Data: Journal of Information Systems and Management
E-ISSN : 3031-0008
Volume. 2, Issue 3, July 2024
Page No: 152-163

Digital Risks in Emerging Economies: Cyber Threat Escalation in Indonesia (2020–2023)

Rinaldo[1], Devi Puspitasari[2]
[1]Sekolah Tinggi Manajemen Ilmu Komputer Mercusuar, Indonesia
[2] Institut Bisnis dan Informatika (IBI) Kosgoro 1957, Indonesia
Correspondent: rinaldo@mercusuar.ac.id[1]

Received : May 21, 2024
Accepted : July 2, 2024
Published : July 31, 2024

Citation: Rinaldo., Puspitasari, D. (2024). Digital Risks in Emerging Economies: Cyber Threat Escalation in Indonesia (2020–2023). Data: Journal of Information Systems and Management, 2 (3), 152-163.

ABSTRACT: Indonesia's rapid digital transformation over the past decade has brought with it a surge in cyber threats, posing significant risks to national security, economic resilience, and public trust. This study investigates the escalation of cyber incidents between 2020 and 2023, analyzing their trends, regulatory responses, and systemic vulnerabilities. Utilizing secondary data from national agencies and international platforms, the research employs both quantitative and qualitative methods to assess incident volumes and policy effectiveness. The results reveal a sharp rise in cyber incidents, from 88 million in 2020 to over 1.65 billion in 2021, driven largely by phishing, ransomware, and malware campaigns. Although regulatory frameworks such as BSSN Regulation No. 8/2020 and Presidential Regulations 82/2022 and 47/2023 represent important steps, enforcement remains weak, and sectoral coordination is limited. Investment in cybersecurity is critically low, averaging only 0.02% of GDP, while SMEs remain particularly vulnerable due to limited resources and awareness. Discussion of these findings highlights systemic barriers such as institutional fragmentation, insufficient technical capacity, and underdeveloped cybersecurity culture. The study emphasizes the importance of inter-agency collaboration, adaptive regulatory frameworks, and increased investment to build national resilience. Comparative insights from global best practices suggest that integrating stakeholder feedback and promoting continuous learning can significantly enhance threat response and governance outcomes. In conclusion, Indonesia's cybersecurity landscape requires urgent strategic realignment. A well-funded, coordinated, and flexible national cybersecurity framework is essential to protect the nation's digital infrastructure and foster sustainable digital development.

Keywords: Cybersecurity. Indonesia, Digital Transformation, Cyber Threats, Policy Response, SME Vulnerability, Investment Strategy

INTRODUCTION

The intensification of cyber threats globally has become a critical concern, particularly amidst accelerated digital transformation. As technological advancements facilitate connectivity and data

exchange across borders, they also inadvertently expose institutions and individuals to a wider array of cyber vulnerabilities. Cybercriminals capitalize on these technological improvements to gain unauthorized access to sensitive systems, commit fraud, and disrupt essential services, often resulting in significant financial and operational consequences across public and private sectors (Ngo et al., 2020; Arora, 2024). With the advent of global interconnectivity, national borders offer little protection from cyberattacks, prompting an urgent need for robust, proactive cybersecurity frameworks (Rusman & Kamaludin, 2024; Akdemir et al., 2020).

Within the Southeast Asian context, Indonesia has emerged as a dynamic player in regional digitalization efforts. The country has experienced substantial growth in internet penetration, reportedly reaching over 75% of the population (Cross & Holt, 2021). This rapid expansion has facilitated digital access for millions, supporting both economic development and e-governance. However, it has also introduced a wider attack surface for malicious cyber activity. Recent reports indicate a significant rise in cybercrime incidents in Indonesia, revealing the inadequacy of current infrastructure and institutional readiness to cope with this evolving threat landscape (Rahmat et al., 2023). The need for well-articulated, enforceable cybersecurity policies and systems has become increasingly critical, especially as Indonesia seeks to strengthen its digital economy and public service delivery (Yudhianto, 2023).

