Data: Journal of Information Systems and Management
E-ISSN : 3031-0008
Volume. 2, Issue 1, January 2024
Page No: 14-24

Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Cybersecurity Regulatory Framework (2020–2023)

Tahegga Primananda Alfath[1], Waskita Cahya[2]
[1]Universitas Narotama, Indonesia
[2]Institut Bisnis dan Informatika (IBI) Kosgoro 1957, Indonesia
Correspondent: tahegga.primananda@narotama.ac.id[1]

Received : December 12, 2023
Accepted : January 6, 2024
Published : January 31, 2024

Citation: Alfath, T, P., Cahya, W. (2024). Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Cybersecurity Regulatory Framework (2020–2023). Data: Journal of Information Systems and Management, 2 (1), 1-9.

ABSTRACT: Indonesia's rapid digital transformation has heightened its exposure to cybersecurity threats, prompting the introduction of several national policies aimed at enhancing cyber resilience. This study evaluates the effectiveness of three key regulations—Peraturan BSSN No.8/2020, Perpres 82/2022, and Perpres 47/2023—through a qualitative policy analysis framework. Data were drawn from national cyber incident statistics, regulatory documents, and secondary literature. Methodologically, the study applies qualitative frameworks and correlates policy timelines with cyber incident volumes between 2020 and 2023. Statistical tools, including time-series and regression analyses, are used to determine regulatory impacts on threat reduction. Findings reveal that while the regulations establish a strong structural foundation, implementation remains weak. Cyber incidents continued to rise post-regulation, and key challenges such as agency fragmentation, underinvestment (0.02% of GDP), and limited stakeholder collaboration persist. Case studies, including breaches at Dukcapil and Imigrasi, underscore the urgent need for better enforcement and inter-agency coordination. Comparative analysis with regional peers like Singapore highlights further room for improvement in governance and public-private synergy. The study concludes that Indonesia's cybersecurity policies are directionally sound but require systemic reforms, centralized coordination, and investment scaling to achieve tangible outcomes. These insights contribute to the literature on regulatory effectiveness and cyber governance in emerging economies.

Keywords: Cybersecurity, Policy Evaluation, Digital Governance, Indonesia, Cyber Threats, Regulatory Effectiveness, ASEAN.

INTRODUCTION

In recent years, the global landscape of cybersecurity has been dramatically reshaped by the rapid digital transformation occurring in many developing countries. These nations, while benefitting

from the efficiencies and growth offered by digitalization, have also become prime targets for increasingly sophisticated cyber threats. Indonesia is no exception. A substantial body of literature illustrates that cyber incidents, such as ransomware attacks and data breaches, have increased markedly between 2020 and 2023 (Khan et al., 2023). This rise correlates with expanded digital footprints and the insufficient development of cybersecurity infrastructures across sectors.

The surge in digital adoption in Indonesia, particularly among government institutions and small to medium-sized enterprises (SMEs), has intensified exposure to cyber risks. Layode et al. (2024) note that the widespread transition to online platforms across health, financial, and public service sectors has not been matched by proportionate security protocols, creating vulnerabilities. Moreover, Benjamin et al. (2024) emphasize that SMEs face unique challenges due to resource limitations and inadequate cybersecurity literacy. These dynamics necessitate context-specific cybersecurity strategies capable of addressing both institutional and SME vulnerabilities effectively.

Indonesia's early cybersecurity policies were often criticized for being reactive rather than proactive. According to Bagui et al. (2023), the initial regulatory approaches lacked coherence and were slow to keep pace with technological developments. However, in the past decade, the government has introduced several comprehensive frameworks to strengthen national cybersecurity posture. These include strategic documents and operational policies, some influenced by ASEAN regional cybersecurity cooperation efforts (Kim et al., 2023).

From 2020 to 2023, three pivotal regulations were enacted: Peraturan BSSN No.8/2020 mandated electronic systems to perform self-risk assessments and align with ISO/IEC 27001 standards; Perpres 82/2022 designated nine sectors as Critical Information Infrastructure (CII), each with sectoral cybersecurity mandates; and Perpres 47/2023 launched a national cybersecurity strategy emphasizing risk identification, mitigation, and crisis management. These regulations represent Indonesia's response to a mounting wave of cyberattacks and data breaches, including high-profile cases affecting the Directorate General of Population and Civil Registration (Dukcapil) and the Directorate General of Immigration in 2023.

