OPEN ACCESS
Indo-JC Indonesia Journal of Computing
ISSN 2460-9056
journals.telkomuniversity.ac.id/indojc

Ind. Journal on Computing
Vol. 10, Issue. 1, August 2025. pp. 1-11
doi:10.21108/indojc.v10i1.8976

The Impact of Ransomware on Indonesia's National Data Security: Case Study of Kominfo Data Leaks

Rahmat Rambe[1], Fairuz Fernanda Hermawan[2]

Faculty of Industrial Engineering, Telkom University
Telecommunication Street No. 1, Bandung 40257, Indonesia

[1] gyurahmat@student.telkomuniversity.ac.id
[2] fairuzbdg@student.telkomuniversity.ac.id

Abstract

Ransomware poses a growing threat to national data security, especially in Indonesia, where government agencies have experienced serious data breaches. This study examines the June 2024 ransomware attack on Indonesia's Ministry of Communication and Informatics (Kominfo) through a systematic literature review (SLR) of 1,200 articles from Semantic Scholar, Scopus, and IEEE Xplore (2015–2024), narrowing to 45 relevant studies. Findings highlight critical vulnerabilities, including weak technical infrastructure, inadequate backup systems, low password security, poor inter-agency coordination, and a shortage of trained cybersecurity professionals. Governance issues such as ineffective regulation and corruption in procurement further increased systemic risk. Current literature shows limited relevance to Indonesia's context, as most studies originate from high-income countries. The study recommends strengthening cybersecurity regulations aligned with frameworks like the GDPR, and improving workforce capabilities through targeted training. Cross-sector and international collaboration are also key to building resilience. These strategies are essential to enhance data protection and prevent future breaches.

Keywords: Ransomware, National Data Security, Data Breach, Cybersecurity Policy, Risk Management, Data Backup, Kominfo, Systematic Literature Review

Abstrak

Ransomware telah menjadi suatu ancaman yang semakin serius terhadap keamanan data nasional di Indonesia, khususnya dengan meningkatnya insiden kebocoran data pada instansi pemerintah. Penelitian ini sendiri bertujuan untuk menganalisis dampak serangan ransomware terhadap keamanan data nasional melalui studi kasus kebocoran data di Kementerian Komunikasi dan Informatika (Kominfo). Metode yang digunakan adalah Systematic Literature Review terhadap 1.200 artikel dari berbagai database ilmiah, yang kemudian disaring menjadi 45 studi yang relevan. Hasil penelitian ini adalah mengungkapkan sejumlah kerentan yang kritis, seperti lemahnya infrastruktur teknis, tidak adanya sistem backup yang memadai, serta kekurangan tenaga profesional di bidang keamanan siber. Selain hal tersebut, faktor tata kelola yang buruk dan lemahnya regulasi turut memperburuk risiko sistemik. Oleh karena itu penelitian ini merekomendasikan penerapan standar keamanan data yang lebih ketat, penguatan pelatihan SDM, serta pengembangan kolaborasi lintas sektor dan internasional untuk meningkatkan ketahanan terhadap serangan siber di masa depan.

Kata Kunci: Ransomware, Keamanan Data Nasional, Kebocoran Data, Kebijakan Keamanan Siber, Manajemen Risiko, Cadangan Data, Kominfo, Tinjauan Literatur Sistematis

Received on January, 2025. Accepted on August, 2025

I. Introduction

In the contemporary digital landscape, Data security has become an increasingly critical issue, impacting sectors such as government, business, and society. Data is recognized as a vital asset that requires robust protection against various threats, particularly cyberattacks like ransomware. Although numerous studies have explored aspects of ransomware and cybersecurity, there is currently no comprehensive review that integrates diverse methodologies and findings to examine vulnerabilities within Indonesia's governmental framework. This gap is especially concerning given the rapid evolution of cyber threats and the fragmented nature of existing research, underscoring the necessity of a systematic literature review (SLR).

Ransomware malicious software that encrypts data and demands a ransom, has not only caused significant financial losses but also disrupted essential operations and infringed on data privacy. Recently, the National Data Center (PDN) of the Ministry of Communication and Informatics (Kominfo) in Jakarta experienced severe disruptions over a specific period, allegedly due to a ransomware attack [1]. Cybersecurity expert Alfons Tanujaya noted that such attacks, increasingly evolving into extortionware, compromise sensitive data (including immigration records) and threaten public trust.

Examining ransomware and its implications for national data security is critical. Existing literature has identified systemic weaknesses—such as shortcomings in risk management, inadequate data backup, and weak policy enforcement—that facilitate successful ransomware attacks. Given the increasing digitization of government services and the consequent risks to national security, a systematic review is necessary to consolidate fragmented studies and to develop targeted strategies for enhancing cybersecurity resilience.

