Data: Journal of Information Systems and Management
E-ISSN : 3031-0008
Volume. 2, Issue 2, April 2024
Page No: 85-92

Cybersecurity Challenges and Investment in Indonesia

Nuraini Purwandari
Institut Bisnis dan Informatika (IBI) Kosgoro 1957, Indonesia
Coresspondent: nuraini.purwandari@gmail.com

Received : February 26, 2024
Accepted : April 12, 2024
Published : April 30, 2024

Citation: Purwandari, N. (2024). Cybersecurity Challenges and Investment in Indonesia. Data: Journal of Information Systems and Management, 2 (2), 85-92.

ABSTRACT: Indonesia's digital economy has expanded rapidly, but this growth has been accompanied by a sharp rise in cyber threats, particularly ransomware and phishing attacks. Despite this, national cybersecurity investment remains critically low, at just 0.02% of GDP—among the lowest in ASEAN. This study analyzes the structural misalignment between the increasing threat landscape and the country's financial and policy responses. Using secondary data from 2020 to 2023, it examines attack frequencies, regional investment comparisons, and projected market growth. Key results indicate that while cyber incidents have escalated—from 88 million in early 2020 to 347 million in H1 2023—Indonesia's cybersecurity market is projected to grow from USD 1.07 billion in 2024 to USD 3.48 billion in 2030. However, regulatory fragmentation, limited SME readiness, and underdeveloped public-private coordination remain significant barriers. The study concludes that addressing policy fragmentation, increasing investment, and integrating SMEs into the national strategy are essential to secure Indonesia's digital future and unlock the potential of its growing cybersecurity market.

Keywords: Cybersecurity, Indonesia, Investment Gaps, Policy Fragmentation, SME Vulnerability, Digital Economy, Governance.

INTRODUCTION

Indonesia's digital transformation has accelerated across sectors, especially in e-commerce, fintech, and digital services. E-commerce is projected to reach more than USD 21 billion by 2025. Government initiatives such as the "20 Million New Digital Jobs by 2025" program aim to strengthen the digital workforce.

At the same time, cybercrime in Indonesia has risen sharply. BSSN reported over 1.6 billion anomalies in 2021 and 347 million cyber incidents in the first half of 2023. Cases such as the data breach at the General Election Commission (KPU) and ransomware attacks on hospitals highlight the severity of threats. These incidents show that Indonesia's digital growth is not matched by adequate cyber resilience. This increase is further compounded by the lag in regulatory responses,

creating a challenging environment for law enforcement and cybersecurity practitioners (Khan, 2024; Saha et al., 2024).

Cybersecurity breaches in Indonesia disrupt essential services, cause major financial losses, and undermine public trust. Without stronger protection, sectors such as finance, health, and government risk repeated service failures. Strengthening cybersecurity investment and governance is thus essential to safeguard not only enterprises but also Indonesia's economic stability. Cyber incidents can lead to severe disruptions in critical infrastructure services, causing damages that can amount to millions or even billions of dollars in recovery and reputation costs (Mphatheni & Maluleke, 2022). For example, the costs associated with cyber disruptions can lead to lost productivity, legal fees, and litigation costs, adversely affecting national economic performance (Mphatheni & Maluleke, 2022).

There exists a strong correlation between cybersecurity investments and growth within the digital economy. Countries prioritizing cybersecurity frameworks tend to have a more robust digital economy, as businesses are more willing to innovate and adopt new technologies in a secure environment (Mphatheni & Maluleke, 2022). A comparative analysis indicates that nations investing heavily in cybersecurity initiatives generally report accelerated economic growth and stability (Mphatheni & Maluleke, 2022).

In the context of Indonesia, national cybersecurity policy frameworks have been implemented to address these challenges, primarily through the National Cyber and Crypto Agency (BSSN). BSSN has initiated several policies aimed at enhancing national security in cyberspace, facilitating cooperation across government entities, and fostering a culture of cybersecurity awareness within both the public and private sectors (Mphatheni & Maluleke, 2022). These initiatives are critical for enabling Indonesia to effectively combat the escalating threat of cyber incidents.