The effectiveness of national cybersecurity strategies, however, remains a topic of academic debate. Arafa et al. (2023) and Ahmad et al. have documented the correlation between strategic cybersecurity investments and lower incident rates. Yet, Indonesia's cybersecurity spending is still significantly lower than its ASEAN counterparts, at just 0.02% of GDP. Despite the structural progress in regulatory design, implementation challenges persist. Khaw et al. (2024) highlight that inter-agency collaboration, enforcement capacity, and stakeholder coordination are essential for the success of any national cybersecurity framework. Nagyfejeo & Solms (2020) similarly caution that awareness campaigns and regulatory mandates often fail without institutional accountability and cultural integration.

The societal implications of cyber breaches in Indonesia extend beyond economic damage. Khan et al. (2023) and Benjamin et al. (2024) argue that recurring breaches erode public trust in digital services, reduce user engagement, and undermine national digital economy goals. These

consequences call for more than policy design; they demand effective implementation, continuous monitoring, and adaptive learning mechanisms to ensure resilience.

In sum, the trajectory of cybersecurity threats in Indonesia has been shaped by rapid digital adoption, regulatory evolution, and persistent implementation gaps. Based on this background, the study is guided by the following research questions: (1) To what extent have Indonesia's cybersecurity regulations (2020–2023) reduced the volume of cyber incidents? (2) What implementation challenges persist in translating policies into effective practices? (3) How do Indonesia's regulatory approaches compare with regional peers? The objective of this study is to critically evaluate the effectiveness of Indonesia's cybersecurity regulations in enhancing national resilience.

METHOD

The evaluation of Indonesia's cybersecurity regulations from 2020 to 2023 necessitates a multifaceted methodological approach, integrating qualitative assessment frameworks, cyber incident data analytics, and contextual policy evaluation suited to emerging economies. This study employs a qualitative policy evaluation strategy to assess the efficacy of Peraturan BSSN No.8/2020, Perpres 82/2022, and Perpres 47/2023 within the broader trajectory of Indonesia's cybersecurity development.

To analyze regulatory effectiveness, this study draws on qualitative methodologies, notably adapted frameworks such as the FDA's Benefit-Risk Framework (Freyer et al., 2024), which, while originally intended for healthcare devices, provides a flexible structure for assessing risk-benefit dynamics in cybersecurity. Complementing this, the multi-criteria decision analysis (MCDA) method facilitates a structured comparison across multiple domains of regulatory performance, including clarity of mandates, institutional coordination, and practical outcomes (Okoye et al., 2024).

Primary data was drawn from secondary sources, including public reports by BSSN (Indonesia's National Cyber and Crypto Agency), international cybersecurity indexes, and academic publications. To deepen insight into stakeholder experiences and regulatory nuances, the study is informed by literature on semi-structured interviews with sectoral experts, highlighting the application of organizational learning frameworks for regulation evaluation (Mahmood et al., 2024).

Cyber incident statistics serve a dual function in this analysis... As Melaku (2023) and Folorunsho et al. (2024) observe, such empirical tracking validates whether regulations have translated into real-world cybersecurity gains. To strengthen validity, triangulation was applied by cross-checking cyber incident data from BSSN, international indexes, and peer-reviewed publications. Potential bias from secondary data was mitigated by comparing multiple sources. Methodological limitations

include the absence of primary interviews and constraints in accessing real-time cyber incident data, which may affect the comprehensiveness of findings.

The implementation effectiveness of each regulation is also evaluated against best practices in cybersecurity policy for emerging economies. Key evaluative criteria include adaptability, stakeholder inclusivity, and alignment with international cybersecurity norms. Oyeniyi et al. (2024) emphasize that systematic reviews of local cybersecurity frameworks, coupled with iterative policy refinement, are crucial. Meanwhile, Yamada (2024) and Abrahams et al. (2024) underscore the importance of multi-stakeholder collaboration and international alignment to enhance policy relevance and resilience.

Therefore, the study synthesizes these three pillars:

1. Qualitative Frameworks – adapted decision-making tools and risk assessment models;
2. Cyber Incident Data Analysis – correlation of regulatory enactments with threat patterns;
3. Best Practice Criteria – drawn from emerging economy contexts, emphasizing flexibility, inclusiveness, and harmonization.

This methodology supports a robust analysis of Indonesia's cybersecurity policy effectiveness, enabling the identification of both strengths and structural gaps in the current regulatory landscape. The integrative design of this evaluation is especially pertinent given the complex and evolving nature of cyber threats in developing digital economies.

