p–ISSN: 2723 – 6609 e-ISSN: 2745-5254
Vol. 6, No. 6, Juni 2025 http://jist.publikasiindonesia.id/

Strategic Intelligence Foresight on Ransomware Threats in Indonesian State-Owned Banks

Eggan Nachson, Puspitasari, Aloysius Mado
Universitas Indonesia
Email: nachson21@gmail.com, mipuspita@gmail.com

*Correspondence: nachson21@gmail.com

Keywords: ransomware, artificial intelligence, cybersecurity, strategic foresight, state-owned banks

ABSTRACT

The escalation of ransomware attacks, particularly those enhanced by artificial intelligence (AI), poses a significant threat to Indonesia's state-owned banks, which are critical to the national financial infrastructure. This study employs a qualitative research approach combined with strategic foresight horizon scanning to analyze ransomware trends from 2020 to 2024 and project mitigation strategies for 2025–2029. The methodology includes event identification, trend analysis, driver mapping, scenario planning, and policy roadmap formulation. Findings reveal a surge in ransomware activities, with the LockBit variant being the most prevalent, and highlight systemic vulnerabilities due to fragmented regulations and inadequate threat intelligence sharing. The study identifies three key drivers: AI-driven attack automation, regulatory fragmentation, and the rise of Ransomware-as-a-Service (RaaS). Scenario planning underscores the urgent need for adaptive cybersecurity measures, such as adopting ISO/IEC 27035 standards, enhancing Security Operation Centers (SOCs), and fostering cross-institutional collaboration. The proposed five-year roadmap outlines phased actions, including early detection system improvements, human resource capacity building, and national strategy integration. The research emphasizes transitioning from reactive to proactive cybersecurity policies, ensuring resilience against evolving AI-based threats. Implications extend to policymakers, urging regulatory harmonization and anticipatory governance to safeguard financial stability and public trust.

INTRODUCTION

In the last five years, the escalation of ransomware attacks in Indonesia's financial sector has shown an increasingly worrying trend. Based on data reported by the State Cyber and Cryptography Agency, throughout 2023, more than one million ransomware activities were detected, with the financial sector being one of the main targets (Adnyana & Ajeng Gemellia, 2021; BSSN, 2023; Hariyadi & Nastiti, 2021; Prabaswari et al., 2022). One of the incidents that highlighted the vulnerability of this sector occurred in May 2023 when Bank Syariah Indonesia (BSI) fell victim to the *LockBit 3.0* ransomware attack, which resulted in the leak of 1.5 terabytes of customer and employee data, as well as the

disruption of digital services such as ATMs and mobile banking for several days (Chakravarti, 2023). In 2024, a similar alleged attack was also reported at Bank Rakyat Indonesia (BRI), although the bank stated that customer data remained safe and that an internal investigation had been carried out (Kompas, 2024). Both incidents indicate that state-owned financial institutions are recurring strategic targets for cyber threat actors.

In this framework, the selection of state-owned banking as the focus of the study is based on its position as a critical information infrastructure that plays a vital role in the management of public funds and as the main driver of the national payment system. Disruption to the digital systems of state-owned banks not only creates technical issues but also has implications for fiscal stability and a decline in public confidence in the national financial system as a whole (Crisanto, Prenio, & Restoy, 2023). Additionally, its wide operational scope and high transaction volume make it a priority target in an attack strategy oriented towards economic gain.

As stated by Simorangkir, Purba, and Hartati (2025), the level of resilience of the cybersecurity system in the national banking sector still faces major challenges in dealing with zero-day-based threats and ransomware supported by the sophistication of artificial intelligence technology. This condition highlights the importance of shifting the approach from a technologically reactive one to a more strategic and anticipatory framework. In this context, strategic intelligence and foresight approaches are highly relevant in supporting the formulation of cyber-attack mitigation policies that are not only based on past incidents but also take into account the dynamics of future risks systematically.

Given the facts above, the urgency of this research has only grown stronger. This study aims to formulate a medium-term-oriented cyber protection strategy, particularly against the potential escalation of ransomware attacks targeting Indonesian state-owned banks from 2025 to 2029. Through the *foresight intelligence* approach, it is hoped that the results of this research can make a concrete contribution to the formulation of early prevention policy directions that are more proactive, systematic, and contextual to the challenges of the digital era.

In line with the increasing complexity of ransomware attacks and the high level of risk exposure faced by the state-owned banking sector, this research is intended to make a strategic contribution through the application of foresight intelligence approaches. The problems that have been formulated previously serve as a foothold in compiling an in-depth analysis of the dynamics of attack escalation, institutional preparedness capacity, and forms of early prevention efforts that align with the needs of strengthening cyber resilience in the future. The scope of this study is limited to identifying trends and incidents of ransomware attacks that occurred from 2020 to 2024, while the projection of prevention efforts is directed towards the period of 2025 to 2029. For this reason, a qualitative approach is used as the main method, which is equipped with the *foresight horizon scanning* technique through five analytical stages: event identification, trend analysis, driver mapping, scenario planning development, and preparation of policy roadmap (Saritas, 2016). All of these approaches will be used to frame the follow-up discussion, which includes conceptual studies, previous literature reviews, and in-depth

thematic analysis that underpins the formulation of intelligence-based early prevention strategies against artificial intelligence (AI)-based ransomware threats targeting the state-owned banking sector in Indonesia.

METHOD

This study employed a qualitative research approach to explore the strategic anticipation of ransomware threats, particularly those powered by artificial intelligence (AI), targeting state-owned banks in Indonesia. The selection of a qualitative design was grounded in the need to generate in-depth, context-rich insights that go beyond statistical generalization, enabling a comprehensive understanding of systemic vulnerabilities and policy gaps.

To guide the investigation, the *Scientific Inquiry for Intelligence Analysis* framework developed by Prunckun (2010) was applied. This framework emphasizes analytical rigor in exploring security threats by combining intelligence assessment, empirical validation, and structured interpretation of trends. The methodology integrates this intelligence-based framework with a *foresight horizon scanning* approach, as conceptualized by Saritas (2016), to anticipate future developments and policy needs.
The foresight process consists of five interconnected phases:

1. **Event Identification**: Mapping significant ransomware incidents in the Indonesian state-owned banking sector from 2020 to 2024. This phase involved collecting data from official government reports, cybersecurity databases (e.g., BSSN, OJK), and peer-reviewed journal articles.
2. **Trend Analysis**: Identifying temporal patterns and escalation tendencies of AI-based ransomware attacks, including anomalies in cyber traffic and variations in ransomware variants. This was supported by secondary data from the Indonesian Cybersecurity Landscape reports and relevant international cybersecurity literature.
3. **Driver Mapping**: Analyzing key enabling factors contributing to the escalation of threats. This included technological advancements in AI-assisted attacks, the rise of *Ransomware-as-a-Service* (RaaS), and regulatory or institutional weaknesses in cyber defense coordination.
4. **Scenario Development**: Constructing four strategic future scenarios for the 2025–2029 period based on two axes: the adaptability level of banking cybersecurity systems and the sophistication of AI-powered ransomware threats. Each scenario was developed through expert judgment, empirical data extrapolation, and comparative policy analysis.
5. **Policy Roadmap Formulation**: Designing a sequential mitigation strategy aligned with the projected scenarios. This roadmap outlined annual action steps involving standard adoption (e.g., ISO/IEC 27035), *SOC* development, threat intelligence integration, simulation-based testing, and cross-agency coordination.