When comparing Indonesia's cybersecurity investments with those of other ASEAN nations, notable disparities exist. Research indicates that while Indonesia is progressively increasing its cybersecurity budget, other countries in the ASEAN region, such as Singapore and Malaysia, exhibit higher per capita investments in cybersecurity measures (Saha et al., 2024). This difference highlights a critical area for Indonesia to enhance its capacities and respond to emerging cyber threats more effectively.

In conclusion, the trends in digital transformation in Indonesia and the wider ASEAN context not only showcase opportunities for economic growth but also underline the pressing need for comprehensive cybersecurity strategies to mitigate the evolving threats of cybercrime. The focus on policy frameworks and investment in cybersecurity will be pivotal in securing the digital future of the region.

METHOD

This study evaluates Indonesia's national cybersecurity preparedness using a descriptive-comparative approach. The analysis is based on secondary data collected from official reports of the National Cyber and Crypto Agency (BSSN) for 2020–2023, supported by international benchmarking such as the Global Cybersecurity Index (GCI). The framework includes institutional capacity, legal frameworks, human resources, technical measures, and public–private partnerships. The indicators combined to form these frameworks typically encompass human resources, legal frameworks, institutional capacity, technical measures, and public-private partnerships (Dutton et al., 2019). For instance, the Global Cybersecurity Index (GCI) employs a set of 25 indicators to evaluate the cybersecurity commitment of countries, thus providing a comparative understanding of cybersecurity preparedness (Nguyen et al., 2021).

Secondary data were obtained from five BSSN annual and half-yearly reports (2020–2023) and industry analysis platforms (Mordor Intelligence, regional ASEAN data). Data were analyzed descriptively and compared across ASEAN countries. This allowed identification of investment trends, cyberattack frequencies, and policy gaps. However, the reliability of these sources may vary based on their data collection methodologies, the recency of the data, and any potential biases inherent in their reporting (Abdelhamid et al., 2019; Abrahams et al., 2024). Both BSSN and relevant industrial analysis platforms are regarded as reputable sources, yet it's important to cross-validate findings with primary research and other credible data to substantiate conclusions drawn from such secondary analyses (Abdelhamid et al., 2019; Abrahams et al., 2024).

Indicators used include: (1) frequency and type of cyber incidents (BSSN data), (2) investment levels in cybersecurity as % of GDP, (3) compliance with legal frameworks such as Perpres 82/2022, and (4) SME readiness. Findings were validated through triangulation by comparing multiple data sources and reviewed by two cybersecurity policy experts. Qualitative indicators often focus on public sentiments towards government cybersecurity initiatives, employee cybersecurity training effectiveness, and overall cultural attitudes towards cybersecurity within organizations (Dornheim & Zarnekow, 2023). Methodologies also involve stakeholder consultations and evaluations of existing cybersecurity programs and policies against set benchmarks established during national or international collaborations (Abdelhamid et al., 2019; Dornheim & Zarnekow, 2023).

In summary, a comprehensive evaluation of national cybersecurity preparedness employs both quantitative and qualitative methodologies, underpinned by reliable secondary data sources and a variety of key indicators to assess policy effectiveness. This multifaceted approach captures the complexities inherent in national cybersecurity readiness and allows for a thorough understanding of the strengths and weaknesses that exist in current frameworks

RESULT AND DISCUSSION

Cybersecurity Threat Trends

Indonesia's cybersecurity landscape has undergone a significant transformation in recent years, marked by the rapid escalation of ransomware, malware, and phishing threats. These attacks predominantly target the human element of security through social engineering tactics and exploit weaknesses in national infrastructure. Notably, ransomware attacks have emerged as a key threat vector, especially during the shift to remote work in the COVID-19 era. Government data from BSSN reveals annual spikes linked to global ransomware campaigns affecting Southeast Asia.

The most vulnerable sectors include finance, healthcare, government, telecommunications, and e-commerce, primarily due to their high data value and transaction volume. When benchmarked against regional averages, Indonesia experiences one of the highest incidences of cyberattacks in Southeast Asia, highlighting systemic cybersecurity vulnerabilities.