RESULT AND DISCUSSION

Regulatory Design and Sectoral Responsibility

Indonesia's regulatory framework for cybersecurity underwent notable advancements through the introduction of three major policies. Peraturan BSSN No.8/2020 established foundational mandates for public institutions, including risk assessment protocols, incident management, and compliance with ISO/IEC 27001. The regulation's structured approach emphasized protecting state assets through mandatory controls and regular evaluations (Ramadhan, 2022).

Perpres 82/2022 and Perpres 47/2023 built upon this by assigning sector-specific roles and responsibilities. Perpres 82/2022 outlined responsibilities across ministries and agencies, aiming to foster inter-agency coordination. Perpres 47/2023 expanded this with a tiered implementation model emphasizing cross-sector collaboration and integrated response strategies. These frameworks align Indonesia with global best practices and highlight a national commitment to cohesive cybersecurity governance (Alexandri et al., 2023).

Table 1. Timeline of Major Cyber Regulations (2020–2023)

Year	Regulation	Description
2020	Peraturan BSSN No.8/2020	Risk-based assessment, ISO/IEC 27001 compliance.
2022	Perpres 82/2022	Defines 9 critical sectors with sectoral risk governance.
2023	Perpres 47/2023	Introduces national cybersecurity strategy and crisis protocols.

Comparative Policy Maturity in ASEAN

Indonesia's progress is consistent with regional trends, though gaps remain when compared to mature systems like Singapore's. While Singapore emphasizes real-time threat intelligence and robust compliance systems, Indonesia is still developing enforcement capacity. Nevertheless, Indonesia demonstrates a proactive trajectory, illustrated by its regulatory expansion and agency development (Estiyovionita & Sitamala, 2022).

Strategic Goals of Cybersecurity Regulation

The overarching goals of Indonesia's regulatory framework include:

- Enhancing cyber resilience of critical infrastructure
- Improving national incident response capabilities
- Building public-private partnerships
- Promoting cybersecurity education and awareness These goals signify a strategic orientation toward long-term digital resilience (Kalderemidis et al., 2022).

Incident Trends and Policy Correlation

Cyber incident data from 2020 to 2023 reflect a consistent increase in attacks:

Table 2. Cyber Incidents and Regulatory Timeline

Period	Incident Volume	Regulation Active
Jan–Apr 2020	88 million	Pre-regulatory period
2021	1.65 billion	BSSN No.8/2020
Q1 2022	11 million	Pre-Perpres 82/2022
Full 2022	~1 billion	Under Perpres 82/2022
H1 2023	347 million	Under Perpres 47/2023

This increase, despite regulatory actions, suggests gaps in policy enforcement and organizational preparedness (Mishra et al., 2022).

Analytical Models and Correlation Techniques

Using time-series and regression analyses, researchers correlated policy implementation with cyber incident volumes. These analyses showed that while policies were introduced timely, observable reductions in incident rates were minimal due to lag in execution. Predictive models are being used to forecast future threats, further underscoring the need for responsive regulatory frameworks (Layode et al., 2024; Pramoda et al., 2022).

Implementation Challenges and Investment Benchmarks

Multiple factors hinder effective policy implementation:

- Resource disparities among agencies and SMEs
- Bureaucratic inefficiencies and poor coordination (Fortin & Héroux, 2022)
- Public unawareness and cultural underreporting tendencies

Table 3. Policy Evaluation Matrix

Regulation	Key Features	Implementation Score (1–5)	Key Weaknesses
BSSN No.8/2020	Self-assessment, ISO standard	2	SME participation low
Perpres 82/2022	Sector-specific risk planning	3	Sectoral silos persist
Perpres 47/2023	Crisis readiness planning	2	Coordination inefficiency

Benchmarking reveals Indonesia's cybersecurity spending remains at 0.02% of GDP—far below ASEAN peers. Structural Equation Modeling (SEM) confirms that financial commitment is key to compliance and policy success (Rattanapong & Ayuthaya, 2025).

Coordination Issues and Lessons from Breach Cases

Coordination remains a systemic issue due to fragmented responsibilities and poor communication channels. Case studies, such as the Dukcapil and Imigrasi breaches, expose noncompliance and weak enforcement. These breaches highlight the urgent need for continuous training, public awareness, and post-incident audits to prevent recurrence (Hersugondo et al., 2022; Kalderemidis et al., 2022; "Investing in cybersecurity", 2020).