Data were primarily collected through document analysis from official regulatory bodies (e.g., Financial Services Authority, BSSN), global cybersecurity reports (e.g.,

CrowdStrike, ENISA), and scientific publications relevant to cybersecurity governance, strategic foresight, and AI-based threats.

By combining scientific intelligence analysis with foresight planning, this methodology aims to bridge the gap between reactive cyber policies and strategic, anticipatory governance. The result is a policy-relevant, evidence-based roadmap tailored to enhance the cyber resilience of Indonesian state-owned banks in the face of evolving digital threats.

RESULTS AND DISCUSSION

Banking Cybersecurity Regulations in Indonesia

In order to strengthen the resilience of the national financial sector to digital threats, various regulations have been issued by the Financial Services Authority (OJK), the State Cyber and Cryptography Agency (BSSN), and the central government. POJK No. 11/POJK.03/2022 is the main regulation that regulates the implementation of information technology by commercial banks, with an emphasis on aspects of information technology governance, risk management, and the application of the principles *of confidentiality, integrity,* and *availability* (CIA) (Badan Siber dan Sandi Negara, 2022; Badan Siber Dan Sandi Negara, 2023; BSSN, 2022; Haryanto & Sutra, 2023; Sutra & Haryanto, 2023). In addition, this regulation also regulates banks' obligations to report cyber incidents and carry out regular technology audits (Financial Services Authority, 2022). Previously, POJK No. 38/POJK.03/2016 had regulated the implementation of risk management in the use of information technology, but its scope was still limited and less responsive to the development of the complexity of digital threats. On the other hand, Presidential Regulation No. 82 of 2022 stipulates the banking sector as part of the *vital information infrastructure* (IIV) that must receive maximum protection, although the implementation of this regulation is still general and has not yet detailed its operational technical guidelines. Meanwhile, SEOJK No. 29/SEOJK.03/2022 provides technical guidelines regarding IT security, including the obligation to carry out *vulnerability assessment* and *penetration testing* as part of systematic preventive measures (Financial Services Authority, 2022). Another relevant regulation is BSSN Regulation No. 4 of 2021 which contains a comprehensive cyber risk management framework for electronic system operators, including the stages of asset identification, risk analysis, and response management to digital incidents (State Cyber and Cryptography Agency, 2021).

However, the overall regulation has not fully addressed the contemporary challenges posed by increasingly sophisticated forms of cyberattacks, particularly those that utilize *artificial intelligence* (AI) to accelerate the escalation of attacks, avoid security system detection, and exploit loopholes in cloud-based systems (CrowdStrike, 2025). POJK No. 11/POJK.03/2022 does not explicitly regulate the types of AI-based threats, nor collaborative mechanisms in cross-institutional detection. In addition, the deadline for reporting cyber incidents set for three business days is considered inadequate when compared to the speed and destructive power of AI-based cyberattacks, which in many cases can result in systemic disruptions in a matter of hours (National Institute of

Standards and Technology, 2024). The mechanism for sharing *threat intelligence has* also not been regulated operationally and in real-time in existing regulations, even though it is considered crucial in anticipating the spread of systemic attacks (CONCORDIA, 2021).

In terms of substance, these regulations reflect the regulator's commitment to building a solid cybersecurity governance framework for the banking sector. However, at the implementation level, challenges arise along with the lack of optimal integration between regulatory agencies, slow incident reporting, and the lack of policy design based on projections and medium-term scenarios. The approach, which is still reactive, is not in line with the dynamics *of* the escalation of modern ransomware threats that are adaptive and layered, and are growing rapidly through the support of smart technology (Cybersecurity and Infrastructure Security Agency, 2024).

Ransomware Threats to Banking

In the development of an increasingly complex digital ecosystem, the state-owned banking sector in Indonesia is facing an escalation of *ransomware* threats strengthened by *artificial intelligence (AI) technology*. Attack patterns that were previously static have now evolved to be adaptive and dynamic, making early detection efforts increasingly challenging. Cutting-edge variants such as *RansomAI* reportedly utilize *a reinforcement learning approach* to automatically adjust deployment patterns based on the conditions of the target network, allowing them to penetrate systems with high efficiency and without any unexpected attack patterns (Zhou, Lin, & Patel, 2023). The *process of lateral movement* and mapping of digital assets is automated, allowing threat actors to exploit system gaps in minutes (CrowdStrike, 2025), ultimately weakening the effectiveness of manual responses that banking institutions have relied on.

The annual report *of Indonesia's Cybersecurity Landscape 2024* shows that throughout the year there were 514,508 *ransomware* activities detected in the national cyberspace. Of these, the LockBit variant is the most dominant type with 102,798 activities, and the financial sector, including banking, is categorized as one of the sectors with the highest level of vulnerability (State Cyber and Cryptography Agency, 2024). The attack techniques used vary, ranging from *phishing*, abuse of administrator privileges, to exploitation of security loopholes from application systems that have not been updated. This situation is increasingly crucial when targeting institutions such as state-owned banks that have large amounts of digital assets and public mandates as fund managers and state payment systems.

From a financial perspective, *ransomware* attacks on state-owned banks have a significant impact. According to the report Halcyon 2025, the average loss due to a single incident in the global financial sector reached USD 6.08 million by 2024. This amount includes the cost of system recovery, IT infrastructure replacement, ransom payments, and loss of revenue due to service interruptions. For example, in the case of the attack on the EquiLent platform, operational disruptions caused the affected financial institutions to adjust capital and bear the surge in operational costs. In Indonesia, Bank Syariah Indonesia (BSI) is one of the real examples of the financial impact of *ransomware* attacks.

In May 2023, BSI was attacked by *the LockBit* 3.0 ransomware group which claimed to have stolen 1.5 terabytes of customer data and demanded a ransom of IDR 200 billion. This attack caused disruption of banking services, including ATMs and mobile banking applications, for several days, impacting customer operations and trust (Kompas.id, 2023). If such a scenario were to occur in the *core banking systems* of other state-owned banks, then the risk to operational and financial stability would be much greater.

Reputational damage is another aspect that often has long-term impacts. Data leak incidents and paralysis of digital services due to *ransomware attacks* have caused a disruption of public trust in the competence of state financial institutions in maintaining information confidentiality and security. Affected reputations not only affect customer loyalty, but also weaken the institution's position in attracting new investors and maintaining internal financial stability. Given the strategic position of state-owned banks as development agents and implementers of state fiscal policies, the impact of this reputation can develop into a systemic problem.

