CYBERSECURITY POLICIES DIFFERENCES IN INDONESIA A SYSTEMATIC LITERATURE REVIEW OF PUBLIC AND PRIVATE SECTOR

Rahmat Rambe[*], Mochamad Teguh Kurniawan[*]
[*]*Department of Information System, School of Industrial Engineering, Bandung, Indonesia,*
gyurahmat@student.telkomuniversity.ac.id, teguhkurniawan@telkomuniversity.ac.id

Email Correspondence : teguhkurniawan@telkomuniversity.ac.id

Received : July 28, 2025 Accepted : January 28, 2026 Published : June 30, 2026

Abstract: Rapid digital transformation has increased the reliance of various sectors on information technology, while simultaneously giving rise to increasingly complex cybersecurity risks. Threats such as malware, ransomware, and attacks on critical infrastructure not only result in economic losses but can also disrupt national stability and undermine public trust. In this context, both the public and private sectors play crucial roles through their implemented cybersecurity policies. The public sector, represented by institutions such as the National Cyber and Crypto Agency (BSSN), has a primary mandate to safeguard public interests and national resilience through a top-down approach based on formal regulations. Meanwhile, the private sector is more driven by market demands, the need for innovation, and efforts to maintain customer trust. Therefore, its cybersecurity policies tend to be adaptive, adopting international standards such as ISO/IEC 27001 or the NIST Cybersecurity Framework. This study uses a descriptive-qualitative method with a Systematic Literature Review (SLR) approach to identify, evaluate, and synthesize findings from scientific journals, national policy documents, and recent cybersecurity reports. The results reveal fundamental differences in motivation, governance, and risk mitigation strategies between the public and private sectors in Indonesia. The public sector places greater emphasis on legal compliance and protecting vital infrastructure, while the private sector focuses more on speed of response and protecting business reputation. However, both sectors face similar challenges, such as limited cybersecurity expertise, technology adoption gaps, and weak cross-institutional coordination. This study recommends strengthening public-private collaboration through strategic partnerships to comprehensively and sustainably enhance national cybersecurity resilience.
Keywords: cybersecurity; public policy; public sector; private sector; digital risks; mitigation strategies

Abstrak: Percepatan transformasi digital meningkatkan ketergantungan berbagai sektor pada teknologi informasi sekaligus memperluas kompleksitas risiko siber. Ancaman seperti malware, ransomware, dan serangan terhadap infrastruktur kritis tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam stabilitas negara serta kepercayaan publik. Dalam situasi ini, sektor publik dan swasta berperan penting melalui kebijakan keamanan siber. Sektor publik, melalui lembaga seperti Badan Siber dan Sandi Negara, bertugas melindungi kepentingan masyarakat dan ketahanan nasional dengan

pendekatan top-down berbasis regulasi. Sebaliknya, sektor swasta didorong kebutuhan pasar, inovasi, dan kepercayaan pelanggan sehingga kebijakannya lebih adaptif dengan standar internasional seperti ISO/IEC 27001 dan NIST Framework. Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan SLR untuk menelaah dan mensintesis temuan dari jurnal, dokumen kebijakan, dan laporan terbaru. Hasil menunjukkan perbedaan mendasar pada motivasi, tata kelola, dan mitigasi risiko di Indonesia: sektor publik menitikberatkan kepatuhan hukum serta perlindungan infrastruktur vital, sedangkan sektor swasta pada respons cepat dan reputasi bisnis. Meski demikian, keduanya menghadapi kendala serupa berupa keterbatasan ahli, kesenjangan teknologi, dan lemahnya koordinasi. Studi ini merekomendasikan penguatan kemitraan publik-swasta guna memperkuat ketahanan siber nasional secara berkelanjutan.