Numerous studies have shown a clear link between internet penetration and national cybersecurity vulnerabilities. As more people come online, especially in regions where digital literacy is still developing, there is often a lack of awareness about online risks. This gap makes users more susceptible to cyber threats such as phishing, social engineering, and identity theft (Khan et al., 2022; Mupila et al., 2023). Furthermore, individual behavior online can amplify these risks, necessitating structured public education campaigns focused on safe internet practices (Kurniasih, 2023; Drew, 2020). Failure to bridge this gap between inclusion and awareness can result in increased exposure to cybercrime, jeopardizing national economic stability and individual privacy (Hadlington & Chivers, 2018).

Cyber threats are not confined to personal data breaches but extend to the disruption of vital public services. In developing economies like Indonesia, attacks on critical infrastructure—including health systems, water utilities, and transportation networks—can have devastating effects. The global ransomware attack known as WannaCry in 2017 severely impacted healthcare systems and served as a stark reminder of the consequences of insufficient cybersecurity protocols (Zhang et al., 2023; Lee et al., 2019; Monteith et al., 2021). The ability of these threats to paralyze essential services underscores the urgency of developing and implementing comprehensive cybersecurity strategies at the national level (Akdemir et al., 2020; Holt & Lee, 2019).

Raising public awareness is essential to preventing cybercrime at a national scale. Citizens who are informed about the nature of cyber threats and equipped with the knowledge to recognize potential risks are far more likely to engage in protective behaviors. Programs that emphasize reporting protocols and offer guidance on secure digital practices can cultivate a more resilient digital community (Shukurov & Jafarov, 2023; Suarmita & Purnomo, 2024). Empirical evidence suggests that education and awareness are directly correlated with reduced victimization, making them key

components of any national cybersecurity strategy (Drew & Farrell, 2018; Althibyani & Al-Zahrani, 2023). For example, the Indonesian government's cybercrime prevention initiatives, including campaigns on social media platforms like Twitter, reflect an understanding of the pivotal role that public engagement plays in cybersecurity resilience (Rahmat et al., 2023).

Globally, governments have adopted diverse strategies to combat the rise in cyber threats. These range from comprehensive legislation such as the European Union's General Data Protection Regulation (GDPR) to the formation of national cybersecurity agencies that coordinate cross-sectoral threat responses (Fissel & Lee, 2023). Countries like India have also taken steps to enact specialized cybercrime laws that aim to protect citizens and enforce compliance among institutions (Sankhwar et al., 2023; Kaur & Saini, 2022). These efforts are often supported by investments in law enforcement training, public-private partnerships, and advanced threat detection technologies (Malik & Islam, 2019; Razaque et al., 2021). Such comprehensive approaches illustrate the necessity of integrating legislation, awareness, and technological tools to construct a robust national cybersecurity ecosystem.

In summary, the global cybersecurity environment is rapidly evolving in response to technological change, and Indonesia is at a critical juncture. The nation’s aspirations for digital modernization must be matched by an equally ambitious strategy to protect its digital assets and citizens. This study seeks to explore the trajectory of cyber threats in Indonesia between 2020 and 2023, assess the effectiveness of regulatory responses, and identify the strategic gaps that hinder cybersecurity implementation. Through a synthesis of empirical data and policy analysis, this research aims to contribute to the formulation of a more secure, inclusive, and resilient digital infrastructure for Indonesia.

METHOD

This study adopts a descriptive-analytical methodology aimed at understanding the escalation of cyber threats in Indonesia from 2020 to 2023. The approach is rooted in the structured analysis of secondary data, supplemented by qualitative assessment of regulatory documents. The goal is to ensure methodological rigor while addressing the limitations of budgetary constraints and access to proprietary datasets.