This study systematically assesses the impact of ransomware on Indonesia's national data security by focusing on the recent data breach at Kominfo. By conducting an SLR, we identify key vulnerabilities within Indonesia's governmental cybersecurity framework, addressing significant gaps in risk management and data backup practices. The findings provide a foundation for future research and offer practical recommendations—such as adopting stricter security standards, enhancing backup protocols, and exploring innovative solutions like blockchain technology and GDPR-like regulations—to bolster Indonesia's resilience against cybersecurity threats.

II. Literature Review

To deepen the knowledge in the research conducted, we sought information regarding the definition of each keyword used.

The first keyword is **ransomware**, Ransomware is a type of malware that encrypts user data and demands ransom, often distributed via phishing, software exploits, or compromised systems. Beaman et al. (2021) observed a dramatic increase in ransomware during COVID-19, highlighting phishing and software vulnerabilities as key vectors, while evaluating detection and mitigation tools [2].

The second keyword is **national data security**. National data security refers to the efforts and policies undertaken by a country to protect sensitive and vital information and data essential for the functioning of government, economy, and national security from threats and disruptions, both domestic and foreign. Data security also encompasses the protection against unauthorized access, data theft, espionage, and cyberattacks, which can disrupt critical infrastructure and public services [3].

The third keyword is **data breach**. A data breach is a security incident where sensitive, protected, or confidential information is accessed, disclosed, stolen, or used by someone without authorization. Data breaches can occur due to various factors, including cyberattacks, human error, or system failures, leading to financial losses, privacy violations, and a loss of trust [3].

The fourth keyword is **risk management**. Risk management is a systematic process for identifying, analyzing, evaluating, controlling, and monitoring risks that could affect the achievement of an organization's goals. Another objective of risk management is to minimize the negative impact of risks while maximizing opportunities that may arise from those risks [4].

The fifth keyword is **data backup**. Data backup is the process of creating copies of data that are stored in a secure location to protect against data loss or damage due to system failures, cyberattacks, or human error. The purpose of creating these copies is to ensure that data can be restored in the event of an incident that leads to the loss of the original data [5].

The sixth keyword is **data protection**. Data protection encompasses a series of actions, policies, and technologies used to safeguard the confidentiality, integrity, and availability of data from unauthorized access, breaches, or damage. The aim of data protection is to ensure that data remains secure against both internal and external threats, while also complying with relevant regulations and security standards [6].

The seventh keyword is **cyber-attack**. A cyber-attack is an action carried out by individuals or groups using computer technology to target information systems, networks, or devices connected to the internet. The purposes of cyber-attacks vary, ranging from stealing sensitive information and disrupting operations to damaging or destroying data and infrastructure [7].

The last keyword is **Kominfo**. Kominfo is a government agency, fully known as the Ministry of Communication and Information of the Republic of Indonesia. This agency is a central ministry responsible for managing communication, information, and technology in Indonesia. Kominfo plays a crucial role in regulating, developing, and overseeing the telecommunications sector, broadcasting, internet services, as well as data protection and cybersecurity in the country [8].

III. Research Method

This research employs Systematic Literature Review (SLR), SLR is a rigorous method for identifying, appraising, and synthesizing relevant literature [9]. Our SLR is guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, which ensures transparency and reproducibility by outlining clear steps for the identification, screening, eligibility assessment, and final inclusion of studies [10]. This standardized approach not only consolidates fragmented evidence but also provides a robust basis for deriving meaningful insights into the impact of ransomware on Indonesia's national data security.

A. Research Question (RQs)

This study is anchored by two central research questions that guide the review:

- RQ1: What specific weaknesses in Indonesia's national data security infrastructure have been revealed by ransomware attacks?
- RQ2: What strategic measures can be taken to improve the country's cybersecurity resilience against such threats?

B. Literature Search Strategy

The research method employed in this study is the SLR using PRISMA approach. This process begins with identifying a research problem, which serves as the foundation for the study, followed by searching for relevant information sources, including books, papers, journals, and other materials using predefined keywords.

To ensure a comprehensive review, the researcher conducted searches across three major academic databases: Semantic Scholar, Scopus, and IEEE Xplore. The search utilized carefully selected keywords, including "Cyber Attack," "Data Backup," "Data Breach," "Data Protection," "Kominfo," "National Data Security," "Ransomware," and "Risk Management."

To maintain the relevancy of the references, only articles published between 2015 and 2025 were considered. Additionally, all keywords were entered in English to ensure the broadest possible scope of literature retrieval.