In sum, Indonesia's cybersecurity regulatory framework demonstrates clear strategic intent and structural evolution. However, its effectiveness is undermined by resource constraints, fragmented coordination, and delayed implementation. The integration of predictive analytics and inter-agency collaboration remains vital for future regulatory efficacy.

Cybersecurity governance in multi-agency systems is inherently complex and fraught with challenges. In Indonesia, these challenges manifest in several critical ways. One primary issue is the fragmentation of roles and responsibilities. Without clear jurisdictional boundaries and unified cybersecurity objectives, multiple agencies often work in silos, leading to redundant efforts, inefficiencies, and gaps in national defense systems (Oliha et al., 2024). Moreover, the disparity in institutional capabilities and resources further exacerbates this fragmentation, as smaller agencies may lack the technical expertise and infrastructure to comply with national mandates effectively.

Political and organizational dynamics also play a significant role in impeding cybersecurity governance. Agency priorities may be influenced by political considerations, resulting in misalignment with national cybersecurity goals (Slater et al., 2024). These internal conflicts hinder inter-agency collaboration and diminish the overall coherence of national cybersecurity strategies.

Comparative insights from the ASEAN region further highlight the shortcomings in Indonesia's approach. Singapore, for instance, has developed a centralized and comprehensive cybersecurity model that integrates proactive threat management, strong public awareness campaigns, and a resilient regulatory structure (Huang et al., 2021). Indonesia, by contrast, continues to face challenges in enforcing compliance and mobilizing public engagement (Weiss & Jankauskas, 2018). Singapore's model, which leverages robust public-private partnerships, illustrates the potential of coordinated frameworks that Indonesia has yet to fully capitalize on (Familoni & Shoetan, 2024).

The importance of public-private collaboration cannot be overstated in enhancing cybersecurity resilience. Collaborative initiatives enable the pooling of resources, the sharing of threat intelligence, and the co-creation of adaptive cybersecurity standards. By aligning government oversight with private sector agility, such partnerships can address real-time challenges more effectively (Atkins & Lawson, 2021). A culture of shared responsibility also encourages ongoing dialogue and mutual accountability in cybersecurity implementation.

To overcome the structural challenges within Indonesia's cybersecurity framework, several strategic reforms are necessary. First, establishing a centralized cybersecurity coordination body could streamline communication and ensure regulatory consistency across sectors (Juanatey et al., 2024). This institution should be equipped to monitor, evaluate, and enforce policies, while fostering stakeholder collaboration. Second, cybersecurity training and education programs must be institutionalized across all governmental levels and extended to the private sector and civil society. This would promote widespread literacy and a proactive cybersecurity culture (Blamire & Rees, 2025).

Furthermore, introducing measurable performance indicators and accountability mechanisms would support continuous improvement and foster inter-agency trust. These metrics can guide policy adjustments and incentivize agencies to align with national objectives (Elendu et al., 2024). Lessons from high-profile data breaches in Indonesia underscore the urgent need for rigorous post-incident evaluations and strategic recalibrations.

In conclusion, Indonesia's cybersecurity governance faces multifaceted challenges that stem from systemic fragmentation, underutilized public-private synergy, and limited institutional readiness. Learning from regional exemplars and investing in integrative, performance-driven strategies will be essential to strengthen national resilience in the evolving cybersecurity landscape.

CONCLUSION

Indonesia has made substantial progress in formulating a national cybersecurity regulatory framework through Peraturan BSSN No.8/2020, Perpres 82/2022, and Perpres 47/2023. These policies reflect a structured approach to enhancing resilience through institutional mandates, sectoral coordination, and crisis management strategies. However, cyber incident trends indicate that practical enforcement lags behind policy formulation. Inter-agency fragmentation, limited funding (0.02% of GDP), and weak public-private collaboration remain persistent obstacles.

This study has several limitations. It relies primarily on secondary data sources, which may not capture the full complexity of institutional practices. In addition, the analysis is context-specific to Indonesia and may not be generalizable to other settings. Future studies should conduct in-depth qualitative research on policy implementation at institutional levels, and comparative regional analyses across ASEAN states.

In conclusion, the effectiveness of Indonesia's cybersecurity framework depends not only on regulatory design but also on implementation capacity, adequate investment, and inclusive stakeholder engagement. Strengthening centralized coordination, scaling investment, and fostering public-private partnerships are strategic imperatives for building sustainable national resilience.