Kata Kunci: keamanan siber; kebijakan publik; sektor publik; sektor swasta; risiko digital; strategi mitigasi

Recommended APA Citation :

Rambe, R. & Kurniawan, M. T. (2026). Cybersecurity Policies Differences in Indonesia A Systematic Literature Review of Public and Private Sector. *Elkawnie*, *12*(1), 1-13. https://doi.org/10.22373/ekw.v12i1.31730

Introduction

In the era of rapid digital transformation, nearly all aspects of people's lives are connected through information technology. Organizations across various sectors are increasingly relying on digital systems to support business processes, public services, and even daily activities (Afrilia et al., 2024). This has led to the emergence of a new paradigm in which data has become a strategic asset that can drive economic growth, bureaucratic efficiency, and innovation in public and private services. However, this high reliance on technology also increases exposure to cybersecurity risks. Threats such as malware, ransomware, distributed denial of service (DDoS) attacks, and sensitive data leaks can not only cause significant financial losses but also undermine social stability and public trust(Wibowo et al., 2025) .

In this context, cybersecurity has evolved into a strategic issue that is inseparable from efforts to maintain the sustainability of the economic system and national resilience. Cyberattacks targeting vital infrastructure such as electricity grids, transportation, healthcare, and government systems can paralyze public services and trigger a broader social crisis. Therefore, cyber risk management is a critical priority that requires serious and structured handling.

In response to these challenges, two main groups of actors have emerged with significant responsibility for developing and implementing cybersecurity policies: the public and private sectors. The existence of these two sectors stems from their distinct roles and objectives within the national ecosystem. (Sutra & Haryanti, 2023). Regulations such as the Personal Data Protection Law (PDP Law), Presidential Regulation No. 47 of 2023 concerning the National Cybersecurity Strategy, and the implementation of the ISO/IEC 27001 standard within the

government demonstrate the strong top-down approach adopted by this sector. This approach emphasizes the importance of legal compliance, strict bureaucracy, and accountability in every security measure.

On the other hand, the private sector, which includes technology companies, e-commerce companies, digital banking companies, and startups, operates primarily with the goal of generating profits and maintaining business sustainability amidst intense market competition. This motivation makes them more flexible and adaptive in managing cybersecurity risks. Companies like Tokopedia and other fintech entities such as BliBli,, GoPay, OVO, DANA generally adopt global standards like ISO/IEC 27001, PCI DSS for the financial industry, or the NIST Cybersecurity Framework. They also utilize innovative technologies like artificial intelligence for early detection, advanced encryption, and even the creation of real-time Security Operation Center (SOC) teams (Soesanto et al., 2023). Thus, the private sector's approach is more bottom-up and driven by the need to maintain customer trust, protect reputations, and meet the demands of global partners.

The fundamental differences between the public and private sectors in formulating cybersecurity policies can be traced to their institutional objectives. The public sector is focused on collective interests and national stability, leading to a highly regulatory orientation, while the private sector is driven by market dynamics and the need for rapid innovation (Mulyani & Rulandari, 2024). As a result, despite facing similar types of cyber threats, their mitigation strategies, resource allocation, and decision-making patterns often differ significantly. The public sector is bound by lengthy formal procedures, resulting in a relatively slow response to incidents, but guaranteeing high levels of control and accountability. In contrast, the private sector can quickly implement security measures or post-incident recovery due to its streamlined bureaucratic processes (Gordon et al., 2018).

However, amidst the ever-evolving complexity and cross-border nature of cyber threats, these two sectors cannot operate in isolation. Cross-sector collaboration through public-private partnership (PPP) schemes is a global trend that continues to be strengthened. Several international policies have even begun to mandate the exchange of threat intelligence, incident reporting within 72 hours, the implementation of the Zero Trust Architecture framework, and the harmonization of data protection standards such as GDPR or NIS2 in Europe (Trocoso-Pastoriza et al., 2022). In Indonesia, although the National Cyber and Cyber Security Agency (BSSN) has encouraged the formation of CSIRT teams in every government agency and invited the private sector to participate in various training programs, challenges in cross-institutional coordination, limited human resources, and gaps in technology adoption remain major obstacles (Romadhon & Salman, 2025).