The absence of relevant regulatory updates and low adoption of predictive technologies magnify the potential for threat escalation. The absence of explicit provisions on AI-based threats in domestic regulations, weak real-time incident reporting systems, and non-optimal *threat intelligence sharing* mechanisms between institutions open up space for systemic incidents to occur. In the worst-case scenario, coordinated attacks on state-owned banks can simultaneously trigger fiscal disruption and reduce public confidence in the digital financial system.

To face these challenges, the adoption of international standards such as *ISO/IEC 27035* is considered very important. This standard provides a systematic approach to handling security incidents, starting from the process of detection, isolation, recovery, to post-attack learning (International Organization for Standardization, 2018). However, most of the regulations in force in Indonesia, such as POJK and Presidential Regulations, have not fully integrated these principles into institutional technical governance. The absence of early *containment* guidelines and weak coordination between regulators magnify the potential for losses and slow down the recovery process which should be integrated and fast.

Thus, the strategy to strengthen cybersecurity in the state-owned banking sector should not only focus on technical aspects, but also lead to regulatory transformation that is adaptive to AI-based threat dynamics. The development of *scenario-based preparedness scenarios*, strengthening internal cyber intelligence capacity, and harmonizing policies with global standards must be the main elements in designing the cyber resilience of the country's financial sector as a whole.

Foresight Horizon Scanning

Event

In the framework *of horizon scanning*, the event identification stage is carried out to map actual events that are relevant and have a direct impact on information system security in the state-owned banking sector. Based on the analysis of the period 2020 to

2024, there are two main events that clearly reflect the increasing intensity and complexity of *ransomware attacks* against state-owned financial institutions.

The first event occurred in May 2023, when the LockBit 3.0 ransomware managed to penetrate the digital security system of Bank Syariah Indonesia (BSI). The attack resulted in a massive data leak of up to 1.5 terabytes, and paralyzed digital banking services, **including *mobile banking*,** ATM networks, and other internal systems for more than five days (Chakravarti, 2023). The immediate effect of this attack was felt by millions of customers in the form of disrupted access to basic banking services. Given BSI's status as an entity as a consolidated entity of national sharia institutions, this incident also triggered a decline in public confidence in the readiness of new institutions in managing strategic cyber risks.

The second incident concerns an alleged *ransomware* attack on **Bank Rakyat Indonesia (BRI)** at the end of 2024. Although there has been no official confirmation regarding the data leak, media reports say that this incident had an impact on the disruption of several digital services. The bank conducted an internal investigation to trace the cause and scope of the incident. This event reinforces the perception that artificial *intelligence-based ransomware threats* have reached SOEs' security systems that were previously seen as relatively resilient to large-scale cyberattacks (Kompas, 2024).

In line with this event, *the 2024 Indonesian Cybersecurity Landscape* report released by the State Cyber and Cryptography Agency shows that in 2024 alone, there will be 514,508 *ransomware* activities recorded in Indonesia's cyberspace. Of these, the LockBit variant was recorded as the most active, with 102,798 activities detected and traced by the national monitoring system (State Cyber and Cryptography Agency, 2024). This data confirms that ransomware is the form of attack with the most significant growth rate and targets vital sectors, including finance.

The two major incidents involving BSI and BRI not only illustrate an increase in the frequency of attacks, but also demonstrate an increasingly systemic pattern of attacks, with a tendency to exploit internal vulnerabilities of systems through adaptive infiltration methods. With the use of AI, cybercriminals are able to map and exploit critical paths in a bank's digital infrastructure with high efficiency and extremely short reaction times.

Therefore, these two events are important stepping stones in the process of strategic intelligence-based foresight. The identification of these incidents not only provides an overview of the characteristics of current threats, but also provides an empirical basis for developing medium-term mitigation scenarios for the period 2025–2029, as part of measurable and contextual early prevention measures.

Trend Analysis

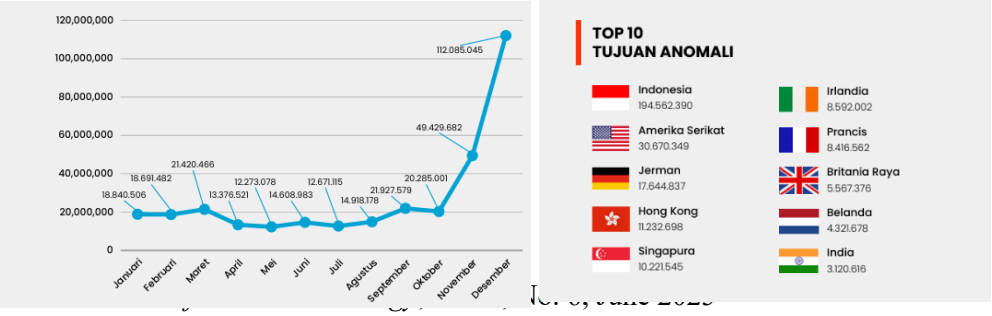

Figure 1. Traffic Anomalies of Cyber Attacks in Indonesia

Referring to *Indonesia's Cyber Security Landscape in 2024*, cyber anomaly traffic in Indonesia throughout the year shows an increasing trend, especially towards the end of the year. The monthly graph shows a relatively fluctuating anomaly intensity during the period January to October 2024, with a range of between 12 and 21 million activities per month. However, there was a drastic spike in November which recorded 49,429,682 activities, and reached its peak in December with 112,085,045 activities. This doubling of the increase in a span of one month indicates a significant escalatory trend (State Cyber and Cryptography Agency, 2024).

This trend indicates that the national digital system is under higher pressure in the year-end period, allegedly related to the increased volume of digital transactions, the tightening of security controls during the long holiday period, as well as the exploitation of security loopholes that have not been fully closed. This exponential increase reflects the urgency of strengthening early detection systems that are not only reactive to incidents, but capable of predicting seasonal cycles based on annual attack patterns.

In addition to depicting temporal dynamics, the graph also shows that Indonesia is ranked highest globally as the country with the most cyber anomaly traffic in 2024, reaching 194,562,390 activities. This number far exceeds other countries such as the United States (36,670,349), Germany (17,644,837), and Singapore (10,221,545). The dominance of this position indicates the high exposure of the vulnerability of national systems to various types of attacks, including *ransomware*, and confirms that Indonesia has become a prime target in the global digital threat landscape (National Cyber and Cryptography Agency, 2024).

In the foresight framework, these findings reinforce the trend analysis phase as an important stage in mapping the tendency of recurrent and progressive threats. The identification of non-linear escalation patterns at the end of the year provides strategic signals for the formulation of medium-term mitigation policies. This pattern also strengthens the need to integrate temporal supervision of the digital banking system, especially in the state-owned sector which has the characteristics of large transactions, attachment to the national system, and high exposure to systemic cyber-attacks.

