

Kadin's Industry Report and Strategic Guide: **Cybersecurity for a Sustainable and Resilient Digital Indonesia**

by Kadin Kominfo

Table of Contents

| | | |
|------------------|--|----|
| | Disclaimer | 6 |
| | Foreword | 8 |
| | Executive Summary | 12 |
| Chapter 1 | Introduction | 13 |
| 1.1 | Background and Importance of Cybersecurity | 14 |
| 1.2 | Kadin's Cybersecurity Industry White Paper and Implementation Roadmap Strategic Objectives | 14 |
| Chapter 2 | Current Cybersecurity Landscape | 16 |
| 2.1 | Global and National Cybersecurity Environment | 17 |
| 2.2 | Sector-Specific Landscape | 20 |
| 2.3 | Cost of Cybercrime in Indonesia | 25 |
| Chapter 3 | Strategic Pillars for Cybersecurity | 26 |
| 3.1 | Pillar 1: Cyber Resilience in Critical Infrastructure | 27 |
| 3.2 | Pillar 2: Enhancing Cybersecurity Governance and Regulations | 28 |
| 3.3 | Pillar 3: Developing Cybersecurity Talent and Awareness | 28 |
| 3.4 | Pillar 4: Public-Private Partnerships | 29 |
| 3.5 | Pillar 5: Aligning Indonesia with Standardized Cybersecurity Methodologies and Standard | 29 |
| 3.6 | Pillar 6: Strengthening Local Players in Indonesia Cybersecurity Industry Growth s | 29 |
| Chapter 4 | Sector-Specific Cybersecurity Insights | 30 |
| 4.1 | Asset Mapping and Attack Surface Management | 31 |
| 4.2 | Sector-Specific Cybersecurity Analysis | 34 |
| 4.3 | Recommendations Based on Sectoral Assessments | 45 |



Table of Contents

| | | |
|------------------|--|----|
| Chapter 5 | Regulatory and Governance Framework | 47 |
| 5.1 | Overview of Indonesia's Current Cybersecurity Regulations | 48 |
| 5.2 | Proposed Regulatory Enhancements | 52 |
| 5.3 | Enhance The Governance Model and Institutional Roles | 56 |
| Chapter 6 | Public-Private Partnerships & Industry Collaboration | 67 |
| 6.1 | Developing a National Public-Private Partnership Program | 68 |
| 6.2 | Developing a Real-Time Threat Intelligence Sharing Platform | 69 |
| 6.3 | Establish a Cyber Incident Review Board or Similar Forum | 70 |
| 6.4 | Strengthening International Collaboration in Cybersecurity | 70 |
| Chapter 7 | Cybersecurity Education and Talent Development | 72 |
| 7.1 | Current Challenges in Cybersecurity Talent and Awareness | 73 |
| 7.2 | Designating a Lead Agency for Cyber Education and Awareness | 74 |
| 7.3 | Comprehensive Cyber Security Employee Training | 75 |
| 7.4 | Growing Cybersecurity Talent in Indonesia | 76 |
| 7.5 | Career Path and Occupation Mapping for Cybersecurity Talents | 78 |
| 7.6 | Certification Programs and Standards | 78 |
| 7.7 | Case Studies: Industry Support for Cybersecurity Education | 81 |
| Chapter 8 | Cybersecurity Methodologies and Risk Management Frameworks | 83 |
| 8.1 | Adopting a Standardized Cybersecurity Methodology | 84 |
| 8.2 | Security Controls Based on NIST Cybersecurity Framework | 84 |
| 8.3 | Tailoring Cybersecurity Methodologies to Organizational Categories | 86 |
| 8.4 | Advanced Cybersecurity Enhancement Recommendations | 90 |
| 8.5 | Enhancing Critical Infrastructure Protection | 91 |

Table of Contents

| | | |
|-------------------|---|-----|
| Chapter 9 | Strengthening Local Players in Cybersecurity Industry Growth | 92 |
| 9.1 | Strengthening Policy and Regulatory Support for Local Industry | 94 |
| 9.2 | National Cybersecurity Industry Roadmap Strategic Objectives | 95 |
| 9.3 | Supporting Local Firms' Participation in Government Projects | 96 |
| 9.4 | Encouraging Technology Transfer and Fair Competition | 97 |
| Chapter 10 | Implementation Roadmap | 98 |
| 10.1 | Periodical Target | 99 |
| 10.2 | Measuring Success | 105 |
| | Work Cited | 110 |
| | Appendices | 115 |



Kadin's Industry Report and Strategic Guide: Cybersecurity for a Sustainable and Resilient Digital Indonesia

Kadin INDONESIA
Indonesian Chamber of Commerce and Industry

Jl. H. R. Rasuna Said Blok X-5 No.Kav. 2-3,
Kuningan, Jakarta 12950
www.kadin.id

Disclaimer

Kadin's Industry Report and Strategic Guide: Cybersecurity for a Sustainable and Resilient Digital Indonesia is an initiative owned and led by Kadin Indonesia (the Indonesian Chamber of Commerce and Industry), with support from the US-ASEAN Business Council where they serve as the knowledge partner, providing expertise, and guidance throughout the project.