C. Inclusion and exclusion criteria

TABLE I
INCLUSION CRITERIA AND EXCLUSION CRITERIA

Inclusion Criteria	Exclusion Criteria
Peer-reviewed articles that explicitly address ransomware and its implications for national data security.	Studies falling outside the publication year range or lacking a direct focus on ransomware issues in a governmental context.
Articles written in English and Bahasa	Publications that are not peer-reviewed
Articles can be accessed in full view	Same article from different Journal Databases

D. Article Selection Process

The initial search returned approximately 1.200 articles. A multi-stage screening process was then conducted:

- Stage 1 – Identification Process: in this stage, all retrieved articles were examined based on their titles and abstracts to assess their initial relevance. Articles that clearly did not meet the predetermined inclusion criteria such as those outside the publication timeframe, not in English, bahasa and not focused on ransomware and its implications for national data security were excluded. This stage also included the removal of duplicate records to refine the pool further.
- Stage 2 – Screening Process: Articles that passed the initial screening were subjected to a more detailed review. During this stage, the full text of each article was evaluated to ensure it aligned with the study's focus and met all inclusion criteria. This in-depth examination allowed for the identification of studies that provided substantive insights into the vulnerabilities of Indonesia's governmental data security in the context of ransomware attacks.
- Final Stage: After completing the full-text evaluation, a total of 45 articles met all the selection criteria and were included for comprehensive qualitative analysis. These articles form the basis of our systematic review, as depicted in the 'Included' section of the PRISMA flow diagram below:

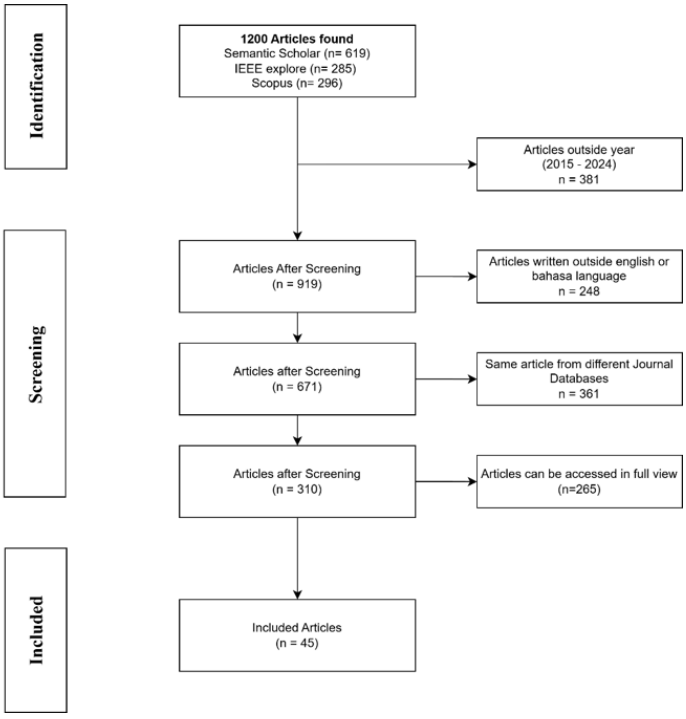

Fig. 1. SLR diagram process Using PRISMA

E. Analysis Method

A qualitative synthesis approach was used to analyze the selected articles. The data were examined through thematic coding to extract and categorize recurring patterns and critical insights related to cybersecurity vulnerabilities and resilience strategies. This structured analysis enabled the development of meaningful conclusions and recommendations for future research and policymaking.

IV. RESULTS AND DISCUSSION

This chapter specifically discusses and answers three main research questions that have been formulated in this study, namely: (1) What specific weaknesses in Indonesia's national data security infrastructure have been revealed by ransomware attacks? (2) What strategic measures can be taken to improve the country's cybersecurity resilience against such threats? To answer these questions, a synthesis was carried out on 45 relevant scientific studies.

A. Previous Search

Table 2 below discusses and answers Research Question 1, namely: What specific weaknesses in Indonesia's national data security infrastructure have been revealed by ransomware attacks? By synthesizing findings from 33 relevant scientific studies and credible news sources, several critical vulnerability themes were identified. These themes are organized into six main categories: Technical Weaknesses, Human Resource Gap, Governance Issues, Regulatory Implementation, Procurement and Infrastructure, and Public Awareness. The analysis highlights that these categories significantly contribute to Indonesia's exposure to ransomware threats. Recognizing and addressing these weaknesses is vital for building a more resilient and secure national data infrastructure.

TABLE II
WEAKNESSES ASPECT IN INDONESIA INFRASTRUCTURE

Category	Brief Explanation	Article / news
Technical weaknesses	Reliance on Centralized Systems Without Data Backups	[11]
Human Error	Weak Passwords and Network Protection	[12], [13], [14], [15]
Human Resource Gap	Shortage of Cybersecurity Personnel and Resources	[16],[17], [18]
Governance Issues	Poor Coordination and Accountability	[19]
Regulatory Implementation	Poor Implementation of Data Protection Regulations	[20], [21], [22]
Procurement and Infrastructure	Problematic IT Infrastructure Procurement	[22]

Table 2 summarizes key findings on regulatory and technical approaches to national data protection and ransomware mitigation. The review is structured into six key areas: Technical weaknesses,Human Error,Human Resource Gap,Governance Issues, Regulatory Implementation, Procurement and Infrastructure.

According to the Ministry of Communication and Informatics (Kominfo), the absence of a proper backup system was a critical flaw, which exacerbated the impact of the June 2024 ransomware attack on Indonesia's National Data Center (PDN) [10] . Literature on IT Disaster Recovery Planning (DRP) and Business Continuity (BC) emphasizes the necessity of backup infrastructure to prevent data loss and service downtime during cyber incidents [11].