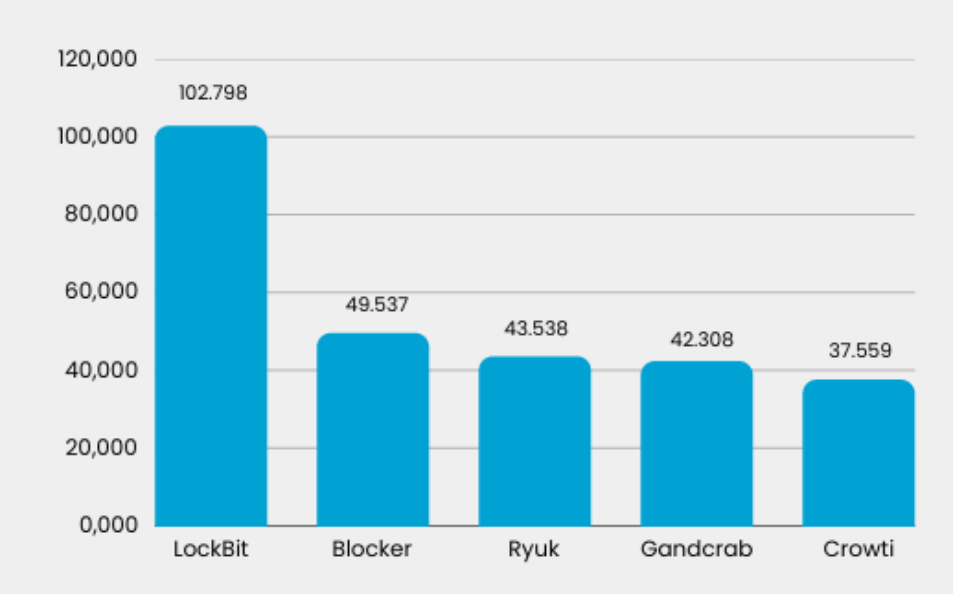

Figure 2. Trend Images of Lockbit Attack Types

Based on *the 2024 Indonesian Cybersecurity Landscape* report, 514,508 ransomware activities were detected in the national cyberspace throughout the year (State Cyber and Cryptography Agency, 2024). *Ransomware* is a form of *malware* that works by encrypting the victim's system or data, then requesting payment as a condition for restoring access to the data. These types of attacks target multiple layers of entities, from individuals to strategic institutions, and have a broad impact on the operational, financial, and reputational aspects of the affected institutions.

The bar graph visualization presented in the report illustrates the five ransomware variants with the highest attack intensity found in Indonesia's cyberspace. The LockBit variant takes the top spot with 102,798 activities, which is significantly higher than other variants. Below it, there are respectively the Blocker variant (49,537 activities), Ryuk (43,538 activities), Gandcrab (42,308 activities), and Crowti (37,559 activities). The dominance of LockBit indicates the level of effectiveness and penetration ability of this variant in exploiting the weaknesses of information systems, including in the complex digital infrastructure of the financial sector and having high data traffic.

The concentration of activity on certain variants shows that ransomware escalation is not only happening quantitatively, but also shows a pattern of technical consolidation in certain *strains* that are more aggressive and difficult to combat. This phenomenon is an important indicator in the *trend analysis stage in the* foresight *approach*, because it reveals the direction of threat evolution and the technical preferences of cyber actors in selecting the most effective attack vectors against critical infrastructure.

The impact on the state-owned banking sector is very strategic considering the high volume of data, transactions, and dependence on electronic systems in these institutions. Attacks launched by highly destructive *ransomware* variants such as LockBit and Ryuk have the potential to cause widespread disruption of banking services, loss of public trust, and increased operational costs as a consequence of the recovery and re-security process.

For this reason, a structured anticipatory policy is needed, based on the analysis of active variant trends and strengthening the detection system against specific attack patterns on the national banking sector.

Drivers

Driver 1: Automation and Complexity of Artificial Intelligence-Based Attack Technologies

The development of *artificial intelligence* (AI) technology has driven the evolution of ransomware from static attacks to adaptive and automated attack instruments. Today, these types of attacks are not only capable of executing encryption of data, but can also perform *real-time scanning* to identify system weaknesses, penetrate the network through *lateral movement* techniques, and tailor the infection method to the target profile at hand. Variants such as LockBit and Ryuk have adopted *a machine learning-based* approach to improve attack efficiency and avoid *signature-based detection* (Zhou, Lin, & Patel, 2023).

The *CrowdStrike Threat Report 2025* shows that more than 30% of global ransomware incidents currently use AI-integrated *automation toolkit* technologies , such as *fileless infection* techniques, *stealth* capabilities, and *auto-deploy payloads*. This condition causes the time it takes to disable a target system (*time-to-compromise*) to be drastically reduced—from a matter of hours to just a few minutes (CrowdStrike, 2025).

This trend indicates that cybersecurity policies in the financial sector, especially state-owned banks, must be designed with the speed and flexibility of attacks in mind. Conventional mitigation strategies that are not predictively based will have a hard time responding to ever-changing attack patterns in real-time.

Driver 2: Policy Fragmentation and Weak Cyber Intelligence Exchange

Although a number of regulations such as POJK No. 11/POJK.03/2022 and Presidential Regulation No. 82 of 2022 have been issued in response to increased cyber risks, the weakness of inter-agency coordination and the absence of an *operational national threat intelligence sharing* system remain the main challenges. Disintegration between regulatory authorities, industry players, and digital security service providers slows down the process of early detection and response to systemic cyberattacks.

Research shows that failures in building real-time threat information exchange systems, including sharing attack metadata and *tactics, techniques, and procedures (TTP),* have become a significant obstacle in mitigating ransomware attacks in the financial sector in various countries, including in Asia (CONCORDIA, 2021). This causes threat management strategies to run in silos, and do not reflect the need for a collective response in the face of coordinated attacks.

In the context of *foresight*, the weakness of intelligence sharing infrastructure should be seen as a crucial driver that can magnify systemic risks in the state-owned banking sector if not anticipated through collaborative and integrated cross-agency policy frameworks.

Driver 3: Industrialization of Cybercrime through Ransomware-as-a-Service (RaaS)

The phenomenon of industrialization of digital crime through *Ransomware-as-a-Service (RaaS)* schemes has created conditions where attackers no longer need to have in-depth technical expertise. Attackers can purchase or rent ransomware services available on dark web forums, which are generally equipped with graphical user interfaces, technical guides, and crypto-based support systems for transactions and communications.

The study found that more than 60% of ransomware campaigns targeting the financial sector today come from the RaaS model. The subscription fee for these services ranges from USD 200 to 300 per month, but it can generate huge losses for the financial institutions that are victims, both financially and reputationally (Kumar & Upadhyay, 2023).