This Report aims to provide a comprehensive framework and actionable recommendations to enhance cybersecurity across Indonesia's public and private sectors. The objective is to strengthen national cyber resilience, foster a secure digital economy, and protect critical infrastructure from evolving cyber threats. The ultimate goal is to contribute to a safer and more prosperous digital future for Indonesia.

Editorial Team



**Firlie
Ganinduto**

Lead Editorial and Project Kadin
Indonesia Cybersecurity Report
and Strategic Guide



**Rorian
Pratyaksa**

Deputy Lead Editorial and Project
Kadin Indonesia Cybersecurity
Report and Strategic Guide



**Mercy
Simorangkir**

Deputy Lead Editorial and Project
Kadin Indonesia Cybersecurity
Report and Strategic Guide



**Mochamad
Andriansyah**

Project Management Officer Kadin
Indonesia Cybersecurity Report
and Strategic Guide



**Raihan
Zairah**

Project and Research Analyst
Kadin Indonesia Cybersecurity
Report and Strategic Guide



**Nizam
Syafik**

Project and Research Analyst
Kadin Indonesia Cybersecurity
Report and Strategic Guide



M. Arsjad Rasjid P.M.

Indonesian Chamber of Commerce and Industry
(Kadin Indonesia)



Foreword

Dear **Industry Leaders, Information Security, and Cyber-Security Specialists,**

In our increasingly connected world, cybersecurity has become one of the most critical challenges we face. While technological advancements have brought great opportunities, they also expose us to new vulnerabilities. Protecting vital infrastructure, ensuring business continuity, and safeguarding sensitive information are now essential for the stability of our economy and society.

Thus, this document is not just a set of guidelines; it reflects a broader understanding of the unique challenges and opportunities across various industries in Indonesia. It also serves as important inputs to the whitepaper “Project Usulan Strategi/Arah Pembangunan Bidang Ekonomi Tahun 2025-2029” by Kadin Indonesia. By recognizing the specific risks faced by different sectors, we aim to provide a framework that helps organizations prepare for and respond to cyber threats effectively.

Not solely focusing on regulations, this document also explores the broader industry landscape. It highlights key areas where improvements can be made to strengthen our collective resilience. Whether in finance, energy, or healthcare, each sector has its own unique challenges, and it's crucial that our cybersecurity approach is flexible and adaptable to these diverse needs. What's clear is that cybersecurity is no longer just an IT issue, it is a business and national priority.

By working together, sharing knowledge, and applying best practices, we can ensure that Indonesian organizations are not only prepared to defend against cyber threats but also well-positioned to thrive in the digital age. This approach will help protect our infrastructure and strengthen the foundations of our economy. The insights in this document provide practical steps that every organization, regardless of size, can take to bolster their defenses and secure their future.

I encourage all stakeholders both public and private to work collaboratively. Cybersecurity is a shared responsibility, and by addressing it together, we can build a safer and more prosperous future for Indonesia.

Sincerely,

M. Arsjad Rasjid P.M.

Chairman of Indonesian Chamber of Commerce and Industry (Kadin Indonesia)



Firlie Hanggodo Ganinduto

Indonesian Chamber of Commerce and Industry -
Communications and Informatics (Kadin Kominfo)



Foreword

Dear **Industry Leaders, Information Security, and Cyber-Security Specialists,**

As we embrace a digital revolution that reshapes our society and economy, Indonesia encounters unique cybersecurity challenges and opportunities. This “Kadin’s Industry Report and Strategic Guide: Cybersecurity for a Sustainable and Resilient Digital Indonesia”, in partnership with the US-ASEAN Business Council (US-ABC), evaluates our cybersecurity state and proposes a comprehensive strategy to bolster our defenses.

The digital transformation has unlocked potential for innovation but has also introduced significant risks. Sectors like financial services, healthcare, and manufacturing increasingly depend on digital systems, exposing them to cyber threats. The data shows a disturbing increase in cyberattacks’ frequency and sophistication, threatening our national security and economic stability.

This report, born from thorough analysis and collaboration, examines our industry landscape to pinpoint vulnerabilities and opportunities for proactive cybersecurity measures. It details sector-specific challenges and suggests tailored defense strategies for effectiveness and resilience.

It stresses the importance of updating regulatory frameworks to match technological and threat landscape advancements. Tightening global compliance necessitates progressive policies to protect our citizens and stakeholders.

At the heart of our strategy is education and training. By enhancing cyber education, we aim to cultivate a knowledgeable workforce adept at defending against cyber threats. Public-private partnerships will also play a vital role, allowing for shared threat intelligence and best practices with industry leaders and international partners, enhancing our response capabilities.