Furthermore, weak authentication practices, particularly poor password management, have been identified as major technical vulnerabilities [11]. According to the analysis by [12] the Public Data Network (PDN) infrastructure exhibited poor credential management practices, including the use of weak and default

administrative passwords that were insufficiently protected and potentially accessible through unsecured channels. This highlights the prevalence of common and easily cracked passwords. Research by Mukherjee et al. (2023) introduced MASCARA, a system for generating secure yet memorable passphrases using a human-centered approach. Their findings show that passphrases generated through structured models significantly improve memorability up to 100% higher recall while maintaining strong resistance to guessing attacks. Additionally, Woods and Siponen (2023) emphasize that memory anxiety plays a critical role in insecure behaviors such as password reuse, underscoring the need for password policies that balance complexity with user cognitive limits. This highlights that a combined technical and psychological approach to authentication design is essential to mitigate risks. Moreover, the deliberate deactivation of Windows Defender security features at Temporary National Data Center (PDNS) site 2 just days before the attack further increased system vulnerability [14]. A lack of cybersecurity-trained personnel was identified as a contributing factor to the breach [15]. This is consistent with global literature highlighting the shortage of certified cybersecurity professionals as a major weakness in national cyber defense systems[16]. Studies emphasize the urgent need for skilled and motivated professionals capable of responding to modern cyber threats. In Europe, strategic actions have been taken to address this gap by expanding the talent pipeline and improving training standards [18]. These efforts include curriculum enhancement, role-based certification schemes, and workforce scaling. The Indonesian context reflects similar needs: increasing both the quantity and quality of cybersecurity personnel is essential to safeguard national data infrastructure.

"Kominfo proceeded with procurement processes without consulting BSSN [19], the Ministry of Communication and Information (Kominfo) proceeded with the PDN procurement process without adequate consultation and coordination with BSSN, leading to fragmented cybersecurity responsibilities. This lack of inter-agency coordination and oversight resulted in exposed citizen data and paralyzed public services. Such findings underscore the importance of clear accountability structures and multi-stakeholder collaboration in national cyber governance frameworks.

Existing regulations, such as the Personal Data Protection Act (PDP Law), still lack enforceability due to vague jurisdictional boundaries, inconsistent sanction application, and weak oversight mechanisms[20]. These limitations hinder the law's effectiveness as a robust foundation for national cybersecurity and data protection.

Highlight that governance issues, including potential irregularities in the PDN procurement process, have persisted since 2020, contributing to systemic vulnerabilities in national data infrastructure [21]. It was revealed that project specifications were manipulated to favor certain vendors, and compliance requirements such as ISO 22301 (Business Continuity Management Systems) were removed. This undermined the integrity and resilience of critical infrastructure from the outset.

Table 3 below discusses and answers Research Question 2, namely: What strategic measures can be taken to improve the country's cybersecurity resilience against such threats? By synthesizing findings from 33 relevant scientific studies, several key themes emerge across five main categories. These categories are: Data Protection regulation using GDPR, Other country General Data Protection, CyberSecurity Framework, Ransomware detection using Machine Learning, and *Advanced Encryption Standard* (AES). The analysis reveals that technical weaknesses, gaps in human resources, governance challenges, regulatory implementation issues, procurement and infrastructure limitations, and public awareness all play significant roles in shaping cybersecurity resilience. Understanding and addressing these factors within each category is crucial for developing effective national strategies to combat cyber threats.

TABLE III
SUMMARY OF KEY THEMES ON CYBERSECURITY STRATEGIC MEASURES

Category	Brief Explanation	Article
Data Protection regulation using GDPR	Discusses GDPR implementation and its role in mitigating ransomware and ensuring data privacy	[23] [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34]

Other country General Data Protection	Evaluates other nation data protection laws and institutional capacity	[35], [36], [37], [38], [34], [39], [40], [41]
CyberSecurity Framework	Reviews national cybersecurity strategy and institutional frameworks (e.g., BSSN roles)	[42]
Ransomware detection using Machine Learning	Explores ML-based approaches for early detection and classification of ransomware attacks	[43], [44], [45]
Advanced Encryption Standard (AES)	Highlights the role of AES encryption in protecting sensitive data from ransomware attacks	[46], [47]

Table 3 summarizes key findings on regulatory and technical approaches to national data protection and ransomware mitigation. The review is structured into five key areas: GDPR implementation, other countries' general data protection strategies, national cybersecurity frameworks, ransomware detection using machine learning, and encryption techniques.