The use of secondary data necessitates strict adherence to best practices in cybersecurity incident research. Data triangulation forms the foundation of this methodology. Incident reports were drawn from multiple authoritative sources, including the Badan Siber dan Sandi Negara (BSSN), international threat intelligence platforms, and public records. This multi-source strategy ensures the reliability and comprehensiveness of the findings. Ramlo and Nicholas (2021) argue that data triangulation strengthens the analytical framework by compensating for inconsistencies and gaps within individual data sets. Ofoegbu et al. (2024) further emphasize the integration of data-driven insights and user-centric protocols in understanding threat dynamics.

Additionally, advanced data analytics techniques were used where available. Sarker et al. (2020) highlight the utility of machine learning in categorizing and detecting cyber threats, particularly in large datasets. While machine learning tools were not directly applied in this study, their role in similar studies supports the trend analysis and inference of attack vectors based on published statistics.

The qualitative dimension of this study involves a comprehensive evaluation of national regulatory documents. These include BSSN Regulation No. 8 of 2020, Presidential Regulation No. 82 of 2022 on Critical Information Infrastructure, and Presidential Regulation No. 47 of 2023 on Cyber Crisis Management. A systematic analysis was conducted by comparing each regulation against internationally recognized standards, particularly ISO/IEC 27001 and the NIST Cybersecurity Framework. Thematic analysis was used to identify recurring challenges in implementation, strengths in strategic formulation, and gaps in inter-agency coordination. Although specific evidence on thematic analysis efficacy in regulatory contexts is limited, this approach offers practical insights into policy alignment and sectoral uptake (Taherdoost, 2022).

Stakeholder perspectives were incorporated indirectly through the examination of commentary and reports from cybersecurity experts, SMEs, and academic discussions, which reflect user experiences and institutional challenges in the field. Pike et al. (2019) stress the value of real-world feedback in evaluating policy implementation, and this principle guided the secondary interpretation of regulatory efficacy.

In contexts with limited financial resources, robust frameworks are necessary to guide efficient cybersecurity development. This study applies principles from the Cybersecurity Capability Maturity Model (C2M2) and the NIST Cybersecurity Framework to benchmark Indonesia's strategic posture. These models are particularly suitable in low-budget environments, offering stepwise improvements without the need for extensive capital investment. Taherdoost (2022) notes their adaptability across institutional and national settings, and their structured approach aligns with the needs of nations undergoing digital transformation.

Local adaptation of these models was considered by referencing national priorities, regulatory scope, and stakeholder capabilities. Krishna and M.P. (2021) underscore the relevance of contextual customization in applying global frameworks to national systems. The research recognizes Indonesia's unique socio-political dynamics, digital infrastructure variability, and regulatory fragmentation, which necessitate localized implementation of global standards.

This methodological approach ensures the study captures both the quantitative escalation in cyber threats and the qualitative dimensions of institutional readiness and policy design. By integrating structured data analysis with contextual policy evaluation, the research contributes to a holistic understanding of Indonesia's cybersecurity landscape and its evolution over the last four years.

RESULT AND DISCUSSION

Cyber Threat Trends

Between 2020 and 2023, Indonesia experienced a marked escalation in cyber threats, consistent with broader trends observed across ASEAN. Phishing, ransomware, and denial-of-service (DoS) attacks were among the most common threats. Phishing gained particular traction due to its effectiveness in deceiving users into disclosing sensitive information, often exploiting human vulnerabilities and emotional triggers (Akdemir & Yenal, 2021; Alabdan, 2020).

Table 1. Cyber Incident Trends in Indonesia (2020–2023)

Year	Incident Volume	Major Threat Type	Notes
2020	88 million	Trojan, Phishing	COVID-themed attacks
2021	1.65 billion	Anomaly traffic	20x increase from 2020
2022	~1 billion	Malware (50%), Data leaks (15%)	Persistent high-level threats
2023	347 million (H1)	Ransomware	High-profile breaches

The COVID-19 pandemic further exacerbated these threats. The onset of the pandemic led to a surge in phishing attacks as cybercriminals exploited public fear and increasing reliance on digital communication. Abroshan et al. (2021) reported a notable increase in phishing emails themed around health updates and emergency relief. Simultaneously, ransomware attacks intensified, particularly in the healthcare sector, where cybercriminals used highly sophisticated tactics to exploit critical service dependencies (Beaman et al., 2021; Naidoo, 2020).