Based on this background, this research focuses on critically analyzing the effectiveness of cybersecurity policies implemented by the public and private sectors in Indonesia. The case study will focus on the National Cyber and Crypto

Agency (BSSN) as a representative of the public sector, and Tokopedia as an example of the private sector. This research is expected to comprehensively illustrate the differences in approaches, challenges faced, and potential for strategic collaboration between the two sectors to strengthen national cyber resilience. Therefore, the research problem formulation includes two main questions aimed at exploring the differences and challenges faced in the implementation of cybersecurity policies. What are the characteristics of cybersecurity policies implemented in the public and private sectors in Indonesia? And what are the challenges faced by both sectors in implementing cybersecurity policies?

This research is structured as follows: Chapter II discusses the literature review, Chapter III explains the research methodology, Chapter IV presents the results and discussion, and Chapter V contains the final conclusions.

Literature Review

Digital transformation has brought fundamental changes to the way public and private organizations manage business processes and provide services to the public. The increasingly widespread use of information systems across various sectors has led to a high dependence on digital infrastructure, increasing exposure to cybersecurity risks. Threats such as malware, ransomware, Distributed Denial of Service (DDoS) attacks, and sensitive data leaks can cause significant economic losses and disrupt social stability (Rahakbauw, 2024). Therefore, cybersecurity policy is no longer viewed solely as a technical endeavor but has evolved into a crucial part of organizational governance that requires a multidisciplinary approach(Ikhsanni & et al, 2024).

From an organizational behavior perspective, the Theory of Planned Behavior (TPB) developed by Ajzen (1991) provides a relevant theoretical framework for analyzing individual compliance with cybersecurity policies. The TPB explains that an individual's behavior is influenced by intentions, which are formed through three main factors: attitudes toward an action, subjective norms, and perceived control over the behavior (Ajzen, 1991). In practice, this theory is often used to assess how employee attitudes toward risk, work environment pressures, and ease of implementing security procedures influence their compliance with organizational policies (Parikh & Nimbekar, 2023).

From a governance perspective, the international standard ISO/IEC 27001 is a key reference for developing an Information Security Management System (ISMS). ISO/IEC 27001:2022 requires organizations to systematically identify information assets, assess threats and vulnerabilities, and then evaluate the level of risk to formulate appropriate security controls (International Organization for Standardization, 2022). This standard is based on the PDCA (Plan-Do-Check-Act) cycle, which ensures continuous policy implementation through the stages of planning, implementation, evaluation, and improvement. Annex A of ISO/IEC 27001 contains 93 security controls grouped into four broad themes: organizational

controls (e.g., security policies and third-party management), people controls (staff training and awareness), physical controls (facility security), and technological controls (encryption, identity management, malware detection, logging) (Culot et al., 2021). This standard is also compatible with ISO/IEC 27701 for privacy management and supports compliance with data protection regulations such as the European GDPR and the Indonesian Data Protection Act. Another advantage of ISO/IEC 27001 is its generic nature, making it applicable to government agencies and private companies across sectors. Implementation of this certification also increases trust among global partners and is a requirement for international contracts, as has been done by Indonesian companies like Tokopedia (Loviana, 2022).

In addition to ISO/IEC 27001, the NIST Cybersecurity Framework is also widely used as a practical guide for managing cybersecurity. This framework divides protection activities into five key functions: identification, protection, detection, response, and recovery (Rose et al., 2020). This approach facilitates organizations in establishing scalable threat response procedures and ensuring the restoration of critical services after an attack.

In the context of cybersecurity policy, there are fundamental differences in character between public and private sector organizations. In the public sector, cybersecurity is positioned as an integral part of safeguarding public interests and national stability. This is evident in the mandate of institutions such as the National Cyber and Crypto Agency (BSSN), which formulates a national strategy through Presidential Regulation No. 47 of 2023 and issues derivative regulations, such as BSSN Regulation No. 1 of 2024 concerning cyber incident management (Ramadhianto et al., 2023). The public sector approach tends to be top-down, bureaucratic, and highly regulatory, which, while ensuring accountability, can lead to relatively slow decision-making (Alfikri et al., 2022). Field implementation requires each ministry/institution to establish a Computer Security Incident Response Team (CSIRT) to monitor incidents, while compliance audits are conducted by state supervisory agencies such as the Financial and Development Supervisory Agency (BPKP) (Triwahyuni et al., 2024).