REFERENCE

Abrahams, T., Ewuga, S., Kaggwa, S., Uwaoma, P., Hassan, A., & Dawodu, S. (2024). *Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity*. Computer Science & IT Research Journal, 5(1), 120-140. https://doi.org/10.51594/csitrj.v5i1.709

Alexandri, M., Usman, I., Narimawati, U., & Taryana, A. (2023). *Unraveling the fintech landscape: a systematic mapping study on the impact of financial technology innovation on investment decision-making in ASEAN banking*. Khazanah Sosial, 5(1), 113-124. https://doi.org/10.15575/ks.v5i1.24555

Arafa, A., Sheerah, H., & Alsalamah, S. (2023). *Emerging digital technologies in healthcare with a spotlight on cybersecurity: A narrative review*. Information, 14(12), 640. https://doi.org/10.3390/info14120640

Atkins, S., & Lawson, C. (2021). *An improvised patchwork: Success and failure in cybersecurity policy for critical infrastructure*. Public Administration Review, 81(5), 847–861. https://doi.org/10.1111/puar.13322

Bagui, L., Lusinga, S., Pule, N., Tuyeni, T., Mtegha, C., Calandro, E., … & Solms, B. (2023). *The impact of COVID-19 on cybersecurity awareness-raising and mindset in the Southern African Development Community (SADC)*. The Electronic Journal of Information Systems in Developing Countries, 89(4). https://doi.org/10.1002/isd2.12264

Benjamin, L., Adegbola, A., Amajuoyi, P., Adegbola, M., & Adeusi, K. (2024). *Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies*. Global Journal of Engineering and Technology Advances, 19(2), 134–153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Blamire, J., & Rees, J. (2025). *Robust local governance responses in the context of turbulence: The case of collaborative and co-created COVID-19 pandemic responses in two local authority areas in England*. Social Policy and Administration, 59(2), 350–359. https://doi.org/10.1111/spol.13126

Darmawan, A., Yuliawan, D., Aida, N., & Husain, F. (2024). *Identifying the influence of foreign direct investment toward the ASEAN Economic Community 2025*. KNE Social Sciences. https://doi.org/10.18502/kss.v9i14.16090

Elendu, C., Omeludike, E., Oloyede, P., Obidigbo, B., & Omeludike, J. (2024). *Legal implications for clinicians in cybersecurity incidents: A review*. Medicine, 103(39), e39887. https://doi.org/10.1097/md.0000000000039887

Estiyovionita, K., & Sitamala, A. (2022). *ASEAN's role in cybersecurity maintenance and security strategy through an international security approach*. Lampung Journal of International Law, 4(2), 77–86. https://doi.org/10.25041/lajil.v4i2.2556

Familoni, B., & Shoetan, P. (2024). *Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria*. Computer Science & IT Research Journal, 5(4), 850–877. https://doi.org/10.51594/csitrj.v5i4.1046

Folorunsho, S., Adenekan, O., Ezeigweneme, C., Somadina, I., & Okeleke, P. (2024). *Ensuring cybersecurity in telecommunications: Strategies to protect digital infrastructure and sensitive data*. Computer Science & IT Research Journal, 5(8), 1855–1883. https://doi.org/10.51594/csitrj.v5i8.1448

Fortin, A., & Héroux, S. (2022). *Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis*. Information and Computer Security, 31(1), 108–123. https://doi.org/10.1108/ics-07-2022-0122

Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., & Gilbert, S. (2024). *Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review*. Journal of Medical Internet Research, 26, e65528. https://doi.org/10.2196/65528

Hersugondo, H., Widyarti, E., Maruddani, D., & Trimono, T. (2022). *ASEAN-5 stock price index valuation after COVID-19 outbreak through GBM-MCS and VAR-SDPP methods*. International Journal of Financial Studies, 10(4), 112. https://doi.org/10.3390/ijfs10040112

Huang, K., Madnick, S., Choucri, N., & Fang, Z. (2021). *A systematic framework to understand transnational governance for cybersecurity risks from digital trade*. Global Policy, 12(5), 625–638. https://doi.org/10.1111/1758-5899.13014

Juanatey, A., Jordana, J., & Sancho, D. (2024). *Multi-level governance in higher education quality assurance: Agencification and policy coordination in Spain*. Review of Policy Research, 42(3), 530–551. https://doi.org/10.1111/ropr.12624

Kalderemidis, I., Farao, A., Bountakas, P., Panda, S., & Xenakis, C. (2022). *GTM: Game theoretic methodology for optimal cybersecurity defending strategies and investments*, 1–9. https://doi.org/10.1145/3538969.3544431