Anomaly detection and cybersecurity intelligence have evolved with the implementation of machine learning algorithms and artificial intelligence. These technologies analyze patterns in network traffic and user behavior, enabling organizations to identify and respond to threats in real-time (Ispahany et al., 2024; Kamal et al., 2020). Furthermore, multilayered security strategies that integrate technical systems with behavioral training have shown promise in enhancing detection and response capabilities (Adu-Manu & Ahiable, 2023).

Case studies and systematic reviews from ASEAN and similar economies confirm a year-on-year rise in cyber incidents during this period. The increased frequency of cyber threats correlated strongly with the acceleration of digital transformation, particularly during the pandemic. Studies show how structural vulnerabilities in digital infrastructure have been exploited amidst rapid change (Chigada & Madzinga, 2021; Awaludin et al., 2023; Ammy-Driss & Garcin, 2020; Zahra et al., 2022).

Regulatory Developments

Indonesia's cybersecurity framework is anchored by BSSN Regulation No. 8/2020, Presidential Regulation No. 82/2022 on Critical Information Infrastructure, and Presidential Regulation No. 47/2023 on Cyber Crisis Management. Implementation of ISO/IEC 27001 has helped

government bodies establish structured security management systems, aligning with global standards. The standard facilitates the development of a security-aware culture and ensures alignment with international privacy regulations (Odimarha et al., 2024; Adegbite et al., 2023). However, persistent issues such as limited employee training and integration challenges affect the overall effectiveness (Familoni & Shoetan, 2024).

Table 2. Indonesian Cybersecurity Regulations and Focus Areas

Regulation	Year	Focus Area	Implementation Notes
BSSN No.8	2020	Risk assessment, ISO27001 compliance	Weak enforcement and uptake
Perpres 82	2022	CII designation, risk governance	Fragmented sector execution
Perpres 47	2023	National strategy, crisis management	Early-stage adoption

Indonesia can draw valuable insights from countries with mature Critical Infrastructure Protection (CIP) systems. International models demonstrate that effective public-private partnerships significantly enhance national resilience. These partnerships support knowledge sharing, cross-sector threat intelligence, and innovation in security protocols (Ramakrishnan & Chittibala, 2024; Mahn et al., 2021). A risk-based approach tailored to infrastructure criticality can further optimize resource allocation and policy enforcement (Adegbite et al., 2023).

Fragmentation remains a significant barrier in Indonesia's cybersecurity regulation landscape. Overlapping mandates among agencies result in inconsistent enforcement, delayed responses, and inefficiencies that cybercriminals exploit (Maphosa, 2024; Dedeke & Masterson, 2019). This fragmented governance also hinders innovation and impairs the deployment of advanced security technologies (Ramotsoela et al., 2018).

To measure the effectiveness of cybersecurity regulations, researchers employ several metrics: compliance with frameworks like NIST and ISO, incident response time, sector-wide enforcement levels, and user awareness (García-Pérez et al., 2021; Angafor et al., 2020). Additional indicators such as employee training coverage and stakeholder satisfaction offer insights into the operational success of cybersecurity initiatives (Chimezie et al., 2024; Ramlo & Nicholas, 2021).

Investment Trends

Indonesia's cybersecurity investment remains among the lowest in ASEAN, averaging only 0.02% of GDP. This contrasts starkly with countries like Singapore, which allocate significantly more in pursuit of regional cybersecurity leadership (Krishna & M.P., 2021). Such disparities highlight investment-based inequalities in preparedness and defense capabilities.

