Journal of Cyber Law and Information Security
Volume 2, Number 1, 2023

Cybersecurity Regulation Against Ransomware Attacks on National Critical Infrastructure: A Legal Analysis of Indonesia's Regulatory Preparedness

Nurul Musyarofah[1*]

[1] Universitas Trisakti, Jakarta, Indonesia

Abstract

Article history:
Received: January 15, 2023
Revised: February 02, 2023
Accepted: April 29, 2023
Published: June 30, 2023

Keywords:
Critical Infrastructure, Cyber Regulation, Cybersecurity, Presidential Regulation No. 82/2022, Ransomware.

Identifier:
Zera Open
Page: 79-94
https://zeraopen.com/journal/jclis

Ransomware attacks on national critical infrastructure have emerged as one of the most destructive cyber threats in the digital era, endangering the continuity of essential public services, including energy, healthcare, finance, and government systems. Indonesia has experienced a significant increase in ransomware incidents in recent years, culminating in a major attack on the *Pusat Data Nasional Sementara* (PDNS) that disrupted hundreds of government services. This study employs a normative-comparative approach to examine two fundamental issues: (1) the extent to which Indonesia's existing cybersecurity regulatory framework, particularly Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure, is effective in addressing ransomware threats; and (2) why strengthening the regulatory framework for national critical infrastructure security has become an urgent priority requiring comprehensive assessment. The findings reveal that the current regulatory framework still contains several critical weaknesses, including fragmented institutional authority, the absence of binding technical cybersecurity standards, and limited coordination in incident response mechanisms. This study recommends the development of a comprehensive sector-specific cybersecurity regulatory framework and the establishment

*Corresponding author:
(Nurul Musyarofah)

of a national Computer Emergency Response Team (CERT) with clearly defined legal authority.

1. Introduction

Cyber threats in the form of ransomware attacks have undergone a dramatic evolution over the past decade. Once primarily viewed as a financial threat targeting individuals and private companies, ransomware has now developed into a cyber weapon capable of crippling a nation's critical infrastructure, disrupting essential public services, and even directly endangering human lives. This phenomenon marks a new chapter in the landscape of national security threats, which are no longer confined to the physical domain but have expanded massively into cyberspace.

Indonesia has not been immune to this escalating threat. In mid-2024, the Brain Cipher ransomware attack paralyzed the *Pusat Data Nasional Sementara* (PDNS), which serves as the backbone of hundreds of digital services for both central and regional governments. This incident exposed profound structural vulnerabilities within Indonesia's governmental digital infrastructure and raised serious questions regarding the adequacy of the existing legal framework in addressing cyber threats of this magnitude (BSSN, 2022). Immigration services, civil registration administration, and numerous other public services were disrupted for

weeks, resulting in losses that extended beyond economic damage to include a significant erosion of public trust.

National critical infrastructure encompasses sectors whose disruption or destruction would have debilitating effects on national security, the economy, and public health or safety. In Indonesia, these sectors include energy, transportation, communications, finance, clean water, healthcare, food supply, and government systems. The increasing dependence of these infrastructures on interconnected information systems has created a vast attack surface that is highly vulnerable to organized cyber exploitation.

From a normative perspective, Indonesia has established several regulations concerning cybersecurity and the protection of critical infrastructure. Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure (Perpres 82/2022) serves as the principal legal instrument specifically governing the protection of critical infrastructure against cyber threats. In addition, Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions (the EIT Law), along with various sectoral regulations issued by *Badan Siber dan Sandi Negara* (BSSN), collectively form Indonesia's current national cybersecurity regulatory framework (Aritonang, 2022).

However, a fundamental question remains: is this regulatory framework sufficiently robust and comprehensive to address ransomware threats that continue to evolve in both complexity and technical sophistication? The gap between the technical sophistication of modern ransomware attacks and the capacity of the existing legal and regulatory framework constitutes the central focus of this study.

Based on this background, this study formulates two research questions. First (RQ1): To what extent is Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure, together with related cybersecurity regulations, effective in protecting national critical infrastructure against ransomware attacks? Second (RQ2): Why is the study and strengthening of cybersecurity regulation in response to ransomware threats against national critical infrastructure an urgent and pressing necessity?.

2. Methods

This study employs a normative-comparative approach that combines doctrinal analysis of existing legislation with a comparative examination of cybersecurity regulations in countries that are more advanced in addressing ransomware threats. The normative approach is used to assess the substance, consistency, and comprehensiveness of Indonesia's cybersecurity regulatory framework in the context of ransomware threats to critical infrastructure. The comparative approach is applied to identify best practices and international standards that may serve as references for strengthening Indonesia's regulatory framework.