The General Data Protection Regulation (GDPR), enacted in 2018, has standardized data privacy protocols across the European Union and influenced global digital governance. It facilitates secondary data sharing in sectors like healthcare but presents ethical and operational challenges concerning consent and anonymization [22][25][26][27]. For example, Austria's COVID-19 platform illustrates GDPR's dual function—supporting innovation while safeguarding privacy [24]. To assist compliance, formal tools such as UML-based models and automated rule checkers have been developed to translate legal provisions into machine-readable language [31][34]. Federated learning and encryption technologies help balance privacy and performance in data systems [33]. Despite corporate strategies adapting to GDPR as a regulatory risk [28], users still express dissatisfaction, particularly regarding transparency and access to personal data [32]. Investigations in Indonesia also emphasize the need for stronger institutional readiness in complying with GDPR principles [30]. In addition, AI-based tools show potential in enhancing policy implementation and optimizing compliance monitoring [29].

Outside of the EU, countries adopt diverse data protection frameworks reflecting local socio-political contexts. Brazil focuses on establishing independent data protection authorities and streamlining data processing practices [37][38]. The United States demonstrates significant variability due to sector-based approaches and high enforcement costs [34]. Malaysia emphasizes citizen authentication and public awareness through its e-government strategy, while South Africa's POPIA law necessitates industry-specific codes of conduct [35]. Indonesia struggles with low digital literacy and vulnerable user groups, prompting recommendations for strengthened oversight and community education [34][40]. In China, strict data localization and government access requirements position data as a sovereign economic asset [42]. Meanwhile, South Asian countries aim for GDPR-inspired harmonization, despite facing legal and political heterogeneity [43].

National cybersecurity strategies are increasingly integrating data protection elements. Italy's National Cybersecurity Framework exemplifies alignment with GDPR principles to ensure both legal and technical safeguards [44]. This highlights the need for unified cybersecurity and data governance policies to address cross-border threats and digital sovereignty concerns.

Machine learning approaches offer promising results for early ransomware detection. Several models report over 99% accuracy in identifying ransomware behaviors before encryption occurs [45]. However, automation remains a challenge in dynamic environments [46]. The RTrap framework introduces a proactive defense by using decoy files and bait monitoring, effectively containing ransomware within seconds [47].

Encryption remains fundamental to data protection. Recent studies showcase hybrid approaches that combine steganography and cryptography for secure messaging in high-risk environments [48]. In a practical context, AES 128-bit encryption has been successfully implemented in web-based applications to ensure confidentiality and access control. For example, [48]developed a browser-based file encryption system using AES-128, demonstrating its effectiveness in protecting sensitive user data through secure upload and decryption mechanisms.

B. Discussion of Related Journals and Relevance to Indonesia

In addressing the two issues above, the researcher has referenced several existing studies to respond to these problems and hopes to provide solutions for the future, including the following:

1. Establishing a National Data Security Emergency Protocol means that, based on the results of the literature and considerations from various sources within the journal, there are several measures that can be taken to prevent similar incidents. These include creating emergency security protocols as outlined in the journal [48] which suggests implementing blockchain to strengthen national data security within Indonesia's digital transformation system, where blockchain serves as a decentralized technology that can ensure better integrity and security of data. This technology requires transparent and immutable recording of transactions or data changes, thereby preventing data manipulation or theft. Blockchain also supports the creation of a stronger authentication system using smart contracts, which only allow access and modification of data by parties with legitimate authority.

2. Establishing a National Personal Data Regulation like Europe's GDPR means that the government should consider creating specific data laws like those implemented in several European countries with their GDPR. Based on the two topics discussed earlier, the protection of personal data in Indonesia requires a strong and comprehensive regulation, akin to the General Data Protection Regulation (GDPR) in Europe. The GDPR itself is a stringent framework for data protection that provides individuals with broad rights over their personal data and establishes clear obligations for organizations in collecting, storing, and processing that data. By creating such regulations, Indonesia can enhance the protection of its citizens' personal data and reduce the risk of data breaches that could undermine public trust. These regulations should also include strict penalties for violators, including hefty fines for organizations that fail to protect personal data or that do not comply with established rules. The government must also ensure that these regulations are adhered to by all sectors and strengthen oversight and enforcement mechanisms. If regulations like the GDPR are established in Indonesia, it is crucial to implement principles such as data minimization, purpose limitation, and transparency to provide better protection for personal data.

3. The current body of literature on ransomware and national data security reveals several important gaps, particularly in the context of Indonesia. Many existing studies tend to generalize cybersecurity challenges and fail to address the unique vulnerabilities within Indonesia's governmental institutions. There is a noticeable lack of empirical research evaluating the effectiveness of existing national data protection policies, as well as a deficiency in studies focusing on recovery protocols and backup systems. The recent ransomware attack on Indonesia's National Data Center highlighted critical shortcomings in data recovery infrastructure and operational oversight, issues that are underexplored in scholarly work. Moving forward, future research should explore the development of decentralized governance models using technologies like blockchain to enhance data integrity and resilience. Comparative studies on international data protection frameworks such as the GDPR could offer valuable insights for shaping Indonesia's own regulations. Furthermore, research into artificial intelligence and machine learning-based solutions for early ransomware detection holds great promise. Investigations into organizational behavior, training, and awareness among public sector employees could also provide practical strategies to mitigate human error—a recurring weakness in current systems. Finally, the review of literature suggests the presence of certain publication biases and inconsistencies. Most studies originate from high-income countries, limiting their applicability to Indonesia's context. Additionally, there is an imbalance between technological and human-centric approaches in cybersecurity research. While many focus on tools and systems, fewer examine institutional culture, user behavior, or training. This calls for a more integrated research perspective that combines technical innovation with policy development and human factors to effectively address cybersecurity threats at a national level.