The recommendations advocate a layered defense strategy, including stringent technical standards and regular system updates to reduce risks. Our goal is to establish a cybersecurity posture that is reactive, predictive, and proactive, capable of countering current and future threats.

In conclusion, the “Kadin’s Industry Report and Strategic Guide: Cybersecurity for a Sustainable and Resilient Digital Indonesia” serves as a roadmap and a call to action, urging stakeholders—government, industry leaders, and citizens—to strengthen our cyber defenses. Together, we can secure Indonesia’s digital future and ensure our nation thrives amidst the cyber challenges ahead.

Let’s commit to this crucial endeavor, as the security and prosperity of our digital tomorrow depend on our actions today.

Sincerely,

Firli Hanggodo Ganinduto

Vice Chairman of Communication and Informatics
Indonesian Chamber of Commerce and Industry
(Kadin Indonesia)

Executive Summary

To support the existing Indonesia government initiatives in building a secure and resilient national cybersecurity. Kadin's Industry Report and Strategic Guide: Cybersecurity for a Sustainable and Resilient Digital Indonesia emphasizes the urgent need for a robust and adaptive cybersecurity framework to support the nation's rapidly growing digital economy. As Indonesia expands its online services, protecting national critical infrastructure—such as energy, telecommunications, and healthcare—has become essential to ensure service continuity and mitigate the impact of cyber incidents. The report outlines strategic pillars, including enhancing cybersecurity governance through improved regulatory frameworks aligned with international standards, and fostering public-private partnerships to strengthen threat detection, response, and mitigation.

This report also introduces six main strategic pillars of cybersecurity for Indonesia inter alia 1) cyber resilience in critical infrastructure, 2) enhancing cybersecurity governance and regulations, 3) developing cybersecurity talent and awareness, 4) public-private partnerships, 5) aligning Indonesia with standardized cybersecurity methodologies and standards, and 6) building a competitive and resilient local cybersecurity industry. Additionally, the Report stresses the importance of

developing a skilled workforce by investing in cybersecurity education, training, and public awareness. It advocates for adopting standardized cybersecurity methodologies to ensure Indonesia's practices are competitive globally. Although Indonesia has made strides in addressing cyber threats, challenges remain, particularly in the form of sophisticated attacks like ransomware, data breaches, and cyber espionage. The government, through its cybersecurity agency, is working to improve national resilience, but further efforts are needed to enhance collaboration and talent development. Furthermore, this white paper also explores the role of Kadin Indonesia in accelerating the implementation of proposed cybersecurity pillars. Overall, the white paper provides a strategic roadmap for securing Indonesia's digital future, ensuring it remains resilient in the face of growing cyber risks.



Chapter

01

Introduction

1.1 Background and Importance of Cybersecurity

Cybersecurity has become a critical element for nations, businesses, and individuals in an increasingly digital world. As one of Southeast Asia's fastest-growing digital economies, Indonesia stands at a pivotal point where immense opportunities are decorated with significant risks.

With over 270 million people, Indonesia's online services are growing rapidly, from e-commerce to financial services and online healthcare to Government platforms. This spread of digital has disrupted every aspect of industries. However, all these developments come with increased vulnerabilities, and failure to address them can put the entire digital ecosystem at risk of instability and compromise.

These cyberattacks have graduated from ransomware attacks on critical infrastructures to highly sophisticated phishing schemes against citizens and businesses. Critical infrastructure sectors in Indonesia, including energy, telecommunications, health care, and financial services, are pretty vulnerable to such emerging threats, which could bring immense financial losses, disruptions in operations, and even threats to national security.

With cyber incidents increasing in frequency and severity, cybersecurity can no longer remain an IT issue; it is a priority concerning national security. As Indonesia continues to expand its digital economy, the need for a robust, adaptive, and comprehensive cybersecurity framework becomes more urgent.

Why Cybersecurity is Critical for Indonesia:

1. Safeguarding National Critical Infrastructure

Critical infrastructure, such as energy grids, health-care services, financial systems and telecommunications networks are the foundation of the Indonesian economy. A ransomware attack that disrupted any of these sectors would cause widespread damage to critical services, disrupt daily activities and endanger lives.

2. Protecting Citizens and Businesses

As more Indonesian citizens and businesses engage with cyberspace, they are exposing themselves to potential cybersecurity threats. Millions of Indonesians have already been affected by personal data breaches, financial fraud and identity theft. They need an effective cybersecurity framework to protect them.

3. Fostering Trust in Digital Systems

Indonesia's digital economy can only develop with public confidence in the security of its online activities, data, and transactions. Breaches and cyberattacks further break that trust, and in this aspect, cybersecurity is an enabler that aids a nation in balancing its move towards the digital age.

1.2 Kadin's Cybersecurity Industry White Paper and Implementation Roadmap Strategic Objectives

The cybersecurity challenges in Indonesia can only be resolved through the implementation of unified and coordinated solutions. This report acts as a foundational guideline for addressing existing vulnerabilities while building long-term resilience in the Indonesian Cybersecurity Industry, combining public and private sector best efforts to build a strong and resilient cybersecurity ecosystem.