In contrast, private sector organizations such as technology companies, e-commerce companies, or financial services companies position cybersecurity policies within the framework of protecting business continuity and maintaining market confidence. The primary motivation stems from the need to maintain reputation, meet global standards, and ensure smooth operations to maintain a competitive advantage(Romanosky et al., 2022). Many private companies have voluntarily adopted ISO/IEC 27001 or PCI DSS, established 24/7 internal Security Operation Centers (SOCs), and conducted regular audits by independent parties such as EY or KPMG to achieve international compliance (Opeyemi Babatunde et al., 2025). In Indonesia, for example, Tokopedia has obtained ISO/IEC 27001 certification to strengthen user data protection (Loviana, 2022).

Globally, several policy trends are influencing the direction of cybersecurity policy in both sectors. One such trend is the implementation of Zero Trust Architecture, which rejects the "trust but verify" assumption and replaces it with "never trust, always verify," requiring strict authentication and authorization for every access request (Rose et al., 2020). Data protection regulations are also becoming stricter with the introduction of the GDPR in Europe and the NIS2 Directive, which expands risk management obligations to critical sectors and mandates incident reporting within a maximum of 72 hours (Seeba et al., 2025). Furthermore, collaboration through public-private partnerships (PPPs) is increasingly emphasized to facilitate the exchange of threat intelligence and technical resources across sectors. Indonesia also needs to strengthen such schemes to accelerate attack detection and response (Arianto & Anggraini, 2019).

Research Methods

This research uses a descriptive-qualitative approach aimed at gaining an in-depth understanding of cybersecurity policies implemented in the public and private sectors in Indonesia, while also identifying differences in characteristics, challenges, and potential for strategic collaboration between the two in building national cyber resilience. To achieve this objective, this research utilizes the Systematic Literature Review (SLR) method designed to systematically identify, evaluate, and synthesize previous research results, international standards, policy documents, and institutional reports relevant to the topic.

The search was conducted using primary keywords such as "cybersecurity policy," "public sector and private sector," "ISO/IEC 27001," "NIST Cybersecurity Framework," "Zero Trust," "GDPR," and "cyber risk management," focusing on publications published between 2020 and 2025 to ensure the topic's freshness.

Table 1. Journal Source and Keywords

Journal Source	Keywords
Scopus	Cybersecurity policy
ScienceDirect	public sector and private sector
SpringerLink	ISO/IEC 27001
ProQuest	NIST Cybersecurity Framework
Garuda	Zero Trust, GDPR
Sinta	Cyber risk management

Table 2. Publication Published Year

Publication Published Year
2020-2025

The initial search process yielded a total of 78 articles and documents identified as relevant to the study topic. Subsequent abstract and preliminary

screening were conducted to ensure alignment with the research focus, which were then narrowed down to 42 articles based on inclusion criteria: scientific publications (journal articles or proceedings) or official policy documents, available in English or Indonesian, and explicitly discussing cybersecurity policy, ISMS governance, or a comparison between public and private sector approaches. Articles lacking a strong methodological foundation, being popular opinion pieces, or solely discussing technical aspects without a policy dimension were eliminated at this stage.

The next step was to fully read the selected articles to conduct an in-depth analysis of the context, findings, and conclusions of each study. This resulted in 23 final journals and documents used as primary sources in this study. The data obtained were then analyzed through data reduction stages by grouping the findings into major themes according to the theoretical framework, namely the theory of planned behavior (TPB), cyber risk management, governance frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework, characteristics of policies in the public sector, private sector approaches, and global trends including Zero Trust Architecture, GDPR, NIS2 Directive, and public-private partnerships schemes. All analysis results were then compiled into a descriptive narrative to comprehensively describe the differences, challenges, and opportunities for synergy between the public and private sectors in building a robust cybersecurity ecosystem in Indonesia.