C. Opinions and Recommendations from the Researcher

Based on the analysis conducted, there are several recommendations proposed by the researcher to enhance national data security in Indonesia, particularly in addressing cyber threats such as ransomware. The researcher suggests three recommended improvement efforts, namely:

1. Strengthening Regulations and Policies refers to the researcher's suggestion that the Indonesian government should reinforce regulations and policies related to personal data protection and cybersecurity. The proposed regulation is akin to the GDPR in Europe or national data protection authority (ANDP) in Brazil, which the Indonesian government can use as a reference to create more comprehensive and stringent laws. The regulation should include minimum security standards that must be adhered to by all organizations responsible for managing data. By implementing such regulations, the protection of citizens' personal data can be enhanced, and the risk of data breaches can be minimized.

2. Enhancing Technological and Human Resource Capacity, in this context, means that in addition to establishing regulations, efforts to improve technological capacity and human resources are also a top priority. The researcher recommends this as part of an effort to increase investment in more advanced cybersecurity technologies, including the implementation of blockchain technology to ensure data integrity and prevent unauthorized modifications. Additionally, the researcher suggests the development of ongoing training for cybersecurity experts to ensure that they are always prepared to face evolving threats. Such training will create skilled and knowledgeable personnel, which is key to addressing increasingly complex cyberattacks.

3. International collaboration, in this context, refers to the researcher's suggestion on the importance of global cooperation in facing cyber threats. Indonesia itself must actively participate in international cooperation to share information, strategies, and best practices in addressing cyberattacks. This includes collaboration with other countries, international organizations, as well as the private sector in efforts to enhance national data security. Such cooperation not only strengthens defense but also provides access to the latest technologies and knowledge that can be implemented to protect national data from various threats.

V. Conclusion

This systematic literature review demonstrates that the June 2024 ransomware attack on Indonesia’s National Data Center was caused by a combination of technical vulnerabilities, a shortage of skilled cybersecurity personnel, and weaknesses in governance and regulatory frameworks. Key factors such as the absence of reliable backup systems, weak password practices, disabled security features, and corruption in procurement processes significantly increased the system’s exposure to cyber threats. Comparative analysis with international standards, including the GDPR, highlights the urgent need for Indonesia to strengthen its cybersecurity posture through an integrated approach that addresses legal, technical, and organizational aspects.

To enhance national resilience against future cyberattacks, the government should prioritize the implementation of robust backup infrastructures and advanced security technologies, such as data encryption and machine learning-based early threat detection. Building human resource capacity through comprehensive training and certification programs is essential to ensure a skilled cybersecurity workforce. Additionally, improving inter-agency coordination, establishing clear accountability mechanisms, and reinforcing regulatory oversight in procurement processes are critical steps to prevent corruption and secure critical infrastructure. Adopting international best practices and frameworks like the GDPR will also help standardize data protection policies and improve compliance.

Future research should focus on developing ransomware detection models specifically adapted to Indonesia’s technological environment, as well as evaluating the effectiveness of policy interventions aimed at raising digital literacy and public cybersecurity awareness. Such efforts will contribute to creating a safer digital ecosystem and strengthening the country’s overall cyber defense capabilities.

References

[1] Derick Musundi Kesa, "Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations," *World Journal of Advanced Research and Reviews*, vol. 18, no. 3, pp. 970–992, Jun. 2023, doi: 10.30574/wjarr.2023.18.3.1166.

[2] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput Secur*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102490.

[3] E. A. Sonjaazillnerr· and J.-C. Anaagarcíaarobles, "The Elements of Big Data Value Foundations of the Research and Innovation Ecosystem," Nov. 2021. doi: 10.1007/978-3-030-68176-0.

[4] P. Dahmen, "Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events," *Risk Management and Insurance Review*, vol. 26, no. 2, pp. 203–245, Jul. 2023, doi: 10.1111/rmir.12245.

[5] M. T. Alrashdan, M. A. Wahed, E. Aljarrah, M. Tubishat, M. Alzaqebah, and N. Aljawarneh, "The impact of data recovery criteria, data backup schedule and data backup prosses on the efficiency of data recovery management in data centers," *International Journal of Data and Network Science*, vol. 8, no. 4, pp. 2539–2546, 2024, doi: 10.5267/j.ijdns.2024.5.004.