The report is designed to realize the following important objectives:

1. Enhancing the Resilience of National Critical Infrastructure

Protecting key assets in critical sectors (finance, healthcare, manufacturing, energy) is vital for Indonesia. A secure and resilient infrastructure is the basis of assuring an uninterrupted supply of goods and services and the minimal economic impact of cyber incidents

2. Enhancing Cybersecurity Governance and Regulatory Frameworks

A strong regulatory framework is essential for governing cybersecurity practices in Indonesia's several different sectors – which can only be achieved by implementing and enforcing modernized cybersecurity law and synchronizing Indonesian national law with international standards. A robust legal framework ensures that Indonesia's cybersecurity practices are standardized, enforceable, and adaptable to new threats.

3. Fostering Public-Private Partnerships and Collaboration

To achieve a secure and resilient digital nation in 2045, strong collaboration between the government, private sector, academic sector and any international partners is essential. Developing public-private partnerships where resources and knowledge are combined can be an effective approach to creating a secure and resilient digital nation in 2045. The partnerships ensure that every stakeholder plays a role in securing the cyber landscape in Indonesia.

4. Growing Cybersecurity Talent and Awareness

Growing a pool of highly qualified cybersecurity talent is one of the key foundations in an attempt to address the shortage of cybersecurity profes-

sionals in the workforce. Through targeted actions at all levels of the education system, training, and upskilling initiatives, Indonesia can address this challenge. In addition, awareness of cybersecurity issues should be elevated in every layer of Indonesia's local society, covering ordinary citizens to the large corporations, as this is essential for building a culture of security awareness in Indonesia.

5. Aligning Indonesia with Standardized Cybersecurity Methodologies and Standards

In an attempt to effectively handle cyber incidents, we should encourage the establishment of standardized cybersecurity methodologies and risk frameworks that align with existing best global frameworks. The harmonization of Indonesia's cybersecurity standards ensures consistency and continuity in cybersecurity practices across industries. Moreover, with this alignment, Indonesia will become the regional leader in cybersecurity and, most importantly, ensure the nation's security frameworks remain globally competitive.

6. Strengthening Local Players in Indonesia Cybersecurity Industry Growth

Competitive and resilient local cybersecurity industry is crucial to reducing dependence on foreign enterprises and ensuring national digital sovereignty. Key to this will be creating favorable regulations, offering financial incentives for local R&D, establishing a certification framework for local companies, and encouraging public-private partnerships to eventually support the growth of Indonesian cybersecurity companies, creating a more sustainable ecosystem for fulfilling the needs of both domestic and global markets. A reinforcement of the local capacity bolstered Indonesia's national security and promoted economic prosperity and technological leadership within the region.



Chapter

02

Current Cybersecurity Landscape

2.1 Global and National Cybersecurity Environment

The threat landscape of global cybercrime continues to evolve. Attacks on both public and private sectors are becoming increasingly sophisticated. These are increasingly dependent on new attack vectors empowered by AI and ML, while ransomware-as-a-service attacks boast very focused and destructive breaches. Then, there is cyber espionage and cyber war carried out by nation-state actors, further complicating this threat environment. Indeed, against a background of increasing incidence and intensity of data breaches, ransomware incidents, and supply chain compromises, robust cybersecurity is an issue that takes on an international dimension of imperatives.