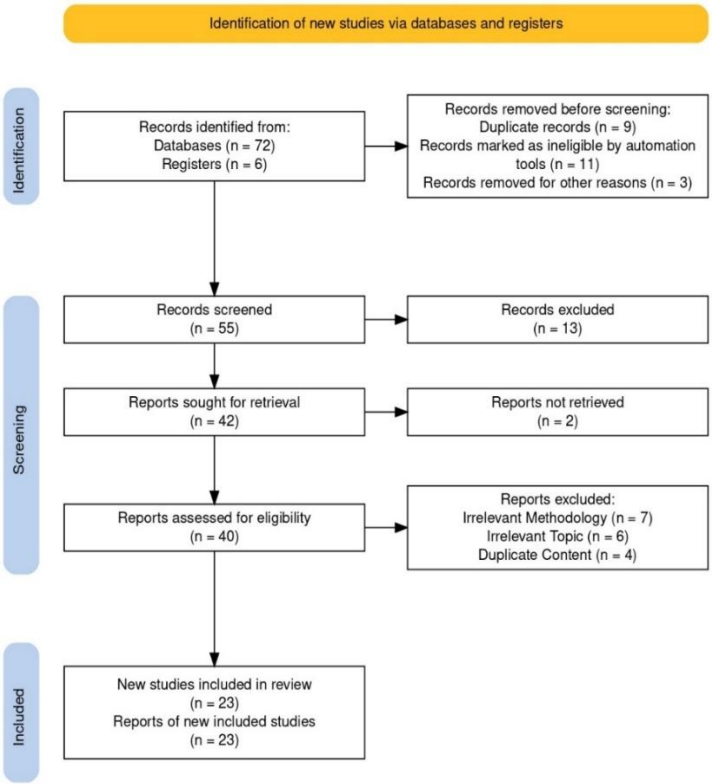


Figure 1. Analysis with PRISMA

Results And Discussion

Research results obtained from integrating primary document reviews and a systematic literature review (SLR) of 23 journals and policy documents revealed several key findings regarding differences in cybersecurity policy approaches between the public and private sectors in Indonesia. The analysis shows that public sector organizations, such as ministries and government agencies, generally manage cybersecurity through a top-down approach with a strict bureaucratic structure. The primary impetus arises from formal regulatory mandates, such as Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy, as outlined in various regulations of the National Cyber and Crypto Agency (BSSN), which mandates the establishment of a Computer Security Incident Response Team (CSIRT) in each agency. This approach ensures cross-agency compliance with minimum data security standards, while also ensuring a structured reporting mechanism and audits by state institutions such as the Financial and Development Supervisory Agency (BPKP). However, this hierarchical process often results in relatively slow response to incidents.

In contrast, private sector companies, particularly in the digital technology and finance sectors, are developing more bottom-up and adaptive cybersecurity policies. The primary driving factors are the need to maintain business continuity, market reputation, and meet global security standards required by international cooperation contracts. Companies like Tokopedia and Gojek are known to have comprehensively implemented ISO/IEC 27001, have 24/7 Security Operation Centers (SOCs) to detect and mitigate cyberattacks in real time, and regularly undergo independent audits by global auditors to ensure compliance with international standards (Loviana, 2022; Opeyemi et al., 2025). This allows the private sector approach to respond more quickly to dynamic attacks, with a high degree of decision flexibility due to being less tied to internal bureaucracy.

Table 3. Comparison of Public and Private Sector Standards and Approaches

Aspects	Public Sector	Private Sector
Regulations	Presidential Regulation No. 47/2023, PDP Law, BSSN	Optional, as needed for global contracts
Standards	Standards adjusted, BPKP audits	ISO/IEC 27001, PCI, DSS, NIST Framework
Objectives	Legal compliance, national stability,	Reputation, consumer trust, ROI
Approached	Top-down, procedural, strict bureaucracy,	Bottom-up, risk-based, adaptive
Audit/Evaluation	Conducted by state institutions (BPKP)	Independent auditors (EY, KPMG)

Table 4. Public Table of Cyber Incidents, Recovery Time, and Dominant Attack Types (2019-2024)