Greater investment in cybersecurity enhances national readiness and supports economic stability. Gordon et al. (2018) argue that nations with robust cybersecurity frameworks attract more foreign investment due to increased trust in digital infrastructure. Investment also supports workforce development, infrastructure upgrades, and real-time threat detection systems.

Studies have confirmed a strong link between underinvestment and data breach frequency. Organizations with inadequate funding tend to lack current technologies and employee training,

increasing susceptibility to cyberattacks (Neuhaus & Plattner, 2013). High-profile breaches often originate in systems that lack comprehensive security postures.

Economic models like the Gordon-Loeb model help estimate the ROI of cybersecurity spending. According to Rathod and Hämäläinen (2017), optimal spending should be a calculated proportion of expected loss from cyber incidents. Cost-benefit analyses further support evidence-based policymaking by weighing implementation costs against potential losses (Çifci, 2022).

Overall, strategic and well-calibrated investment in cybersecurity is not just a defense mechanism but a catalyst for economic resilience and institutional integrity. Indonesia must elevate its financial commitment to match its growing digital exposure.

Indonesia's escalating exposure to cyber threats reflects broader structural challenges typical of developing nations undergoing digital transformation. The results indicate that while regulatory initiatives and technological progress are in motion, several systemic barriers continue to inhibit a cohesive and effective national cybersecurity posture. These barriers, common across many developing countries, include financial limitations, skills shortages, fragmented policies, and cultural misperceptions regarding cybersecurity.

Financial constraints significantly affect the implementation of cybersecurity governance. Developing countries, including Indonesia, often prioritize urgent socio-economic issues such as healthcare, education, and poverty alleviation, resulting in limited budget allocations for cybersecurity infrastructure and personnel development (Tambunan, 2011; Perozzo et al., 2022). This underinvestment hampers the acquisition of advanced threat detection systems and the development of necessary human capital. Compounding this issue is the lack of technical expertise within both government institutions and private enterprises. Without skilled professionals to implement, manage, and enforce cybersecurity frameworks, even well-intentioned policies are unlikely to achieve their intended outcomes (Slayton, 2015).

Another layer of complexity arises from cultural attitudes and misconceptions. Many small and medium enterprises (SMEs) in Indonesia underestimate their exposure to cyber risks, believing they are unlikely targets for cybercriminals. This perception discourages them from taking proactive measures to secure their digital assets (Adriko & Nurse, 2024; Neyole et al., 2024). Research consistently shows that SMEs view cybersecurity as a cost rather than a strategic investment, particularly when they lack the financial health or organizational maturity to prioritize digital risk management (Pekarčík et al., 2024; Neri et al., 2023). Even SMEs that recognize the value of cybersecurity often face difficulties accessing affordable, scalable, and tailored solutions suited to their operational context (Irwandy et al., 2024; Özkan & Spruit, 2020). These challenges perpetuate a cycle of vulnerability, in which limited investment and awareness continue to expose smaller businesses to significant digital threats.

Institutional fragmentation is another persistent challenge in Indonesia's cybersecurity governance. Multiple agencies often operate in silos with overlapping responsibilities, leading to inefficient policy execution and reduced accountability (Neuhaus & Plattner, 2013; Manzoor et al., 2024). This lack of coordination hampers crisis response and creates opportunities for cybercriminals to exploit gaps in the system. Comparative studies suggest that integrated models of inter-agency collaboration, such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA), can

streamline strategic coordination across sectors and stakeholders. Indonesia's National Cyber and Crypto Agency (BSSN) represents a step in this direction, serving as a focal point for collaborative initiatives between public institutions and the private sector (Çifci, 2022). For BSSN to achieve greater impact, sustained inter-organizational communication, shared objectives, and joint implementation strategies are essential (Jaman et al., 2023).