Kamariotou, M., & Kitsios, F. (2023). *Information systems strategy and security policy: A conceptual framework*. Electronics, 12(2), 382. https://doi.org/10.3390/electronics12020382

Khan, N., Ikram, N., & Saleem, S. (2023). *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country*. Security Journal, 37(2), 214–244. https://doi.org/10.1057/s41284-023-00375-4

Khaw, T., Amran, A., & Teoh, A. (2024). *Building a thematic framework of cybersecurity: A systematic literature review approach*. Journal of Systems and Information Technology, 26(2), 234–256. https://doi.org/10.1108/jsit-07-2023-0132

Kim, Y., Go, M., Kim, S., Lee, J., & Lee, K. (2023). *Evaluating cybersecurity capacity building of ASEAN Plus Three through social network analysis*. 網際網路技術學刊, 24(2), 495–505. https://doi.org/10.53106/160792642023032402031

Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). *Company cybersecurity system: Assessment, risks and expectations*. Production Engineering Archives, 29(4), 379–392. https://doi.org/10.30657/pea.2023.29.43

Layode, O., Naiho, H., Adeleke, G., Udeh, E., & Labake, T. (2024). *The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data*. International Medical Science Research Journal, 4(6), 668–693. https://doi.org/10.51594/imsrj.v4i6.1228

Mahmood, S., Chadhar, M., & Firmin, S. (2024). *Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective*. Information, 15(2), 106. https://doi.org/10.3390/info15020106

Melaku, H. (2023). *A dynamic and adaptive cybersecurity governance framework*. Journal of Cybersecurity and Privacy, 3(3), 327–350. https://doi.org/10.3390/jcp3030017

Mishra, A., Alzoubi, Y., Anwar, M., & Gill, A. (2022). *Attributes impacting cybersecurity policy development: An evidence from seven nations*. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Nagyfejeo, E., & Solms, B. (2020). *Why do national cybersecurity awareness programmes often fail?*. International Journal of Information Security and Cybercrime, 9(2), 18–27. https://doi.org/10.19107/ijisc.2020.02.03

Okoye, C., Nwankwo, E., Usman, F., Mhlongo, N., Odeyemi, O., & Ike, C. (2024). *Securing financial data storage: A review of cybersecurity challenges and solutions*. International Journal of Science and Research Archive, 11(1), 1968–1983. https://doi.org/10.30574/ijsra.2024.11.1.0267

Oliha, J., Biu, P., & Chimezie, O. (2024). *Securing the smart city: A review of cybersecurity challenges and strategies*. Open Access Research Journal of Multidisciplinary Studies, 7(1), 094–101. https://doi.org/10.53022/oarjms.2024.7.1.0013

Oyeniyi, L., Ugochukwu, C., & Mhlongo, N. (2024). *Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices*. Computer Science & IT Research Journal, 5(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049

Pramoda, M., Pramoda, S., & Correa, Z. (2022). *Luster regained: A novel cyber incident risk prediction model using machine learning*. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 01–19. https://doi.org/10.32628/cseit2283125

Ramadhan, I. (2022). *ASEAN consensus and forming cybersecurity regulation in Southeast Asia*. https://doi.org/10.4108/eai.31-3-2022.2320684

Rattanapong, P., & Ayuthaya, S. (2025). *Influential factors of cybersecurity investment: A quantitative SEM analysis*. Management Science Letters, 15(1), 31–44. https://doi.org/10.5267/j.msl.2024.3.005

Slater, S., Lawrence, M., Wood, B., Sêrodio, P., Akker, A., & Baker, P. (2024). *The rise of multi-stakeholderism, the power of ultra-processed food corporations, and the implications for global food governance: A network analysis*. Agriculture and Human Values, 42(1), 177–192. https://doi.org/10.1007/s10460-024-10593-0

Trim, P., & Lee, Y. (2022). *Combining sociocultural intelligence with artificial intelligence to increase organizational cyber security provision through enhanced resilience*. Big Data and Cognitive Computing, 6(4), 110. https://doi.org/10.3390/bdcc6040110

Weiß, M., & Jankauskas, V. (2018). *Securing cyberspace: How states design governance arrangements*. Governance, 32(2), 259–275. https://doi.org/10.1111/gove.12368

Yamada, R. (2024). *Impact of cybersecurity regulations on corporate compliance practices in Japan*. International Journal of Law and Policy, 9(2), 28–38. https://doi.org/10.47604/ijlp.2705