Type and Sources of Data. This study relies on secondary data derived from three categories of legal materials. Primary legal materials include Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure, Law No. 19 of 2016 amending the Electronic Information and Transactions Law, cybersecurity regulations issued by the BSSN, Indonesia's National Cybersecurity

Strategy 2020-2024, as well as comparative regulations from the United States (the NIST Cybersecurity Framework and Cybersecurity and Infrastructure Security Agency directives), the European Union (the NIS2 Directive), and Singapore (the Cybersecurity Act 2018). Secondary legal materials consist of scholarly journals in law and information technology, cybersecurity incident reports issued by governmental and private institutions, and proceedings from international cybersecurity conferences.

Data Collection Technique. Data were collected through a systematic literature review, including searches of international academic databases such as Scopus, IEEE Xplore, and Web of Science, as well as primary legal sources from official Indonesian government institutions and international cybersecurity organizations such as European Union Agency for Cybersecurity, Cybersecurity and Infrastructure Security Agency, and INTERPOL.

Data Analysis Technique. The data were analyzed using qualitative content analysis with a descriptive-analytical-comparative approach. The analytical stages consisted of: (1) mapping the applicable cybersecurity regulations relevant to ransomware threats; (2) identifying regulatory gaps through a gap analysis between existing legal provisions and the technical characteristics of modern ransomware; (3) conducting a comparative analysis of cybersecurity legal frameworks in the United States, the European Union, and Singapore; and (4) synthesizing the findings to formulate recommendations for regulatory enhancement.

3. Results & Discussion

3.1 The Effectiveness of Indonesia's Cybersecurity Regulatory Framework in Addressing Ransomware Threats to Critical Infrastructure (RQ1)

3.1.1 Mapping Indonesia's Cybersecurity Regulatory Framework

Indonesia's current cybersecurity regulatory framework consists of multiple layers of regulation that are complementary in nature, although not yet fully integrated. At the highest level, Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure (Perpres 82/2022) serves as the legal instrument most directly relevant to this study. This regulation defines Vital Information Infrastructure (VII) as information infrastructure whose disruption or destruction could result in the failure of public service systems, disruption to the national economy, or threats to national defense and security (Perpres 82/2022, Article 1(1)).

Perpres 82/2022 designates eight sectors as Vital Information Infrastructure: government, energy and mineral resources, transportation, finance, healthcare, information and communication technology, food, and defense. The regulation requires VII operators in each sector to implement risk identification, protection, detection, response, and recovery as part of a continuous cybersecurity management cycle. The National Cyber and Crypto Agency (BSSN) is designated as the national technical coordinator, while sectoral ministries and agencies are responsible for oversight within their respective sectors (Aritonang, 2022).

In addition to Perpres 82/2022, this regulatory framework is supported by the Electronic Information and Transactions Law (EIT Law), which criminalizes

unauthorized access to electronic systems and data destruction; the National Cybersecurity Strategy 2020–2024, which provides macro-level policy guidance; and various BSSN regulations concerning technical information security standards. Normatively, this combination of regulations appears sufficiently comprehensive to establish a foundational framework for the protection of vital information infrastructure.

3.1.2 Regulatory Gaps in Addressing Ransomware Threats

Despite the apparent adequacy of the existing normative framework, a deeper analysis reveals several structural deficiencies that undermine its effectiveness in addressing ransomware threats, which are rapid, coordinated, and often transnational in nature.

First, there is a fragmentation of authority coupled with weak inter-agency coordination. Perpres 82/2022 divides responsibility for VII protection between BSSN as the technical coordinator and sectoral ministries as operational supervisors. In practice, this division creates ambiguity regarding authority, potentially hindering rapid response during cyber incidents. The ransomware attack on the National Temporary Data Center (PDNS) demonstrated how fragmented coordination among the Ministry of Communication and Informatics, BSSN, and data center operators contributed to significant response delays and exacerbated the impact of the attack (Nugroho, 2022).

Second, there is an absence of legally binding technical cybersecurity standards. Perpres 82/2022 does not establish specific and enforceable minimum technical standards for VII operators. The obligations it imposes are general and

principle-based, without measurable technical benchmarks. As a result, individual VII operators may adopt varying interpretations and levels of implementation, creating uneven levels of cyber resilience that can be exploited by ransomware actors through a "weakest-link" approach (Lestari & Wahyudi, 2022).

Third, the regulatory framework contains insufficient provisions concerning backup management and disaster recovery. One of the defining characteristics of ransomware attacks is the encryption of data, often accompanied by the destruction or compromise of backup systems. Existing regulations do not explicitly mandate secure backup standards, including offline or air-gapped backups and periodic recovery testing. This regulatory omission significantly increases the potential impact of ransomware incidents.