This model causes the threat landscape to become more dynamic and difficult to predict, as it expands access to attack tools to actors who previously had no technical resources. In the framework of *foresight*, the existence of RaaS is a strategic signal of the need for a predictive approach that is able to simulate a spectrum of actors, ranging from state actors to opportunistic criminals with access to dangerous platforms.

Scenario Planning

X-Axis – Adaptability of Cybersecurity Systems

This axis represents the capacity of state-owned banking institutions in developing and adapting their cyber defense systems in line with the increasingly complex dynamics of digital threats, especially against artificial intelligence-based ransomware attacks. This dimension includes internal regulatory aspects, operational readiness, and the existence of an adaptive incident detection and response system. The level of maturity in the implementation of international information security standards such as *ISO/IEC 27001* and *ISO/IEC 27035*, as well as the ability to upgrade system architectures and security procedures, are important indicators in measuring the level of institutional adaptability (International Organization for Standardization, 2018).

Other elements that are also taken into account are the technical readiness of human resources in charge of the Security *Operation Center*, the functioning of the threat *intelligence sharing system* across agencies, and the effectiveness of internal audits and periodic system vulnerability testing. Institutions with a high level of adaptation tend to have implemented the principle of *zero trust architecture*, as well as build real-time incident reporting schemes to accelerate responses to cyber anomalies (National Institute of Standards and Technology, 2024; CONCORDIA, 2021).

Y-axis – AI-Based Cyberattack Capabilities

This axis measures the complexity and technical capabilities of cyberattacks that use *artificial intelligence technology*, particularly in the form of *ransomware* targeting the banking sector. Attacks in this spectrum are characterized by a high level of automation, the use of *stealth* techniques, the exploitation of *zero-day vulnerabilities*, and the use of rapid deployment tactics such as *lateral movement*. The LockBit and Ryuk

variants of ransomware are case examples of how AI is used to increase the effectiveness of infiltration and reduce the likelihood of being detected by traditional security systems (Zhou, Lin, & Patel, 2023).

The complexity of threats is also increasing with the *rise of the Ransomware-as-a-Service (RaaS)* model, which allows actors with low technical capabilities to launch large-scale attacks using ready-to-use devices. In this context, the magnitude of the impact is determined not only by the sophistication of the technology used, but also by the accessibility of the service-based digital crime ecosystem (Kumar & Upadhyay, 2023). Increased attack capabilities mean that defense systems that are not anticipatively oriented will be vulnerable to adaptive and simultaneous attacks.

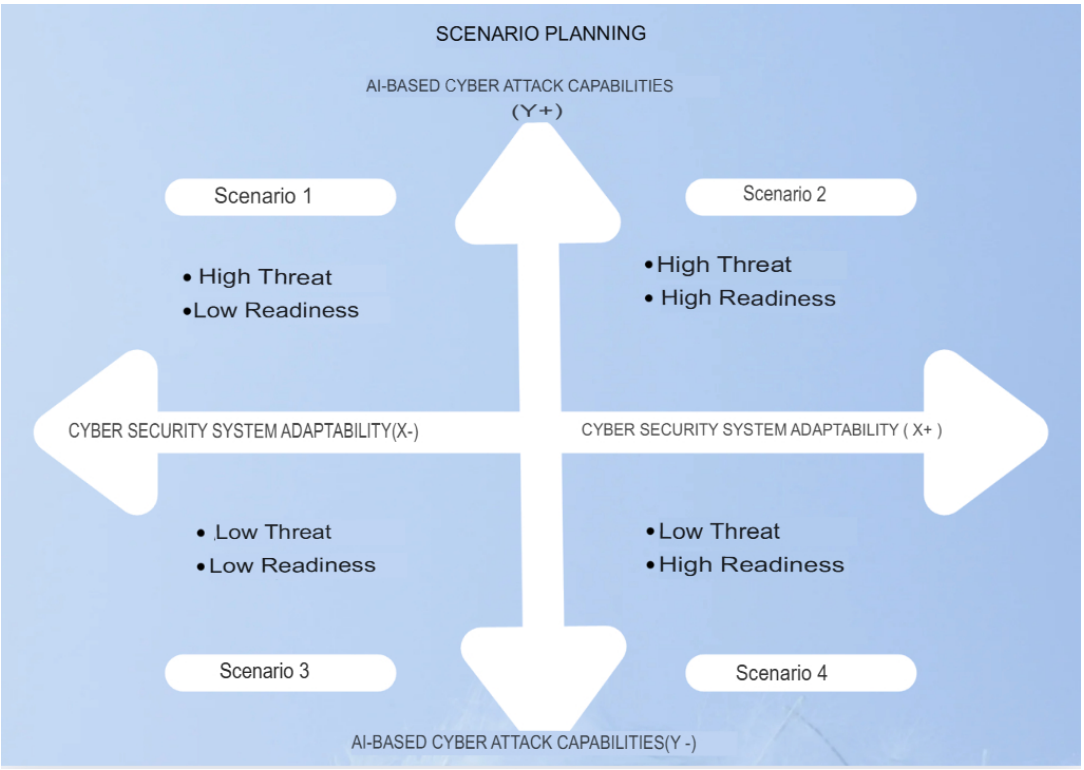

Figure 3. AI-Based Ransomware Threat Scenario Planning Drawing on State-Owned Banking (2025–2029)

Scenario 1

This scenario represents the most critical condition for the state-owned banking sector, where the intensity and complexity of *artificial intelligence* (AI)-based cyberattacks have increased significantly, while the adaptability of digital security systems remains weak or even regressive. In this context, threat actors are expected to increasingly rely on *AI-enhanced ransomware* types that have the ability to automate exploitation, perform *lateral movements*, simultaneously encrypt core systems, and be able to circumvent signature-based detection systems (Zhou, Lin, & Patel, 2023).

This condition is exacerbated by a number of internal factors, such as the implementation of security audits that have not been thorough, the lack of integration of *threat intelligence sharing systems* between banking institutions and regulators, and the

limitation of human resources who have not been equipped with the expertise to detect AI attacks quickly and responsively. In this scenario, attacks on *the core banking system* have the potential to paralyze key services such as ATMs, *mobile banking*, and national payment system networks, which could ultimately trigger a crisis of public trust in state financial institutions (Simorangkir, Purba, & Hartati, 2025).

Threat projections for the period 2025–2029 indicate the increasing use of *the Ransomware-as-a-Service (RaaS)* model, driven by low attack costs and high potential financial gains. This phenomenon makes state-owned banking a strategic target, given its role in the management of public funds, the distribution of social assistance, and its vital function in keeping the national payment system stable (Kumar & Upadhyay, 2023).