Addressing these multifaceted challenges requires Indonesia to adopt a dynamic and adaptive policy framework. A static regulatory approach is ill-suited for a cybersecurity landscape that evolves with unprecedented speed. Flexible, risk-based governance models can enhance responsiveness to emerging threats and allocate resources more efficiently based on sectoral criticality and threat exposure (Neuhaus & Plattner, 2013). Continuous policy revision, informed by stakeholder consultations, threat intelligence, and global trends, is essential for effective governance. Engaging a wide range of stakeholders, including SMEs, cybersecurity professionals, and academic experts, will ensure that policy development is grounded in practical realities and emerging innovations (Carías et al., 2020).

The integration of adaptive learning into Indonesia's cybersecurity strategy is also crucial. This includes supporting research and development in cybersecurity technologies and fostering an ecosystem that encourages innovation. By enabling institutions to rapidly learn from incidents and adapt strategies accordingly, Indonesia can build resilience against both conventional and novel cyber threats (Irwandy et al., 2024; Pekarčík et al., 2024; Slayton, 2015).

In conclusion, Indonesia’s cybersecurity posture is at a critical juncture. The country must overcome systemic governance barriers, transform the perception of cybersecurity among SMEs, foster institutional coordination, and implement flexible, risk-aware policies. These efforts will require substantial investment, cultural transformation, and sustained cross-sector collaboration. As Indonesia continues to integrate digital technologies across its economy and governance structures, strengthening cybersecurity must become a parallel national priority.

CONCLUSION

This study has explored the significant escalation of cyber threats in Indonesia between 2020 and 2023, uncovering critical insights into the nation's cybersecurity posture, regulatory evolution, and systemic challenges. The findings reveal a stark increase in cyber incidents—from 88 million in 2020 to over 1.65 billion in 2021—driven by a combination of digital expansion, increased attack sophistication, and vulnerabilities across public and private sectors. These trends reflect broader global and regional dynamics, particularly in the wake of the COVID-19 pandemic, which created fertile ground for phishing, ransomware, and data breach incidents.

Despite Indonesia’s proactive steps in establishing cybersecurity regulations—such as BSSN Regulation No. 8/2020, Perpres 82/2022, and Perpres 47/2023—implementation gaps remain. Regulatory fragmentation, weak enforcement, and underfunding continue to impair national readiness. The country’s cybersecurity investment stands at just 0.02% of GDP, the lowest in ASEAN, signaling a critical misalignment between threat exposure and financial preparedness.

The research also highlights challenges faced by SMEs, which often underestimate cyber risks and lack resources for comprehensive security measures. Meanwhile, government agencies struggle with inter-institutional coordination, and regulatory policies fail to fully account for the dynamic nature of digital threats. These systemic and cultural challenges are consistent with those documented in other developing countries, pointing to a shared need for integrated, well-funded, and adaptive cybersecurity frameworks.

In terms of scientific contribution, this study provides a rare and comprehensive integration of quantitative cyber threat data and qualitative policy evaluation. It maps Indonesia's cyber threat trajectory alongside institutional responses and benchmarks these developments against regional and global standards. The inclusion of literature on machine learning, stakeholder engagement, and investment modeling adds further depth to the analysis.

Looking forward, the findings support several key recommendations: Indonesia must increase its cybersecurity budget, foster multi-stakeholder collaboration, and implement risk-based, adaptive policies. Emphasizing user awareness, SME support, and data-driven governance models will be critical for building resilience. Future research should examine micro-level case studies on regulatory efficacy, user behavior, and technological innovation in cyber defense.

Ultimately, as Indonesia moves toward greater digital integration, cybersecurity must transition from a peripheral concern to a central pillar of national development and governance.