Fourth, there is no clear and legally binding obligation for timely incident reporting. Unlike the European Union's notification requirements under the General Data Protection Regulation (GDPR), which mandate reporting within 72 hours, Indonesia's cybersecurity regulations do not impose a specific timeframe for reporting ransomware incidents. The absence of such a requirement results in underreporting or delayed reporting, thereby limiting BSSN's ability to coordinate responses effectively and conduct comprehensive threat intelligence analysis.

3.1.3 Comparative Analysis with International Cybersecurity Regulations

A comparison with cybersecurity regulations in more advanced jurisdictions provides valuable insights into the gaps that Indonesia needs to address. The United States, through the Cybersecurity and Infrastructure Security Agency (CISA), has issued Binding Operational Directives that require federal agencies to remediate

known vulnerabilities within strict deadlines. The NIST Cybersecurity Framework provides comprehensive technical standards that have been widely adopted across the private sector. Specifically regarding ransomware, CISA has published detailed technical guidance covering mandatory security practices, incident response procedures, and reporting mechanisms.

The European Union, through the NIS2 Directive, has established significantly stricter cybersecurity requirements for operators of essential services and digital service providers. NIS2 mandates comprehensive risk management, incident reporting within 24 hours, substantial administrative penalties, and personal accountability for senior management in cases of cybersecurity failures. Meanwhile, Singapore, through the Cybersecurity Act 2018, has developed a highly comprehensive regulatory regime characterized by specific technical obligations and effective enforcement mechanisms (Greenleaf, 2021). This comparison demonstrates that Indonesia's regulatory framework still lags considerably behind international standards in terms of technical specificity and enforcement strength.

3.2 The Urgency of Strengthening Cybersecurity Regulation Against Ransomware Threats to Indonesia's Critical Infrastructure (RQ2)

3.2.1 The Escalation of Ransomware as a National Security Challenge

The urgency of strengthening Indonesia's cybersecurity regulatory framework is first and foremost driven by the escalating nature of ransomware threats, which have evolved beyond ordinary criminal activity into a matter of national security. Cybersecurity projections indicate that global ransomware-related losses are expected to exceed hundreds of billions of U.S. dollars annually within the coming

decade, with government infrastructure remaining among the most frequently targeted sectors. In Indonesia, BSSN has recorded a dramatic increase in ransomware incidents, making ransomware one of the fastest-growing categories of cyber threats in the country (BSSN, 2022).

What makes this threat particularly alarming is the emergence of the Ransomware-as-a-Service (RaaS) model, which enables actors with limited technical expertise to launch large-scale attacks using rented ransomware infrastructure. This criminal business model has dramatically lowered the barrier to entry for cybercriminals while simultaneously increasing both the volume and sophistication of attacks. Ransomware groups such as LockBit, BlackCat, and Cl0p now operate much like professional corporations, complete with research and development divisions, customer support services, and organized ransom negotiation teams.

3.2.2 Critical Infrastructure Interdependence and the Domino Effect

The urgency of this issue is further underscored by the growing interdependence among critical infrastructure sectors, which creates the potential for highly dangerous cascading effects. A ransomware attack on one critical infrastructure sector is no longer likely to remain isolated; rather, it can rapidly spread to other sectors that are operationally interconnected. For example, an attack on energy infrastructure may immediately affect hospital operations, clean water systems, and communication networks simultaneously.

The PDNS incident demonstrated how a single point of attack can disrupt hundreds of government services interconnected within a centralized digital ecosystem. Dependence on centralized infrastructure without adequate redundancy

and isolation mechanisms creates a classic single point of failure, making such systems particularly attractive targets for organized ransomware groups. Existing regulations do not explicitly establish security architecture standards designed to prevent single-point-of-failure conditions within the government's digital ecosystem (Lestari & Wahyudi, 2022).

3.2.3 Data Sovereignty and National Security Dimensions

Ransomware attacks against national critical infrastructure also carry profound implications for data sovereignty, an issue that remains insufficiently addressed within Indonesia's current regulatory framework. Contemporary ransomware actors no longer merely encrypt data. Under the increasingly prevalent "double extortion" model, they first exfiltrate sensitive information before encrypting systems, then threaten to publish or sell the stolen data if ransom demands are not met. When such exfiltrated data includes state secrets, intelligence information, or defense-related assets, the threat transcends cybercrime and becomes a serious national security concern (Aritonang, 2022).

Existing regulations have yet to adequately integrate ransomware threats into the broader national security legal framework. Coordination among BSSN, the State Intelligence Agency (BIN), and the Ministry of Defense in addressing ransomware incidents with national security implications remains largely ad hoc and lacks a clear legal foundation. Strengthening the regulatory framework to incorporate this dimension is therefore both urgent and strategically necessary.