Responding to these conditions, the necessary mitigation policies must be transformative, starting from the integration of automatic detection systems based on *ISO/IEC 27035 standards*, strengthening the operations of *the Security Operation Center* (SOC), and the preparation of an incident handling framework that allows the implementation of *early containment* within less than an hour of the identification of the attack (International Organization for Standardization, 2018; National Institute of Standards and Technology, 2024). In addition, *the policy roadmap* needs to set a deadline for incident reporting a maximum of 24 hours after the incident and accelerate the construction of a real-time national threat intelligence data center.

If not anticipated through *a foresight-based* approach, this scenario can trigger a systemic crisis in the country's financial sector. The impact is not only on the disruption of fiscal stability and the process of disbursing public funds, but also on the long-term loss of public trust in the national financial system. Therefore, the policy response that is built must no longer be reactive, but must be based on projected technological trends and attack patterns that are growing exponentially.

Scenario 2

This scenario represents a situation where the complexity and escalation of cyberattacks, especially *ransomware* that utilizes *artificial intelligence* (AI) technology, continue to increase. However, this situation is optimally responded to by state-owned banking institutions through the readiness of a high and integrated cybersecurity system. In this configuration, state-owned banks have implemented a number of advanced digital defense technologies such as *automated threat detection*, *zero trust architecture*, and *AI-driven threat analytics systems* that are able to detect and respond to anomalies before reaching critical systems (Suvorova, 2023).

Although the threat level remains high, attack attempts are carried out by cyber actors using advanced methods such as *machine learning*, *fileless malware*, and *ransomware-as-a-service (RaaS) models* that allow penetration into multiple systems simultaneously and in a structured manner (CrowdStrike, 2025). The high readiness of the institution is reflected in the strengthening of *the Security Operation Center* (SOC) unit, increasing the capacity of human resources through continuous training in the field of *cyber threat intelligence*, and the implementation of incident reporting systems that are

directly connected to international protocols such as *ISO/IEC 27035* (International Organization for Standardization, 2018).

For the period 2025–2029, it is estimated that the pace of attacks will be faster and more automatic. This demands a strategic response based on predictive analytics and pre-tested planned scenarios. Relevant mitigation policies include the establishment of *a threat intelligence sharing system* across state-owned institutions and regulators, the establishment of a national cybersecurity crisis control center for the banking sector, and the implementation *of regular cyber resilience testing* to test emergency response capacity against various forms of digital threats.

Although high-scale threats remain looming, this scenario suggests that systemic risks can be significantly minimized if the defense systems deployed are able to adapt and react in a timely manner. Relevant *foresight strategies* emphasize the importance of consistency in strengthening institutional structures, openness in incident reporting, and cross-sectoral integration based on predictive data as the basis for the formulation of responsive and sustainable security policies (Saritas, 2016; Linkov & Kott, 2019).

With the readiness capacity that continues to be maintained and improved, state-owned banks have the opportunity to become a key pillar in strengthening the national cyber resilience architecture. This strategy is considered effective in reducing the risk of systemic disruptions, maintaining the sustainability of public services, and increasing public trust in state-owned financial institutions amid increasingly complex digital threat dynamics.

Scenario 3

This scenario reflects a situation when *the* frequency of ransomware attacks against the state-owned banking sector is at a minimum level in a given period. However, this condition is not accompanied by an adequate increase in security system readiness. The absence of major attacks creates a false perception that the digital environment is in a secure condition, leading to a decrease in the urgency to update the cybersecurity defense architecture, test system vulnerabilities, and strengthen the capacity of human resources to identify potential cyber threats that are latent and invisible.

In a configuration like this, the reinforcement of the security system tends to be overlooked. Early detection tools have not been systematically developed, training for personnel in Security *Operation Centers* (SOCs) is minimal, and the implementation of *a zero-trust-based* security architecture has not been a priority. Cyber incident reporting procedures are still reactive and administrative, without the support of an integrated real-time reporting system. In fact, incident response protocols have not yet referred to international standards such as *ISO/IEC 27035*, which emphasizes the importance of a structured incident handling system (International Organization for Standardization, 2018). In addition, the absence of red *team exercises*, weak cross-agency collaboration in *threat intelligence sharing*, and lack of information security literacy at the management level add to the complexity of vulnerability in this situation.

Although incidents appear to be rare, global trends suggest that cybercriminals are likely to take advantage of situations like this to prepare for attacks with greater scale and

level of precision in the future (Suvorova, 2023). With the development of AI-based technologies and automation, attacks can be designed to execute quickly, massively, and in a very short duration, so that they are not detected in the early stages (Zhou, Lin, & Patel, 2023). When systems are not equipped with machine learning-based predictive detection capabilities, the vulnerability of institutions to large-scale threats becomes very high.

Mitigation in this scenario needs to start from strengthening the foundation of the cybersecurity system. This includes the development *of baseline security controls*, improvement of the quality and frequency of technical training for human resources, the preparation of *incident contingency plans*, and the integration of procedures with international standards as recommended by *NIST SP 800-61* (National Institute of Standards and Technology, 2024). Regulatory reforms are also needed to require the implementation of periodic security audits, thematic simulation of incident scenarios, and mandatory cyber incident reporting within 24 hours of the incident.

This scenario emphasizes that the condition of minimal attacks is not a strong indicator of the resilience of digital systems. Precisely in a stagnant phase like this, structural weaknesses and potential latent threats are the main risks that can have a destructive impact when escalation occurs. Therefore, foresight-based approaches remain relevant and important to use, even in low-threat contexts, to develop anticipatory strategies that are oriented to the medium term and based on technological projections and rapidly changing attack dynamics.

Scenario 4

This scenario illustrates an optimal situation, where the intensity of *ransomware* attacks against the state-owned banking sector is relatively low, but faced with a high and consistent level of cybersecurity preparedness. The low threat escalation does not lead to an easing of protection, but rather is used as a momentum to strengthen system resilience through anticipatory approaches and medium-term risk management.

In this condition, the digital defense system implemented by state-owned banks has adopted the principle of *zero trust architecture*, strengthened machine learning-based detection systems, and followed international standards such as *ISO/IEC 27001* and *ISO/IEC 27035* in the management of information security incidents (International Organization for Standardization, 2018). Personnel in charge of cyber security have been provided with routine training based on attack simulations (*red team exercises*), and are actively updating their capabilities to deal with new cyber-attack patterns. Incident reporting procedures are conducted in *real-time* and are connected to the global incident response framework as set forth in *NIST SP 800-61 Rev. 3* (National Institute of Standards and Technology, 2024).

Although the intensity of attacks is currently relatively low, institutions still apply *predictive analytics-based* approaches and *foresight scenario planning* as tools to project changes in threat patterns in the future. These efforts are realized through strengthening *the threat intelligence sharing* system between agencies, regular system resilience *testing*,

and the establishment of a *cyber crisis command center* that is ready to operate when needed.

The success of maintaining this stability is largely determined by the alignment between regulations and operational infrastructure. Adaptive government policy support, system interoperability standards, and incentives for institutional capacity building initiatives are important elements in shaping a *risk-based cybersecurity* approach. In this context, *cyber resilience* is understood not only as a response to incidents, but as part of a strategic learning system integrated in institutional governance.