Global Cybersecurity Threats

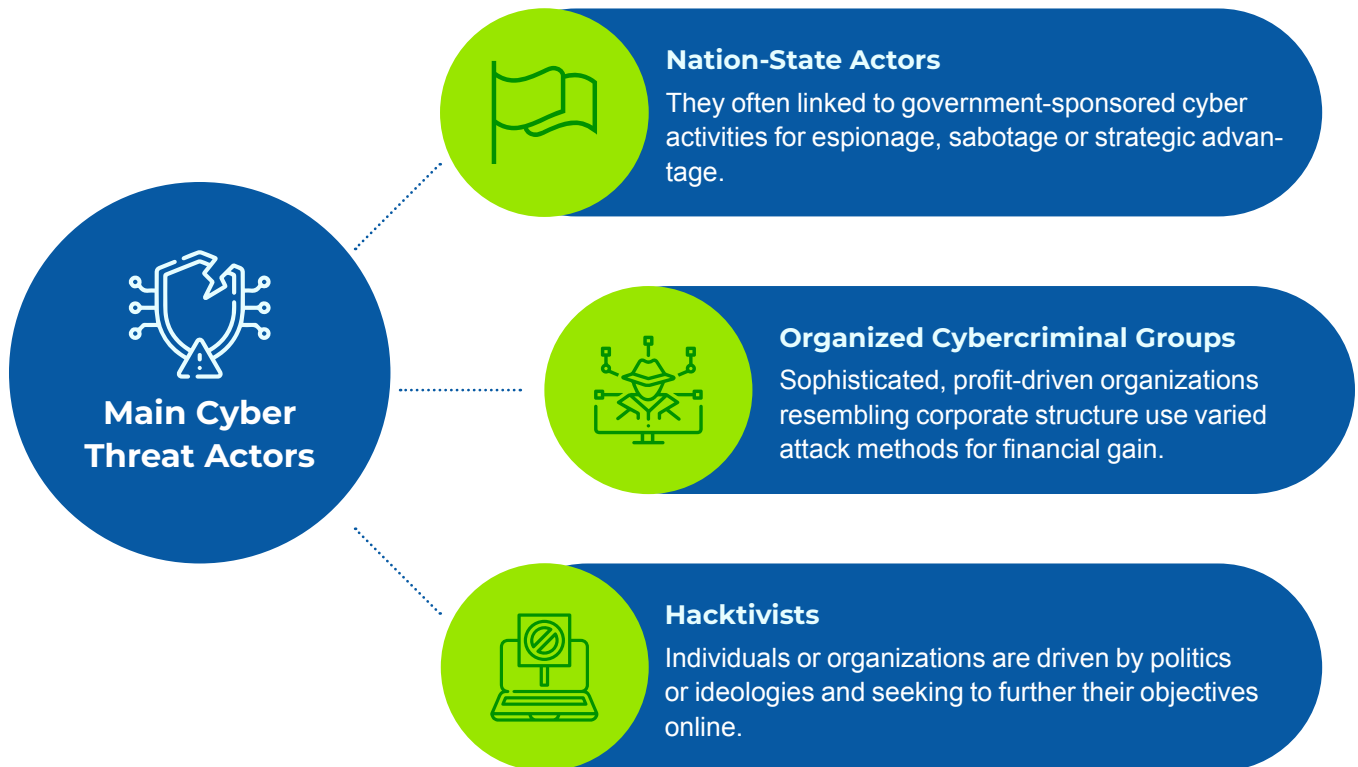


Exhibit 2.1 The Main Threat Actor Categories

More specifically, nation-state actors, organized cybercriminal groups, and hacktivists are continuously evolving new attack methods at the global level. With AI and ML in cyberattacks, attackers can automate large-scale campaigns and amplify their reach and impact. Moreover, with ransomware-as-a-service platforms, the barriers to entry have been lower for less-skilled attackers; thus, the scale of ransomware attacks globally has increased. Taken in concert with the sustained cyber espionage from nation-states, this set of trends creates a complex, rapidly changing threat environment that is difficult for governments and businesses.

National Cybersecurity Landscape in Indonesia

Indonesia faces unique cybersecurity challenges as adversaries operate at speed, scale, and sophistication. Indonesia, the largest economy in the region with its fast digital growth, has emerged as the prime target for cyberattacks in Southeast Asia. With the growing dependency on digital infrastructure among its people, its rapid gains in Internet and mobile usage are widening the attack surface area of the country substantially.

A rapid surge of ransomware attacks, data breaches, and online fraud against businesses and state entities has marked the Indonesian cybersecurity landscape. During the past year, ransomware attacks have targeted

the financial service sector more than any other industry, proving it to be vulnerable to cyber threats. This includes the ransomware attack against the country's national data center, which brought down several public services; the leakage of the Indonesia Automatic Fingerprint Identification System (INAFIS); and the National Armed Forces Strategic Intelligence Agency. Data shared by Palo Alto Networks Unit 42 shows the following industries were most affected in Indonesia because of ransomware activities during the last year:

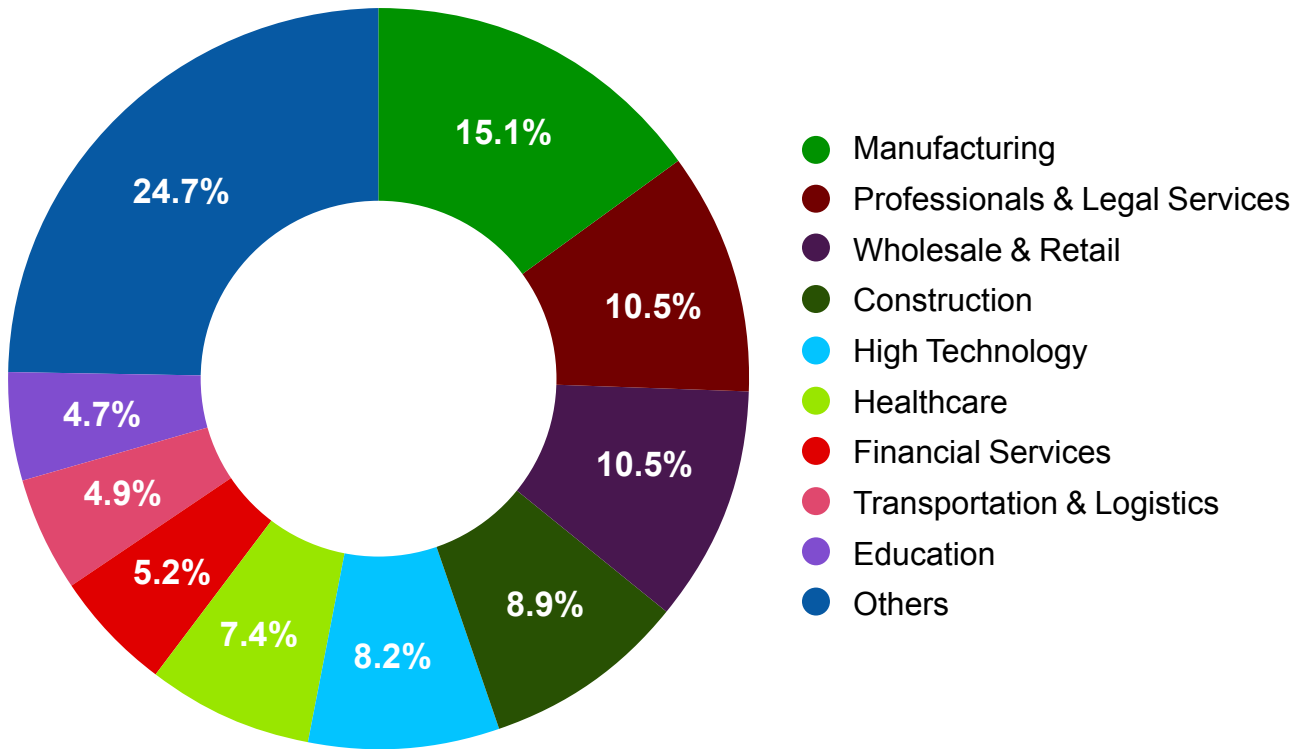


Exhibit 2.2 Indonesia's Most Impacted Industries by Ransomware Attacks in 2023
Source: Palo Alto Unit 42 Threat Intelligence Team

Key Cyber Threat Actors

Data provided by Palo Alto Networks Unit 42 shows that different ransomware activities have caused damage to several industries in Indonesia this year. Indonesia also remains one of the favorite targets of cyber adversaries driven by state-based teams. Some of the recent reported cases include:

- AlloyTaurus (aka GALLIUM, Softcell):**
 This Chinese advanced persistent threat group customarily runs cyber espionage campaigns targeting telecommunications, financial institutions, and Government entities across Asia, Europe, and Africa, including Indonesia.¹
- March 2024 Incident:**
 This report points out two Chinese APT groups involved in cyber espionage activities across ASEAN-affiliated entities and member countries.
- February 2024 Data Leak:**
 I-Soon, a Chinese enabler, was involved in a data breach that revealed access to critical information from Indonesia's Department of Commerce.³

The activities coincide with the ASEAN-Australia Special Summit on March 4-6, 2024. ASEAN entities are natural targets for espionage operations because they contain sensitive diplomatic and economic information.²



Ongoing Government Efforts

The Indonesian Government is already taking steps to develop its cyber capacities, the most prominent of which is the creation of the National Cyber and Crypto Agency. However, there are few challenges that still need to be addressed, including a deficiency of skilled cybersecurity talent and a general absence of the in-depth coordination of public-private collaboration necessary for strengthening cyber defenses.

Overcoming these challenges will require comprehensive action that improves cyber risk management practices across Indonesian sectors, harmonizes the regulatory framework towards International cybersecurity standards-compliant maturity level, invests in capacity-building by establishing a more sustainable model of over-arching education & awareness campaign as well as skill creation mechanism thereby shaping behavioral changes and increasing the future talent pool, and strengthening technical capacities for effective response against attacks on CIIs.

By prioritizing these cybersecurity issues, Indonesia can secure its digital future, increase resilience across critical sectors, and contribute to regional and global cybersecurity efforts.

¹ Unit 42, "GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool." Unit 42, June 13, 2022. <https://unit42.paloaltonetworks.com/pingpull-gallium/>

² Unit 42, "ASEAN Entities in the Spotlight: Chinese APT Group Targeting." Unit 42 (blog), March 26, 2024. <https://unit42.paloaltonetworks.com/chinese-apt-target-asean-entities/>

³ Christian Shepherd et al., "China's Hacking Operations Exposed by Document Leak." *The Washington Post*, February 21, 2024. <https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoan/>