Table 1. Year-wise Cyberattack Incidents in Indonesia (2020–2023)

Year/Period	Number of Incidents	Notable Details
Jan–Apr 2020	88 million	Trojan and COVID-19 phishing dominate
2021 (Full Year)	1.65 billion anomalies	Major traffic anomalies, significant escalation
Q1 2022	11 million	22% increase YoY
H1 2023	347 million	Ransomware top contributor

Investment Analysis

Indonesia's cybersecurity investment, measured at just 0.02% of GDP, is the lowest in ASEAN. By contrast, regional peers such as Singapore and Malaysia invest significantly more, reflecting differing levels of cyber readiness. Since 2013, Indonesia has gradually increased its cybersecurity budget—doubling it over the last decade in response to high-profile cyber incidents and growing digital exposure.

Global benchmarks suggest allocating 1–2% of organizational IT budgets to cybersecurity. The gap between Indonesia's current figures and these standards underscores the urgency for policy-driven investment. Empirical studies affirm that increased public funding correlates with a measurable reduction in cyber incidents.

Figure 1. Cybersecurity Budget as % of GDP (ASEAN Comparison)

Country	% of GDP Spent on Cybersecurity
Indonesia	0.02%
Singapore	~0.22%
Malaysia	~0.1%
Thailand	~0.08%
Vietnam	~0.05%

Market Forecast Indonesia's cybersecurity market is expanding rapidly, driven by digital transformation initiatives, regulatory reform, and increased enterprise awareness. The rise of IoT and cloud computing significantly widens the attack surface, necessitating new forms of defense.

According to Mordor Intelligence, the market is projected to grow from USD 1.07 billion in 2024 to USD 3.48 billion in 2030, with a CAGR of approximately 20.8%. Sub-sectors such as cloud security and IoT protection are leading this trend, though the sector faces constraints, including a shortage of skilled labor and limited SME investment capacity.

Figure 2. Indonesia's Cybersecurity Market Forecast (2024–2030)

Year	Estimated Market Value (USD)
2024	1.07 billion
2025	1.35 billion
2030	3.48 billion

Regulatory Environment

Indonesia has implemented several cybersecurity regulations, including the ITE Law and the Personal Data Protection Law, complemented by Perpres 82/2022. These aim to institutionalize national cybersecurity standards and unify agency efforts.

While Perpres 82/2022 has enhanced regulatory visibility and interagency collaboration, challenges remain. Cybersecurity governance continues to suffer from fragmented leadership and inconsistent technical maturity across ministries. Additionally, SMEs struggle to comply with evolving regulations due to financial and expertise constraints.

A centralized, enforced policy framework remains essential to coordinate national responses and mitigate risks across both public and private sectors.

Fragmented policy frameworks can significantly undermine national cybersecurity efforts by creating silos that impede comprehensive threat management and coordination. When multiple

agencies establish their own policies without adequate alignment, inconsistencies can arise, leading to gaps in coverage and increased vulnerabilities. This disjointed approach can result in duplicated efforts or conflicting regulations, creating confusion among stakeholders regarding compliance and incident reporting. A lack of unified governance also impairs the flow of critical information needed for early threat detection and coordinated responses. Integrated cybersecurity policies are thus essential, encouraging inter-agency collaboration and fostering a unified culture of security awareness.

Underinvestment in cybersecurity is particularly detrimental to Small and Medium-sized Enterprises (SMEs). With limited resources, SMEs often fail to implement basic protections, leaving them exposed to increasingly complex threats such as phishing, ransomware, and data breaches. These vulnerabilities can lead to significant financial losses and reputational damage, further threatening their sustainability. Without targeted support and investment, SMEs struggle to adopt modern security frameworks, deepening the digital divide and weakening the broader national defense.

Integrating cybersecurity policy across sectors requires the adoption of best practices such as the establishment of a centralized cybersecurity authority. This body would harmonize governance, facilitate collaboration, and set common compliance standards. Regular cross-sectoral training and knowledge-sharing initiatives can also bridge gaps in expertise and policy understanding. Moreover, engaging the private sector in cybersecurity strategy ensures shared accountability and leverages industry innovations in defense.