During the 2025–2029 projection period, this scenario offers a reflection of best *practices* in managing cybersecurity when threat conditions are low. Consistency in maintaining high readiness allows state-owned banks to become the locomotive in strengthening the national digital resilience ecosystem. This position becomes crucial to maintaining the continuity of public services and fiscal stability as the threat escalates again.

RoadMap

In the framework of *foresight analysis*, the current position of the state-owned banking sector (SOEs) in Indonesia can be classified as in **Quadrant I**, which is a condition with a high threat escalation but with a low level of adaptive readiness. Based on data obtained from *the 2024 Indonesian Cybersecurity Landscape* published by BSSN, it is recorded that ransomware variants such as *LockBit*, *Ryuk*, and *the Ransomware-as-a-Service* (RaaS) model have been active and target various national strategic sectors. In particular, LockBit is the most dominant variant by detecting more than 102,000 activities throughout 2024, indicating the high intensity of attacks that have integrated artificial intelligence elements in the system of deployment, penetration, and detection evasion (State Cyber and Cryptography Agency, 2024).

However, in terms of the readiness of the cybersecurity system of state-owned banking institutions, the response to the dynamics of these threats still does not show optimal adaptive capabilities. Two important events are concrete indications of the weak structural resilience of the institution, namely the LockBit 3.0 ransomware attack on Bank Syariah Indonesia (BSI) in May 2023 which caused operational service disruptions for several days (Chakravarti, 2023), and reports of alleged similar incidents that befell Bank Rakyat Indonesia (BRI) at the end of 2024 which have not been accompanied by open confirmation regarding the actual impact (Kompas, 2024). This weakness is shown by the delay in incident reporting, the lack of adoption of incident handling standards such as *ISO/IEC 27035*, and the low integration in *the threat intelligence sharing system* between banks and between banks and regulators (Simorangkir, Purba, & Hartati, 2025).

Therefore, the strategic position of the state-owned banking sector can be said to be in a fairly high vulnerability zone. The high level of artificial intelligence-based cyber threats is not in line with tactical and structural readiness in responding, mitigating, and anticipating systemic attacks. This situation underscores the importance of the formulation of prevention policies based on *a foresight approach*, which is not only

technical in nature, but must also involve institutional, regulatory and multi-stakeholder collaboration aspects in the national cybersecurity system.

Table 1. Cyber Security Policy Roadmap Table in State-Owned Banking

Year	Strategic Focus	Key Actions	Targets and Indicators
2025	*Early Detection and Standardizatio n*	- Adoption of ISO/IEC 27035 across state-owned banks	- All SOEs adopt minimum information security standards
		- Annual NIST-based cybersecurity readiness audit	- Incident reporting <24 hours (OJK Compliance)
		- Establishment of a ransomware-specific AI incident response team	
2026	*HR Capacity and SOC Infrastructure*	- SOC training on AI-based threat detection	- >90% of SOC personnel are certified
		- Increased capacity of SIEM (Security Information and Event Management)	- SIEM systems installed in 100% state-owned banks
2027	*Collaboration and Threat Intelligence Sharing*	- Threat sharing platform between SOEs and regulators	- Active and real-time threat sharing platform
		- Cross-sector coordination protocol (Bank-BSSN-OJK)	- Joint simulations are conducted twice a year
2028	*Scenario Simulation and Resilient Resilience*	- National Scale Red Team Exercise	- Cyber Resilience Index for the SOE sector >80%
		- RaaS attack simulation with preparedness assessment	
2029	*Evaluation and Integration of National Strategies*	- Evaluation of the roadmap and integration into the National Cybersecurity Strategy	- State-Owned Enterprises (SOEs–national integration documents) ratified
		- Cyber contingency plan based on national level AI scenarios	- Zero-day response plan implemented

Year 2025

The initial stage in 2025 focuses on strengthening early detection systems and standardizing cybersecurity governance standards across state-owned banks. One of the strategic priorities is the implementation of the international standard *ISO/IEC 27035* related to information security incident management. This standard is designed to ensure that each institution has a systematic framework in efficiently detecting, responding to, and recovering from cyber incidents (International Organization for Standardization, 2018). In addition, an annual cybersecurity readiness audit based on the framework of the *National Institute of Standards and Technology* (NIST) has also begun to be implemented, to measure the level of compliance, operational readiness, and effectiveness of the IT security system that has been implemented (National Institute of Standards and Technology, 2024).

Furthermore, this year has been an important momentum to establish *an AI-based ransomware dedicated Computer Security Incident Response Team* (CSIRT), in response to the rise of automated and adaptive attacks such as LockBit and Ryuk (Zhou, Lin, &

Patel, 2023). This team is expected to be able to provide a quick response to incidents with the ability to *quickly contain* and escalate strategic information in real-time. The target indicators of success in this stage include the full adoption of minimum-security standards by all state-owned banks and the achievement of incident reporting times in accordance with OJK regulations, which is a maximum of 24 hours from detection. With these measures, the technical and institutional foundations for building medium-term resilience begin to be strengthened comprehensively.

Year 2026

The strategic focus in 2026 is directed at strengthening the capacity of human resources and supporting infrastructure in dealing with AI-based cyberattacks. The main step includes intensive training for Security Operation Center (SOC) personnel, especially in automated threat detection capabilities based on *machine learning* technology and *AI-assisted threat analytics*. This training aims to improve the technical responsiveness of personnel in identifying system anomalies and taking mitigation actions quickly and appropriately. The target to be achieved is a minimum of 90 percent of SOC personnel certified nationally or internationally in the field of AI-based cyber threat detection (CrowdStrike, 2025).

In addition to strengthening human resources, institutions are also required to increase the capacity of SIEM (*Security Information and Event Management*) infrastructure to ensure the accuracy of anomalous data correlations on a large scale and in real time. All state-owned banks are targeted to have installed a fully integrated SIEM system before the end of 2026. SIEM implementation is an important component in automatic detection and *predictive risk dashboard* creation (Suvorova, 2023). With the strengthening on these two sides—human resources and technology—institutions are expected to be ready to carry out the next phase that focuses on collaboration and interoperability between institutions.

Year 2027

Entering 2027, the national strategy is directed at strengthening the collaborative ecosystem, especially in terms of threat information exchange or *threat intelligence sharing*. State-owned banks and regulators are required to develop information sharing platforms that are active and run in real-time, including attack metadata, *adversary tactics*, and compromise indicators (IOCs). According to CONCORDIA (2021), the effectiveness of the response to nationwide attacks is highly dependent on the ability to integrate and exchange technical information between agencies instantly.