[6] H. Jamal, N. A. Algeelani, and N. A. Al-Sammarraie, "Safeguarding data privacy: strategies to counteract internal and external hacking threats," *Computer Science and Information Technologies*, vol. 5, no. 1, pp. 46–54, Mar. 2024, doi: 10.11591/csit.v5i1.pp46-54.

[7] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions," Oct. 01, 2022, *MDPI*. doi: 10.3390/electronics11203330.

[8] S. Aminah and H. Saksono, "Digital transformation of the government: A case study in Indonesia," *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 37, no. 2, pp. 272–288, 2021, doi: 10.17576/JKMJC-2021-3702-17.

[9] R. Randles and A. Finnegan, "Guidelines for writing a systematic review," *Nurse Educ Today*, vol. 125, Jun. 2023, doi: 10.1016/j.nedt.2023.105803.

[10] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.

[11] Derick Musundi Kesa, "Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations," *World Journal of Advanced Research and Reviews*, vol. 18, no. 3, pp. 970–992, Jun. 2023, doi: 10.30574/wjarr.2023.18.3.1166.

[12] C. D. Darko, "Weak Credential Information as a Threat to Online Security," *Advances in Multidisciplinary and scientific Research Journal Publication*, vol. 1, no. 1, pp. 35–40, Jul. 2022, doi: 10.22624/AIMS/CRP-BK3-P6.

[13] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," *Heliyon*, vol. 7, no. 3, Mar. 2021, doi: 10.1016/j.heliyon.2021.e06522.

[14] N. Woods and M. Siponen, "How memory anxiety can influence password security behavior," *Comput Secur*, vol. 137, Feb. 2024, doi: 10.1016/j.cose.2023.103589.

[15] T. Ncubukezi, "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses," Feb. 2022.

[16] Mahendra Citra Yustika and Pinatih Arya Setiawati Desy Komang Ni, "STRATEGY FOR HANDLING CYBER SECURITY IN INDONESIA," *Journal of Education and Teaching Review*, vol. 6, Nov. 2023.

[17] B. J. Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training," *Technol Soc*, vol. 67, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.

[18] M. Ismail *et al.*, "Cybersecurity activities for education and curriculum design: A survey," *Computers in Human Behavior Reports*, vol. 16, Dec. 2024, doi: 10.1016/j.chbr.2024.100501.

[19] S. Ma'ruf, "CRISIS MANAGEMENT AND INCIDENT RESPONSE: A NATIONAL DATA CENTER CASE STUDY," *JICN*, vol. 1, no. 3, Jun. 2024.

[20] V. Ibrahim, Y. S. Hasan, and P. Ishak, "Personal Data Protection Policies and Their Impact on Victims of Cybercrime," *Kyadiren Journal of Legal Studies*, vol. 6, no. 2, pp. 13–25, 2025, doi: 10.46924/jihk.v6i2.225.

[21] B. Adinegoro, M. Fuad, A. Ruhuputy, I. Pambudi, and T. Arrahman, "INDONESIA'S ONE DATA POLICY: AN ANTITHYSIS OF THE SPIRIT OF OPENNESS AND PUBLIC INFORMATION," *Journal of Administrative Sciences*, vol. 16, no. 1, 2025.

[22] Y. Sanjaya, A. Fuad, L. Lazuardi, F. Ramdhani, W. A. Baros, and E. Dhanalvin, "Research Database Based on BPJS Health Secondary Data," Aug. 2020. doi: https://doi.org/10.22146/jisph.60510.

[23] A. Vlahou *et al.*, "Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics?," Apr. 01, 2021, *Lippincott Williams and Wilkins*. doi: 10.1161/HYPERTENSIONAHA.120.16340.

[24] J. Vukovic, D. Ivankovic, C. Habl, and J. Dimnjakovic, "Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective," *Archives of Public Health*, vol. 80, no. 1, Dec. 2022, doi: 10.1186/s13690-022-00866-7.

[25] H. J. Pandit, "Making Sense of Solid for Data Governance and GDPR," *Information (Switzerland)*, vol. 14, no. 2, Feb. 2023, doi: 10.3390/info14020114.

[26] M. Mohammad Amini, M. Jesus, D. Fanaei Sheikholeslami, P. Alves, A. Hassanzadeh Benam, and F. Hariri, "Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate," Sep. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/make5030053.

[27] C. Peukert, S. Bechtold, M. Batikas, and T. Kretschmer, "Regulatory Spillovers and Data Governance: Evidence from the GDPR," *Marketing Science*, vol. 41, no. 4, pp. 318–340, Jul. 2022, doi: 10.1287/mksc.2021.1339.

[28] M. Ferreira, T. Brito, F. Santos, and N. Santos, "RuleKeeper: GDPR-Aware Personal Data Compliance for Web Frameworks," 2023, doi: 10.1109/SP46215.2023.00058.

[29] A. Bowyer, J. Holt, J. Go Jefferies, R. Wilson, D. Kirk, and J. David Smeddinck, "Human-GDPR Interaction: Practical Experiences of Accessing Personal Data," in *Conference on Human Factors in Computing Systems - Proceedings*, Association for Computing Machinery, Apr. 2022. doi: 10.1145/3491102.3501947.