3.2.4 Readiness for Global Digital Security Standards

Finally, the urgency of this study is closely linked to the increasingly stringent global digital security standards required in the context of international digital economic integration. Trading partners and foreign investors increasingly require compliance with international cybersecurity standards as a prerequisite for cooperation and investment in the digital sector. As Indonesia seeks to position itself as a leading digital economy hub in Southeast Asia, it cannot afford to disregard the imperative of harmonizing its cybersecurity regulations with international standards (Moedjiono & Sarwono, 2022).

Beyond economic considerations, strengthening cybersecurity regulation constitutes a strategic investment in building trust the essential foundation of a sustainable digital ecosystem. Without both domestic and international confidence in the security of Indonesia's digital infrastructure, the nation's digital transformation agenda will face obstacles far greater than the technical challenges currently at hand.

4. Conclusion

Based on the analysis conducted, this study arrives at several important conclusions that address the two research questions formulated.

In response to RQ1, Indonesia's current cybersecurity regulatory framework, particularly Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure, has, from a normative standpoint, established a reasonably adequate foundation for the protection of critical infrastructure. However, in addressing increasingly complex and organized ransomware threats,

this regulatory framework contains several critical structural deficiencies: fragmented inter-agency coordination and authority, the absence of binding and measurable technical cybersecurity standards, the lack of specific obligations concerning backup management, and inadequate incident reporting mechanisms with clearly defined timelines. These shortcomings render the existing framework insufficiently effective in responding to modern ransomware threats, especially those with national security implications.

In response to RQ2, the urgency of strengthening cybersecurity regulation against ransomware threats to Indonesia's critical infrastructure is grounded in four principal considerations: the escalation of ransomware into a national security threat; the growing interdependence of critical infrastructure sectors, which creates the potential for dangerous cascading effects; the significant implications for data sovereignty and national security that remain inadequately addressed under the current regulatory framework; and the need to harmonize Indonesia's cybersecurity regulations with global digital security standards in the context of international digital economic integration.

Based on these findings and conclusions, this study offers several strategic recommendations. First, Indonesia should promptly issue comprehensive implementing regulations under Presidential Regulation No. 82 of 2022, establishing legally binding minimum cybersecurity standards for each critical infrastructure sector, including standards for backup systems, encryption, access management, and periodic security testing. Second, a clear and legally robust ransomware incident response coordination mechanism should be established, designating the National

Cyber and Crypto Agency (BSSN) as the single command authority during national cyber crises. Third, Indonesia should adopt mandatory cyber incident reporting requirements with clearly defined reporting deadlines, in line with international best practices, accompanied by strict sanctions for non-compliance.

Fourth, the government should promote the establishment of a national Computer Emergency Response Team (CERT) endowed with clear legal authority, adequate technical capacity, and strong international cooperative networks to address cross-border ransomware threats effectively. Fifth, the Electronic Information and Transactions Law should be revised to explicitly classify ransomware attacks against critical infrastructure as serious criminal offenses, punishable by sanctions proportionate to the severity of the harm caused. The synergistic implementation of these recommendations would significantly enhance Indonesia's national cyber resilience and strengthen the protection of its critical infrastructure against the evolving threat of ransomware.

References

Aritonang, D. M. (2022). *Perlindungan infrastruktur informasi vital dalam hukum siber Indonesia: Tinjauan atas Perpres Nomor 82 Tahun 2022*. Jurnal Hukum dan Teknologi Informasi, 4(1), 22–41.

Badan Siber dan Sandi Negara (BSSN). (2022). *Laporan Tahunan Keamanan Siber Indonesia 2022*. Jakarta: BSSN.

Cybersecurity and Infrastructure Security Agency (CISA). (2022). Ransomware Guide: Best Practices for Ransomware Prevention and Response. *Washington, DC: U.S. Department of Homeland Security.*

European Union Agency for Cybersecurity (ENISA). (2022). *ENISA Threat Landscape 2022*. Heraklion: ENISA.

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, 171, 1–14.

Lestari, D., & Wahyudi, A. (2022). *Analisis kerentanan infrastruktur informasi vital Indonesia terhadap serangan siber: Perspektif hukum dan teknis*. Jurnal Keamanan Nasional, 8(2), 67–89.

Moedjiono, S., & Sarwono, J. (2022). *Tantangan implementasi regulasi perlindungan data pribadi di Indonesia dalam era cloud computing dan artificial intelligence*. Jurnal Ilmu Komputer dan Informasi, 15(2), 88–101.

Nugroho, Y. (2022). *Kerentanan hukum dalam tata kelola keamanan siber nasional: Kajian atas fragmentasi regulasi dan kewenangan*. Jurnal Hukum dan Teknologi, 3(1), 45–62.

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital. (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197.

Sautunnida, L. (2022). *Urgensi undang-undang perlindungan data pribadi di Indonesia: Pelajaran dari Uni Eropa dan beberapa negara Asia*. Ius Quia Iustum Law Journal, 26(3), 451–473.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2016). Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.