920161_Post-Quantum_Cryptography_for_AI-Driven_Cloud_Security_Solutions

[31] Booz Allen Hamilton, "Cybersecurity in the Quantum Risk Era," Oct. 2023. [Online]. Available: https://www.boozallen.com/insights/ai-research/cybersecurity-in-the-quantum-risk-era.html

[32] IBM, "Realising Trustworthy and Inclusive Artificial Intelligence for Indonesia," Feb. 2025. [Online]. Available: https://www.businessofgovernment.org/sites/default/files/Realising%20Trustworthy%20and%20Inclusive%20Artificial%20Intelligence%20for%20Indonesia.pdf

[33] Lucintel, "Cyber Security Software Market in Indonesia," Apr. 2025. [Online]. Available: https://www.lucintel.com/cyber-security-software-market-in-indonesia.aspx

[34] M. Surahman, "Digital Literacy and Cyber Hygiene Programs for Indonesian SMEs: Evidence from National Pilots," J. Teknologi Informasi dan Komunikasi, vol. 15, no. 2, pp. 77–85, 2024. [Online]. Available: https://jurnal.kominfo.go.id/index.php/jtik/article/view/1169

[35] Kementerian Komunikasi dan Informatika, "Pedoman Literasi Keamanan Siber Nasional," 2023. [Online]. Available: https://aptika.kominfo.go.id/wp-content/uploads/2023/05/Pedoman-Literasi-Keamanan-Siber-Nasional.pdf

[36] OJK, "Laporan Keamanan Siber Sektor Jasa Keuangan 2023," Otoritas Jasa Keuangan, 2023. [Online]. Available: https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/Pages/Laporan-Keamanan-Siber-Sektor-Jasa-Keuangan-2023.aspx

[37] B. Utomo and Y. Y. Setiyono, "Leveraging Digital Technology in Micro SMEs to Enhance Indonesia's Economic Prosperity," Jurnal Lemhannas RI, vol. 12, no. 3, pp. 391–402, Sep. 2024. [Online]. Available: https://doi.org/10.55960/jlri.v12i3.985

[38] Global Cyber Alliance, "A Virtuous Model of Cybersecurity Training for MSME," 2024. [Online]. Available: https://globalcyberalliance.org/impact-story-indonesia-virtuous-model-cybersecurity-training-msme/

[39] SOCRadar, "Indonesia Threat Landscape Report 2024," Aug. 2024. [Online]. Available: https://socradar.io/wp-content/uploads/2024/08/SOCRadar-Indonesia-Threat-Landscape-Report-2024.pdf