Year	Public Incident	Public Recovery	Public Dominant Attack
2019	120	76	*Phising, Malware*
2020	140	72	*Ransomware, DDoS*
2021	160	68	*Phising, SQL, Injection*
2022	180	65	*Zero-day Exploit, DDoS*
2023	200	62	*Insider Threat, Malware*
2024	220	62	*Ransomware, Suppy Chain*

Table 5. Private Table of Cyber Incidents, Recovery Time, and Dominant Attack Types (2019-2024)

Year	Private Incident	Private Recovery	Private Dominant Attack
2019	95	68	*Phising, Malware*
2020	130	65	*Ransomware, DDoS*
2021	155	61	*Phising, SQL, Injection*
2022	170	57	*Zero-day, Bussiness Email Compromise*
2023	190	52	*Malware, Supply Chain*
2024	210	48	*Ransomware, Suppy Chain*

A review of 23 journal articles and final documents supports this pattern. Approximately 15 articles confirm that public sector organizations generally place greater emphasis on regulatory controls and procedural audits, while eight others indicate that the private sector prioritizes a risk-based approach and global certifications such as ISO/IEC 27001 and PCI DSS. A review of 23 journal articles and final documents supports this pattern. Approximately 15 articles confirm that public sector organizations generally place greater emphasis on regulatory controls and procedural audits, while eight others indicate that the private sector prioritizes a risk-based approach and global certifications such as ISO/IEC 27001 and PCI DSS primarily to protect business reputation, ensure service continuity, and maintain consumer trust. Nearly half of the reviewed literature further highlights the growing relevance of Zero Trust Architecture, which redefines cybersecurity assumptions by treating all access points as untrusted until continuously verified, thereby responding to the increasing sophistication of modern cyber threats (NIST, 2020; Wang & Wang, 2024).

At the same time, regulatory developments at the international level, particularly the European Union's GDPR and NIS2 Directive, are gradually emerging as benchmarks for cross-border cooperation and digital contracts, indirectly shaping the cybersecurity policies of Indonesian organizations that operate within global value chains. The IndoSecSummit (2024) literature also underscores the strategic importance of public–private partnerships (PPPs) in enhancing threat intelligence sharing and improving cross-sector incident mitigation efficiency. Viewed through the lens of the research problem formulation, these findings clarify how cybersecurity policies are characterized and operationalized differently across sectors. In addressing the first research question, the public sector is shown to adopt a governance-oriented model in which

cybersecurity is institutionalized as a state responsibility, structured through statutory mandates, hierarchical authority, and standardized procedures issued by central institutions such as BSSN.

Thus, although the public and private sectors in Indonesia exhibit different motivations, policy patterns, standards, and response speeds, both face challenges such as limited cybersecurity expertise and the urgent need to adapt to the evolving global threat landscape. In relation to the second research question, the findings reveal that both sectors face substantial implementation challenges, although their nature differs. Public sector organizations are primarily constrained by bureaucratic rigidity, limited inter-agency coordination, and a persistent shortage of specialized cybersecurity professionals, which weakens the translation of well-established regulatory frameworks into effective operational practices. Lengthy procurement procedures, budgetary constraints, and centralized decision-making further impede rapid responses to emerging threats, particularly in cases involving zero-day exploits or supply chain attacks that demand immediate technical intervention.

Meanwhile, private sector organizations grapple with escalating threat complexity, high cybersecurity investment costs, and uneven levels of maturity across industries, where large corporations may operate advanced SOCs while small and medium-sized enterprises struggle with limited resources. Competition for skilled cybersecurity personnel further exacerbates workforce instability and operational costs, while ongoing regulatory evolution at both national and international levels introduces additional uncertainty. Taken together, these findings indicate that despite significant differences in motivation, governance structures, standards, and response speeds, the public and private sectors are increasingly exposed to interdependent cyber risks that transcend organizational and sectoral boundaries. Consequently, the effectiveness of national cybersecurity policy depends not solely on sector-specific strengths but also on the depth of coordination and collaboration between sectors, reinforcing the strategic importance of public–private partnerships as a mechanism to integrate regulatory authority, technological capability, and operational agility in order to build comprehensive and sustainable national cyber resilience

Conclusions

This study concludes that there are fundamental differences in cybersecurity policies between the public and private sectors in Indonesia. The public sector emphasizes compliance with national regulations, with a structured, top-down approach that is often slow to respond to incidents. Meanwhile, the private sector is more adaptive, prioritizing reputation protection and market trust through international certification and the existence of an internal SOC that accelerates mitigation, as evidenced by a shorter average recovery time of approximately 58 hours compared to the public sector's average of 67 hours.