In addition, cross-sector coordination protocols have also begun to be formally regulated between state-owned banks, BSSN, and OJK. This protocol includes an escalation mechanism, distribution of incident response tasks, and emergency communication procedures during *a cyber crisis*. This year's success indicators are marked by the implementation of joint simulations twice a year, involving all key

stakeholders of the national financial sector. This step strengthens cross-institutional preparedness and accelerates response time to potential systemic attacks.

Year 2028

In 2028, the focus of the strategy shifts to cyber *resilience testing* through simulated national-scale scenarios. The trial in the form of *a red team exercise* was conducted to assess the actual response of institutions to attacks based on *Ransomware-as-a-Service* (RaaS) scenarios. The purpose of this simulation is to test the effectiveness of defense systems, internal and external coordination capabilities, and evaluate readiness against automated latent threats (Zhou, Lin, & Patel, 2023).

The assessment based on the cyber resilience index is used as the main metric, with a target index value of at least 80 percent for the SOE sector. The evaluation of the simulation results is used as the basis for adjusting security procedures and policy recommendations in dealing with the development of attacker tactics. This year is an important milestone in the transition from a reactive approach to a scenario-based proactive approach, with measurable and documented *preparedness strategy-based* planning (Saritas, 2016).

Year 2029

The final year of this roadmap, 2029, is focused on the process of evaluation and full integration into national cybersecurity strategic policies. An evaluation was carried out on all achievements, obstacles, and dynamics of the implementation of the roadmap since 2025. Furthermore, this roadmap was aligned and integrated into the framework of the National Cybersecurity Strategy (Linkov & Kott, 2019). The integrated documents are targeted to become official government documents that underlie long-term steps in the country's financial sector.

In addition to macro evaluation, this year was also marked by the preparation of a contingency plan based on a national AI scenario. This plan includes *a zero-day response* protocol, system recovery (*cyber recovery*), and the establishment of an AI threat response coordination center. The implementation of *the zero-response protocol* is a key indicator of success, marking Indonesia's full readiness to respond to the escalation of AI-based ransomware threats with a holistic and sustainable national strategy (National Institute of Standards and Technology, 2024).

CONCLUSION

AI-enhanced ransomware has emerged as a major strategic threat to Indonesia’s state-owned banking sector, with evolving variants like *LockBit*, *Ryuk*, and *Blocker* bypassing traditional defenses through adaptive, automated attacks. The financial sector remains highly vulnerable, as evidenced by over 102,000 *LockBit* attacks in 2024, including incidents paralyzing Bank Syariah Indonesia and Bank Rakyat Indonesia, exposing weaknesses in incident response, human resources, and real-time threat

detection. Despite existing regulations like *POJK No. 11/2022*, gaps persist in addressing AI-driven threats and fostering inter-institutional threat intelligence sharing.

Attack patterns peak during fiscal year-end, with November–December 2024 seeing 160 million cyber anomalies, linked to increased digital transactions and holiday-period vulnerabilities. Key drivers include AI automation, fragmented regulations, and the rise of *Ransomware-as-a-Service* (RaaS), enabling even non-technical attackers. Currently, state banks are in a high-risk, low-readiness quadrant, necessitating a five-year roadmap (2025–2029) to shift toward proactive resilience. This includes adopting *ISO/IEC 27035*, establishing *CSIRT*, enhancing *SOC* and threat intelligence, conducting national audits, and harmonizing crisis response systems. A *foresight*-based approach is critical to transitioning from reactive to proactive cybersecurity, ensuring fiscal stability and public trust amid escalating AI-powered threats.

REFERENCES

Adnyana, I. M., & Ajeng Gemellia, A. D. (2021). Analisis kinerja aparatur sipil negara di Badan Siber dan Sandi Negara tahun 2019. *Populis: Jurnal Sosial Dan Humaniora, 6*(2). https://doi.org/10.47313/pjsh.v6i2.1387

Badan Siber dan Sandi Negara. (2022). *Lanskap keamanan siber Indonesia 2022*. Badan Siber Dan Sandi Negara.

Badan Siber Dan Sandi Negara. (2023). BSSN ungkap lanskap keamanan siber Indonesia tahun 2022 untuk literasi budaya keamanan siber. *BSSN (Badan Siber Dan Sandi Negara)*.

BSSN. (2022). *Lanskap keamanan siber Indonesia 2022*. Badan Siber Dan Sandi Negara.

BSSN. (2023). *Annual report Badan Siber dan Sandi Negara tahun 2022*. Badan Siber Dan Sandi Negara, Februari.

Chakravarti, A. (2023). LockBit ransomware hits Bank Syariah Indonesia: Timeline and impact. *CyberAsia Journal, 6*(2), 64–78.

CONCORDIA. (2021). Assessing cyber risks and threat intelligence for the finance sector. https://www.concordia-h2020.eu/

Crisanto, J. C., Prenio, J., & Restoy, F. (2023). The evolving role of cyber resilience in financial regulation. *BIS Papers No. 128*. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap128.htm

CrowdStrike. (2025). AI-powered cyber threats: 2025 global report. Retrieved from https://www.crowdstrike.com

CrowdStrike. (2025). Most common AI-powered cyberattacks. https://www.crowdstrike.com

Hariyadi, D., & Nastiti, F. E. (2021). Analisis keamanan sistem informasi menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi Dan Informatika), 5*(1). https://doi.org/10.31603/komtika.v5i1.5134

Haryanto, A., & Sutra, S. M. (2023). Upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017-2020. *Global Political Studies Journal, 7*(1). https://doi.org/10.34010/gpsjournal.v7i1.8141

Kumar, V., & Upadhyay, N. (2023). The economics of ransomware-as-a-service: A study of the dark web ecosystem. *Computers & Security, 125*, 102975. https://doi.org/10.1016/j.cose.2023.102975

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi implementasi kebijakan pembentukan tim tanggap insiden siber pada sektor pemerintah. *Matra Pembaruan, 6*(1). https://doi.org/10.21787/mp.6.1.2022.1-14

Prunckun, H. (2010). *Handbook of scientific methods of inquiry for intelligence analysis*. Scarecrow Press.

Saritas, O. (2016). Systemic foresight methodology. In R. Popper (Ed.), *Mapping the future of foresight studies* (pp. 31–63). Springer. https://doi.org/10.1007/978-3-319-31549-2_2

Simorangkir, S., Purba, D., & Hartati, N. (2025). Evaluation of the cyber resilience of the Indonesian banking sector: Analysis of trends and implications. *National Journal of Information Security, 4*(1), 51–70.

Suvorova, S. (2023). ENISA threat landscape 2023: Top cyber threats and trends. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Sutra, S., & Haryanto, A. (2023). Upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017-2020. *Global Political Studies Journal, 7*(1).

Zhou, Y., Lin, H., & Patel, R. (2023). Reinforcement learning in ransomware propagation and avoidance. *IEEE Transactions on Information Forensics and Security, 18*, 245–259. https://doi.org/10.1109/TIFS.2023.3244567