[30] L. Kyi, S. Ammanaghatta Shivakumar, C. T. Santos, F. Roesner, F. Zufall, and A. J. Biega, "Investigating Deceptive Design in GDPR's Legitimate Interest," in *Conference on Human Factors in Computing Systems - Proceedings*, Association for Computing Machinery, Apr. 2023. doi: 10.1145/3544548.3580637.

[31] R. Y. Wong, A. Chong, and R. Cooper Aspegren, "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures," *Proc ACM Hum Comput Interact*, vol. 7, no. CSCW1, Apr. 2023, doi: 10.1145/3579515.

[32] N. Ettaloui, S. Arezki, and T. Gadi, "An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA," *Data and Metadata*, vol. 2, Jan. 2023, doi: 10.56294/dm2023166.

[33] D. Torre *et al.*, "Modeling Data Protection and Privacy: Application and Experience with GDPR," *Journal of Software and systems modelling*, pp. 1–17, Jun. 2021.

[34] I. Isabella, A. Alfitri, A. Saptawan, N. Nengyanti, and T. Baharuddin, "Empowering Digital Citizenship in Indonesia: Navigating Urgent Digital Literacy Challenges for Effective Digital Governance," *Journal of Governance and Public Policy*, vol. 11, no. 2, pp. 142–155, Jun. 2024, doi: 10.18196/jgpp.v11i2.19258.

[35] N. S. Netshakhuma, "Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA)," *Global Knowledge, Memory and Communication*, vol. 69, no. 1/2, pp. 58–74, Jul. 2020, doi: 10.1108/GKMC-02-2019-0026.

[36] M. M. Ahmed and A. Musa Ahmed, "Citizens' Data Protection in E-government System," *International Journal of Innovative Computing*, vol. 13, no. 2, pp. 1–9, Nov. 2023, doi: 10.11113/ijic.v13n2.389.

[37] C. Staunton, K. Tschigg, and G. Sherman, "Data protection, data management, and data sharing: Stakeholder perspectives on the protection of personal health information in South Africa," *PLoS One*, vol. 16, no. 12 December, Dec. 2021, doi: 10.1371/journal.pone.0260341.

[38] E. D. Canedo *et al.*, "Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)," in *International Conference on Enterprise Information Systems, ICEIS - Proceedings*, Science and Technology Publications, Lda, 2021, pp. 19–30. doi: 10.5220/0010398200190030.

[39] V. Bentotahewa, C. Hewage, and J. Williams, "The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries," *SN Comput Sci*, vol. 3, no. 3, p. 183, May 2022, doi: 10.1007/s42979-022-01079-z.

[40] C. Bian, "Data as Assets in Foreign Direct Investment: Is China's National Data Governance Compatible with its International Investment Agreements?," *Asian Journal of International Law*, vol. 13, no. 2, pp. 342–364, Jul. 2023, doi: 10.1017/S2044251322000595.

[41] V. Bentotahewa, C. Hewage, and J. Williams, "The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries," *SN Comput Sci*, vol. 3, no. 3, May 2022, doi: 10.1007/s42979-022-01079-z.

[42] H. Tao, "Conflicts and Coordination in Data Localization in China and International Trade Law," *Proceedings of the International Conference on Global Trade Law 2024,* pp. 436–446, 2024, doi: 10.2991/978-2-38476-277-4_49.

[43] J. A. Herrera-Silva and M. Hernández-Álvarez, "Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms," *Sensors*, vol. 23, no. 3, Feb. 2023, doi: 10.3390/s23031053.

[44] A. Alraizza and A. Algarni, "Ransomware Detection Using Machine Learning: A Survey," *Big Data and Cognitive Computing*, vol. 7, no. 3, Sep. 2023, doi: 10.3390/bdcc7030143.

[45] G. O. Ganfure, C. F. Wu, Y. H. Chang, and W. K. Shih, "RTrap: Trapping and Containing Ransomware With Machine Learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1433–1448, 2023, doi: 10.1109/TIFS.2023.3240025.

[46] D. Irwanto, "File Encryption and Decryption Using Algorithm Aes-128 Bit Based Website," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 2, pp. 670–677, Apr. 2024, doi: 10.57152/malcom.v4i2.1305.

[47] A. Aprizald, M. A. Hasan, and D. Setiawan, "Web Based Data Security Application Using AES 128 Algorithm For Data Encryption And Decryption," *Journal of Informatics Engineering*, vol. 2, no. 2, pp. 85–95, Jan. 2023, doi: 10.58794/jekin.v2i2.225.

[48] T. W. E. Suryawijaya, "Strengthening Data Security through Blockchain Technology: A Case of Indonesia's Digital Transformation," *Journal of Public Policy Studies*, vol. 2, no. 1, pp. 55–68, May 2023, doi: 10.21787/jskp.2.2023.55-68.