The study also shows that cyberattacks are evolving from phishing and malware to more complex threats such as zero-day exploits and supply chain attacks, demanding greater preparedness from both sectors. Therefore, strategic collaboration between the public and private sectors is crucial to combine regulatory strengths, technology, and response capacity to address the ever-changing threat landscape, while simultaneously building sustainable national cyber resilience.

Conflict of Interest

Rahmat Rambe lead all core aspects of the study, including formulating the research concept, conducting the literature review, designing the methodology, analyzing the data, interpreting the findings, and drafting the manuscript. Mochamad Teguh Kurniawan was involved exclusively in managing the journal submission process to the publisher and had no role in the study design, data acquisition, analytical procedures, result interpretation, or manuscript development. The authors confirm that no conflicts of interest exist in relation to this publication. Artificial Intelligence (AI) tools were utilized only to enhance language clarity and grammatical accuracy and did not affect the scholarly content, analytical processes, or conclusions. Responsibility for the final manuscript rests entirely with the authors.

Acknowledgements

The authors sincerely thank Mochamad Teguh Kurniawan for his meaningful involvement in various stages of this study, including assistance with organizing references, supporting the data synthesis process, and helping prepare the manuscript prior to submission. He also played an important role in coordinating the journal submission to the publisher, which significantly supported the overall publication process. In addition, the authors extend their appreciation to all individuals and institutions who contributed support during the development of this research. This study was conducted without financial support from any public, commercial, or non-profit funding bodies, and all work was carried out independently by the authors.

References

Afrilia, U. A., Mumpuni, A. P., Asy'ary, H., Muhdiarta, U., Mayasari, Y., & Anangkota, M. (2024). *Transforming Public Services: The Role Of Digital Innovation In Indonesian Municipal Governance* (Vol. 16, Issue 1).

Ajzen, I. (1991). The Theory Of Planned Behavior. *Organizational Behavior And Human Decision Processes*, *50*(2), 179–211. Https://Doi.Org/10.1016/0749-5978(91)90020-T

Alfikri, M., Ahmad, I., & Pertahanan, U. (2022). *The Implementation Of Policy For The Establishment Of A Cyber Incident Response Team To Support*

Information Security In The Government Sector. *6*(1), 1–13. Https://Doi.Org/10.21787/Mp.6.1.2022.1-13

Arianto, A. R., & Anggraini, G. (2019). *Building Indonesia's National Cyber Defense And Security To Face The Global Cyber Threats Through Indonesia Security Incident Response Team On Internet Infrastructure (Id-Sirtii)*. Http://M.News.Viva.Co.Id/News/Read/507480-

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The Iso/Iec 27001 Information Security Management Standard: Literature Review And Theory-Based Research Agenda. In *Tqm Journal* (Vol. 33, Issue 7, Pp. 76–105). Emerald Group Holdings Ltd. Https://Doi.Org/10.1108/Tqm-09-2020-0202

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence On The Determinants Of Cybersecurity Investments In Private Sector Firms. *Journal Of Information Security*, *09*(02), 133–153. Https://Doi.Org/10.4236/Jis.2018.92010

Ikhsanni, A., & Et Al. (2024). Cybersecurity Dan Tata Kelola Intelijen. *Jurnal Kajian Stratejik Ketahanan Nasional*, *7*(1). Https://Doi.Org/10.7454/Jkskn.V7i1.10086

International Organization For Standardization. (2022). *Iso/Iec 27001:2022 – Information Security, Cybersecurity And Privacy Protection — Information Security Management Systems — Requirements* ((3rd Ed.)). Iso.