Long-term, insufficient cybersecurity investment poses risks to national development. It diminishes investor confidence, especially in sectors reliant on digital infrastructure, while increasing costs from breaches and remediation. These risks can stall innovation, disrupt essential services, and reduce the adoption of digital technologies. Over time, low investment erodes national competitiveness, undermining the stability of the digital economy.

In summary, policy fragmentation, SME vulnerabilities, weak intersectoral integration, and underinvestment represent systemic barriers to cybersecurity resilience. Strengthening governance, coordinating efforts, and increasing national investment are essential for securing Indonesia's digital future and ensuring inclusive economic development.

CONCLUSION

This study reveals that Indonesia is grappling with a growing disconnect between the escalation of cyber threats and its limited cybersecurity investment. Despite a surge in attack frequency—rising from 88 million incidents in early 2020 to over 347 million in just the first half of 2023—the nation continues to allocate only 0.02% of its GDP to cybersecurity, far below regional peers. While regulatory progress has been made through policies such as Perpres 82/2022, implementation remains fragmented across sectors.

The findings highlight the critical vulnerabilities of SMEs, whose limited resources render them highly susceptible to cyber incidents. Furthermore, the current decentralized and sectoral approach to cybersecurity governance hinders a unified national response to emerging threats.

However, the outlook is not entirely negative. Indonesia's cybersecurity market presents robust growth potential, projected to expand to USD 3.48 billion by 2030. If aligned with strong governance and coordinated policy action, this economic opportunity could enhance national resilience.

To close the gap between threats and defense capabilities, Indonesia must urgently adopt an integrated national cybersecurity strategy. This includes: increasing public investment in cybersecurity infrastructure and training, consolidating regulatory oversight under a centralized authority, enforcing compliance standards, and offering targeted support to SMEs.

By addressing these gaps, Indonesia can transform its cybersecurity landscape—strengthening its digital economy, protecting critical infrastructure, and positioning itself as a resilient leader in Southeast Asia's digital future.

REFERENCE

Abdelhamid, M., Kisekka, V., & Samonas, S. (2019). Mitigating e-services avoidance: the role of government cybersecurity preparedness. *Information and Computer Security*, 27(1), 26–46. https://doi.org/10.1108/ics-02-2018-0024

Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., & Hassan, A. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., & Alturki, R. (2024). A novel IDS with a dynamic access control algorithm to detect and defend intrusion at IoT nodes. *Sensors*, 24(7), 2188. https://doi.org/10.3390/s24072188

Chicha, M., & Phiri, J. (2024). Factors influencing the adoption of e-marketing in the tourism industry by SMEs in developing countries based on UTAUT model. *Open Journal of Business and Management*, 12(1), 521–539. https://doi.org/10.4236/ojbm.2024.121032

Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information and Computer Security*, 32(2), 179–196. https://doi.org/10.1108/ics-07-2023-0116

Dutton, W., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: does it matter? *Journal of Information Policy*, 9, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Khan, A. (2024). Reconceptualizing policing for cybercrime: perspectives from Singapore. *Laws*, 13(4), 44. https://doi.org/10.3390/laws13040044

Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International Journal of Research in Business and Social Science (2147-4478)*, 11(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714

Nguyen, T., Koblandin, K., Suleymanova, S., & Volokh, V. (2021). Effects of 'digital' country's information security on political stability. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1112

Pekarčík, M., Šafár, L., Rutecka, P., & Morawiec, P. (2024). Unveiling the impact of ownership structure on SMEs' cybersecurity perceptions. https://doi.org/10.21203/rs.3.rs-4526358/v1

Prawiyogi, A., & Alwiyah, A. (2023). Southeast Asia's cyber security strategy: multilateralism or self-help. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 4(2), 119–127. https://doi.org/10.34306/itsdi.v4i2.581

Saha, S., Hasan, A., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: a bibliometric analysis and future research agenda. *Multidisciplinary Reviews*, 7(8), 2024168. https://doi.org/10.31893/multirev.2024168