2.2 Sector-Specific Landscape





| Sector | Main Threats | Specific Vulnerabilities | Impact Level |
|---|--|---|---|
|  Financial Services | <ul style="list-style-type: none"> • Ransomware • Spear Phishing • Banking Trojans • Rapid Vulnerability Exploitation | <ul style="list-style-type: none"> • Large customer data troves • Legacy systems in banks • Growing use of cryptocurrency Exchanges | High (Disruption of financial systems, data theft, fraud) |
|  Healthcare | <ul style="list-style-type: none"> • Ransomware • DDoS Attacks • Data Breaches • Insider Threats | <ul style="list-style-type: none"> • Critical reliance on digital records • Large volumes of sensitive personal data • Expanding IoT devices in healthcare | High (Patient safety risks, life-threatening disruptions) |
|  Manufacturing | <ul style="list-style-type: none"> • Ransomware • Nation-State Attacks • Software Supply Chain Compromises • Cyber Espionage | <ul style="list-style-type: none"> • Use of outdated legacy systems • Highly interconnected supply chains • OT (Operational Technology) vulnerabilities | High (Disruption of production lines, IP theft, supply chain risks) |
|  Critical Infrastructure | <ul style="list-style-type: none"> • Ransomware • BEC (Business Email Compromise) • State-Sponsored Cyber Espionage • Supply Chain Vulnerabilities | <ul style="list-style-type: none"> • Complex, interconnected OT and IT systems • Limited downtime tolerance • Geopolitical sensitives and strategic assets | Very High (National security risks, large-scale service disruption) |

Exhibit 2.3 Sector-Specific Threat Matrix

2.2.1 Financial Services Sector

The global financial services sector continues to be threatened by an ever-evolving cyber threat landscape. Threat actors continue evolving tactics to exploit vulnerabilities within this critical industry. This sector includes various organizations, from credit unions and small insurance companies to large cryptocurrency exchanges and stock exchanges. Each industry subgroup has threats specific to its unique characteristics; however, opportunistic and financially motivated cybercriminals, especially ransomware groups and IABs, are the most significant adversaries.

According to intelligence by Palo Alto Networks, a variety of critical threats have emerged as being of particular significance both globally and within Indonesia:

- Spear Phishing and Unpatched Vulnerabilities:**
 Spear phishing emails and unpatched vulnerabilities remain essential methods of initial access for threat actors. These phishing attacks are usually made to revolve around current events or business activities and are very effective. The attackers often use the “spray-and-pray” method, exploiting publicly known vulnerabilities and exposing internet-facing assets to breach financial institutions.
- Rapid Weaponization of Vulnerabilities:**
 The fast exploitation of zero-day and one-day vulnerabilities is one of the critical risks to the financial services sector. Cybercriminals take little time to exploit these weaknesses, sometimes even when patches are available or applied. In this, an underground market exists for ready-to-use tools, thus setting the enabling actors of all skill levels with an acquisition tool, source code, and other resources that increase the frequency and impact of cybercriminal activity.
- Malvertising and SEO Poisoning:**
 Another significant threat is Malware and SEO poisoning. These tactics redirect users to malicious websites with the aim of downloading romanized versions of popular software. These actions compromise security among both users and insti-

tutions, and threat actors find them increasingly attractive.

- Ransomware:**
 Ransomware remains one of the most prevalent threats to the financial services sector. In Indonesia, this vulnerability is particularly acute. Over the past year, Palo Alto Networks Unit 42 has observed 271 ransomware attacks targeting the financial sector, originating from 44 distinct ransomware groups. These groups exhibited opportunistic behavior, targeting the sector without displaying significant preference toward specific sub-industries. The following chart shows the top ransomware operators impacting the financial sector in Indonesia. Sub-industries such as financial and investment consulting, banking and securities, and investment management were affected.
- Banking Trojans:**
 Banking trojans have become one of the growing threats as attackers expand their target base to embrace a wider selection of financial institutions and a variety of data types. While banking trojan malware has become increasingly sophisticated, stealing highly sensitive information across multiple financial services and amplifying the potential impact of these attacks continues unabated.

In Indonesia, these global threats are even more pronounced because of the rapid digital transformation of the sector. The attack surface keeps growing as financial services are delivered utilizing digital infrastructure. This will call for the financial services industry to invest more in continuous monitoring, rapid patching of vulnerabilities, and proactive sharing of threat intelligence across the sector. In Indonesia, the inability of financial institutions to safeguard against the ever-changing cyber world calls for concerted efforts from both the public and private sectors.