Loviana, K. (2022). Cybersecurity And Cyber Resilience In Indonesia: Challenges And Opportunities. *Center For Digital Society*.

Mulyani, S., & Rulandari, N. (2024). Comparison Of Human Resource Management Characteristics Between Public Sector And Private Sector In Indonesia In The Era Of Digital Transformation. *Journal Of Public Administration And Political Science And International Relations, 2 (2)*. Https://Doi.Org/10.61978/Politeia.V2i2

Opeyemi Babatunde, G., Damilola Mustapha, S., Ike, C. C., Alabi, A. A., & Babatunde, G. O. (2025). A Holistic Cyber Risk Assessment Model To Identify And Mitigate Threats In Us And Canadian Enterprises. *Article In International Journal Of Multidisciplinary Research And Growth Evaluation*. Https://Doi.Org/10.54660/.Ijmrge.2025.6.1.773-787

Parikh, V., & Nimbekar, M. (2023). Socializing The Impact: An Analysis Of The Theory Of Planned Behavior's Influence On Increasing University Students' Cybersecurity Awareness. *Journal Of Community Development*, *4*(2), 139–156. Https://Doi.Org/10.47134/Comdev.V4i2.162

Rahakbauw, I. (2024). Analisis Potensi Ancaman Siber Pada Bidang Ekonomi Di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *7*(2). Https://Doi.Org/10.7454/Jkskn.V7i2.10097

Ramadhianto, R., Toruan, T. S. L., Kertopati, S. N. H., & Almubaroq, H. Z. (2023). Analysis Of Presidential Regulations Concerning Cyber Security To Bolster

Defense Policy Management. *Defense And Security Studies*, *4*, 84–93. Https://Doi.Org/10.37868/Dss.V4.Id244

Romadhon, F. W., & Salman, M. (2025). Pengembangan Skenario Serangan Siber Untuk Pelatihan Tim Tanggap Insiden Siber Pemerintah Daerah Menggunakan Framework Mitre Att&Ck Dan Cyber Kill Chain. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(5), 1265–1279. Https://Doi.Org/10.52436/1.Jpti.715

Romanosky, S., Schwindt, K., & Johnson, R. (2022). *Comparison Of Public And Private Sector Cybersecurity And It Workforces*.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. Https://Doi.Org/10.6028/Nist.Sp.800-207

Seeba, M., Valgre, M., & Matulevičius, R. (2025). *Evaluating Organization Security: User Stories Of European Union Nis2 Directive*. Http://Arxiv.Org/Abs/2504.19222

Soesanto, & Et Al. (2023). Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Menigkatkan Proteksi Data Dan Privasi Pengguna. *Jurnal Kewirausahaan Dan Manajemen Bisnis*, *1*(1).

Sutra, S., & Haryanti, A. (2023). Upaya Peningkatan Keamanan Siber Indonesia Oleh Badan Siber Dan Sandi Negara (Bssn) Tahun 2017-2020. *Global Political Studies Journal*, *7 (1)*, 56.

Triwahyuni, D., Putri, S. O., & Nurjati, F. S. (2024). *The Role Of Indonesia's National Cyber And Crypton Agency In Dealing With The Increase In Cybercrime At The Beginning Of The Covid-19 Pandemic* (Pp. 13–22). Https://Doi.Org/10.2991/978-2-38476-269-9_3

Trocoso-Pastoriza, J. R., Mermoud, A., Bouyé, R., Marino, F., Bossuat, J.-P., Lenders, V., & Hubaux, J.-P. (2022). *Orchestrating Collaborative Cybersecurity: A Secure Framework For Distributed Privacy-Preserving Threat Intelligence Sharing*. Http://Arxiv.Org/Abs/2209.02676

Wibowo, B., Luqman Hafiz, & Hidayat, T. (2025). Unveiling The Cybercrime Ecosystem: Impact Of Ransomware-As-A-Service (Raas) In Indonesia. *International Journal Of Science Education And Cultural Studies*, *4*(1), 11–21. Https://Doi.Org/10.58291/Ijsecs.V4i1.320