REFERENCE

Beaman, C., Barkworth, A., Akande, T., Hakak, S., & Khan, M. (2021). *Ransomware: recent advances, analysis, challenges and future research directions.* Computers & Security, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490

Carías, J., Borges, M., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). *Systematic approach to cyber resilience operationalization in SMEs.* IEEE Access, 8, 174200–174221. https://doi.org/10.1109/access.2020.3026063

Çifci, H. (2022). *Comparison of national-level cybersecurity and cyber power indices: a conceptual framework.* https://doi.org/10.21203/rs.3.rs-2159915/v1

Chigada, J., & Madzinga, R. (2021). *Cyberattacks and threats during COVID-19: a systematic literature review.* SA Journal of Information Management, 23(1). https://doi.org/10.4102/sajim.v23i1.1277

Chimezie, O., Akagha, O., Dawodu, S., Anyanwu, A., Onwusinkwue, S., & Ahmad, I. (2024). *Comprehensive review on cybersecurity: modern threats and advanced defense strategies.* Computer Science & IT Research Journal, 5(2), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

Cross, C., & Holt, T. (2021). *Responding to cybercrime: results of a comparison between community members and police personnel.* https://doi.org/10.52922/ti78207

Dedeke, A., & Masterson, K. (2019). *Contrasting cybersecurity implementation frameworks (CIF) from three countries.* Information and Computer Security, 27(3), 373–392. https://doi.org/10.1108/ics-10-2018-0122

Drew, J. (2020). *A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies.* Journal of Criminological Research Policy and Practice, 6(1), 17–33. https://doi.org/10.1108/jcrpp-12-2019-0070

Drew, J., & Farrell, L. (2018). *Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs.* Police Practice and Research, 19(6), 537–549. https://doi.org/10.1080/15614263.2018.1507890

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

Fissel, E., & Lee, J. (2023). *The cybercrime illusion: examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness.* Journal of Criminology, 56(2–3), 150–169. https://doi.org/10.1177/26338076231174639

García-Pérez, A., Sallos, M., & Tiwasing, P. (2021). *Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective.* Journal of Intellectual Capital, 24(2), 465–486. https://doi.org/10.1108/jic-06-2021-0166

Gordon, L., Loeb, M., Lucyshyn, W., & Zhou, L. (2018). *Empirical evidence on the determinants of cybersecurity investments in private sector firms.* Journal of Information Security, 9(2), 133–153. https://doi.org/10.4236/jis.2018.92010

Hadlington, L., & Chivers, S. (2018). *Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors.* Policing: A Journal of Policy and Practice, 14(2), 479–492. https://doi.org/10.1093/police/pay027

Holt, T., & Lee, J. (2019). *Policing cybercrime through law enforcement and industry mechanisms.*, 644–662. https://doi.org/10.1093/oxfordhb/9780198812746.013.34

Irwandy, I., Mangilep, A., Anggraeni, R., Noor, N., Niartiningsih, A., & Latifah, N. (2024). *Cybersecurity culture among healthcare workers in Indonesia: knowledge gaps, demographic influences, and strategic policy solutions.* https://doi.org/10.21203/rs.3.rs-5421169/v1

Ispahany, J., Islam, R., Islam, M., & Khan, M. (2024). *Ransomware detection using machine learning: a review, research limitations and future directions.* IEEE Access, 12, 68785–68813. https://doi.org/10.1109/access.2024.3397921

Jaman, U., Lubis, A., & Suhartono, S. (2023). *Legal challenges in the development of information and communication technology SMEs in Jabodetabek region, Indonesia.* West Science Law and Human Rights, 1(04), 149–156. https://doi.org/10.58812/wslhr.v1i04.321

Kamal, A., Yen, C., Ping, M., & Zahra, F. (2020). *Cybersecurity issues and challenges during COVID-19 pandemic.* https://doi.org/10.20944/preprints202009.0249.v1

Kaur, M., & Saini, M. (2022). *Indian government initiatives on cyberbullying: a case study on cyberbullying in Indian higher education institutions.* Education and Information Technologies, 28(1), 581–615. https://doi.org/10.1007/s10639-022-11168-4

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O., & Vergara, R. (2022). *A systematic literature review on cybercrime legislation.* F1000Research, 11, 971. https://doi.org/10.12688/f1000research.123098.1

Krishna, B., & M.P., S. (2021). *Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis.* Information and Computer Security, 29(5), 737–760. https://doi.org/10.1108/ics-12-2020-0205

Lee, J., Holt, T., Burruss, G., & Bossler, A. (2019). *Examining English and Welsh detectives' views of online crime.* International Criminal Justice Review, 31(1), 20–39. https://doi.org/10.1177/1057567719846224

Malik, M., & Islam, U. (2019). *Cybercrime: an emerging threat to the banking sector of Pakistan.* Journal of Financial Crime, 26(1), 50–60. https://doi.org/10.1108/jfc-11-2017-0118

Manzoor, J., Waleed, A., Jamali, A., & Masood, A. (2024). *Cybersecurity on a budget: evaluating security and performance of open-source SIEM solutions for SMEs.* PLOS ONE, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

Maphosa, V. (2024). *An overview of cybersecurity in Zimbabwe's financial services sector.* F1000Research, 12, 1251. https://doi.org/10.12688/f1000research.132823.2

Mupila, F., Gupta, H., & Bhardwaj, A. (2023). *An empirical study on cyber crimes and cybersecurity awareness.* https://doi.org/10.21203/rs.3.rs-3037289/v1

Naidoo, R. (2020). *A multi-level influence model of COVID-19 themed cybercrime.* European Journal of Information Systems, 29(3), 306–321. https://doi.org/10.1080/0960085x.2020.1771222

Neuhaus, S., & Plattner, B. (2013). *Software security economics: theory, in practice.*, 75–92. https://doi.org/10.1007/978-3-642-39498-0_4

Neyole, J., Okwiri, S., & Mapema, N. (2024). *Exploring the impact of cybersecurity threats on small and medium enterprises' performance: a case study of Kajiado County, Kenya.* https://doi.org/10.20944/preprints202411.0237.v1

Neri, M., Niccolini, F., & Martino, L. (2023). *Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment.* Information and Computer Security, 32(1), 38–52. https://doi.org/10.1108/ics-05-2023-0084

Neri, M., Niccolini, F., & Pugliese, R. (2022). *Assessing SMEs' cybersecurity organizational readiness: findings from an Italian survey.* Online Journal of Applied Knowledge Management, 10(2), 1–22. https://doi.org/10.36965/ojakm.2022.10(2)1-22

Ngo, F., Piquero, A., LaPrade, J., & Duong, B. (2020). *Victimization in cyberspace: is it how long we spend online, what we do online, or what we post online?* Criminal Justice Review, 45(4), 430–451. https://doi.org/10.1177/0734016820934175

Odimarha, A., Ayodeji, S., & Abaku, E. (2024). *Securing the digital supply chain: cybersecurity best practices for logistics and shipping companies.* World Journal of Advanced Science and Technology, 5(1), 026–030. https://doi.org/10.53346/wjast.2024.5.1.0030

Ofoegbu, K., Osundare, O., Ike, C., Fakeyede, O., & Ige, A. (2024). *Proactive cyber threat mitigation: integrating data-driven insights with user-centric security protocols.* Computer Science & IT Research Journal, 5(8), 2083–2106. https://doi.org/10.51594/csitrj.v5i8.1493

Ogunjimi, O., Afoloeunsho, A., & Olukomoro, O. (2018). *Elicitation of SME requirements for cybersecurity solutions through adherence to recommendations.* Advances in Multidisciplinary & Scientific Research Journal Publication, 6(2), 29–34. https://doi.org/10.22624/aims/maths/v6n2p4

Özkan, B., & Spruit, M. (2020). *Cybersecurity standardisation for SMEs.*, 1252–1278. https://doi.org/10.4018/978-1-7998-7705-9.ch056

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

Pike, A., Adams, W., Huggins, R., Mazerolle, S., & Casa, D. (2019). *Analysis of states' barriers to and progress toward implementation of health and safety policies for secondary school athletics.* Journal of Athletic Training, 54(4), 361–373. https://doi.org/10.4085/1062-6050-28-18