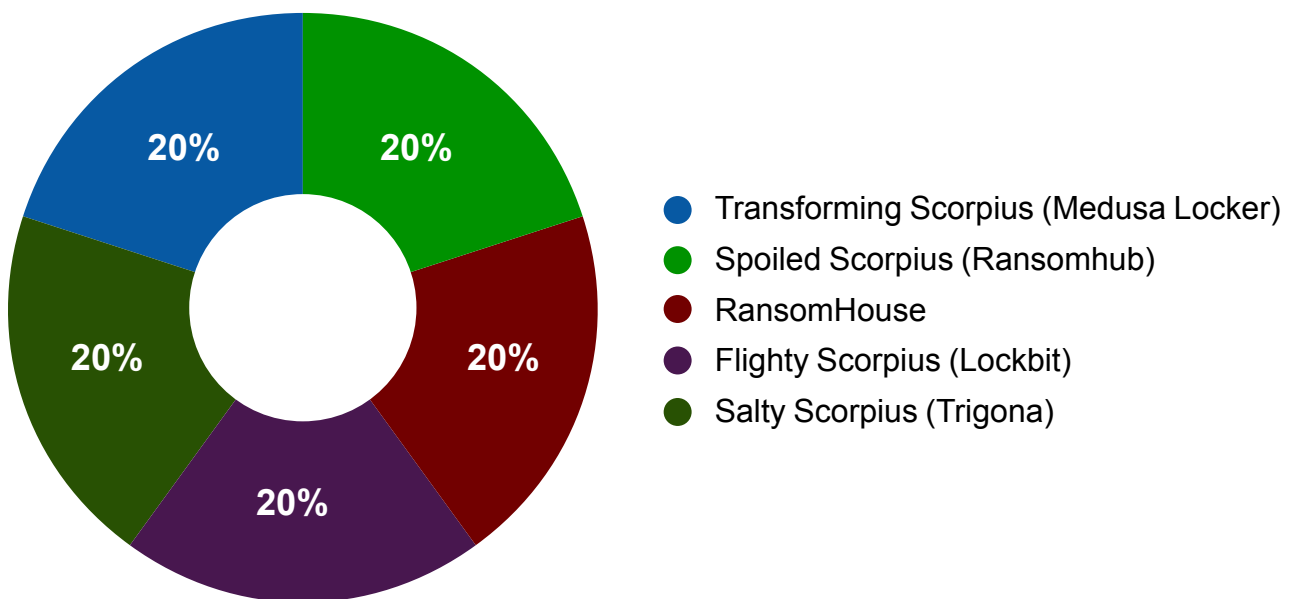


Exhibit 2.4 Top Ransomware Operators Impacting the Financial Sector in Indonesia, **Source:** Palo Alto Networks Unit 42

2.2.2 Healthcare Sector

Numerous cybersecurity risks that could have severe consequences in Indonesia as well as globally confront the healthcare sector. Due to the industry's dependence on digital infrastructure and sensitive personal data, it is a popular target for many types of cyberattacks.

Palo Alto Networks has noted the following actions that have an effect on the healthcare industry:

- **DDoS attacks (Distributed Denial of Service):**
In order to access patient records, telemedicine, and vital internal communications, network connectivity is essential for the companies in the healthcare sector. These Distributed Denial of Service (DDoS) assaults may cause system traffic to overload, interfering with emergency services and potentially postponing patient care or even worse, posing a threat to human life if left unchecked. The repercussions of such attacks could be gravely severe, as our networks are crucial for coordinating lifesaving treatment and maintaining access to timely medical help.
- **Supply Chain Attacks:**
For solutions ranging from medical supplies to IT infrastructure, many healthcare facilities rely on a network of outside vendors. Every link in this supply chain could have a security breach that affects the entire network, resulting in compromised medical devices, data leaks, and disruptions to operations. The risk associated with supply chain security is increased in Indonesia due to the interdependence of suppliers and healthcare providers.
- **Web Application Attacks:**
In healthcare portals, interfaces for provider communication and patient data access are commonplace. Online application hacks like cross-site scripting (XSS) and SQL injection can take advantage of vulnerabilities in online applications to alter patient data, steal private information, or gain unauthorized access to healthcare systems. These attacks might have a major effect on patient data security and integrity.
- **Ransomware:**
This form of virus encrypts important data and locks down computers until a ransom is paid. This may result in hospital operations being disturbed, patient care being stopped, and closed access to patient records for healthcare facilities, which might cause serious delays in life-saving treatments. Recent assaults in Indonesia demonstrate the rising threat posed by ransomware as a result of the country's fast digital transition in the healthcare sector.
- **Data Breach:**
There may be dangerous repercussions if personal health information is stolen or viewed without authorization. Data breaches can be exploited for fraud, identity theft, or the black market. For patients, this means a breach of privacy and even financial loss; for institutions, it means legal trouble and a decline in confidence. Like their international counterparts, Indonesian healthcare institutions manage substantial volumes of personal data, which makes them desirable targets for hackers.
- **Insider Threats:**
Negligence or malicious intent may turn workers or contractors with network and sensitive data access into threats. The repercussions of selling data, treating it improperly, or inadvertently disclosing it can be disastrous, compromising patient safety and resulting in problems with the law and large financial damages. Similar difficulties impacted Indonesia's healthcare industry, where insider threats seriously jeopardize data security.
- **Large Attack Surface of IoT Devices:**
A typical mid-size hospital includes about 100 imaging-related servers or workstations (such as PACS servers or DICOM image viewers) and about 75 various kinds of medical imaging instruments (like X-ray, MRI, CT, or ultrasound scanners). The attack surface is increased by these IoT gadgets, which offer several ports of entry for cyberattacks.

Healthcare organizations in Indonesia and throughout the world may better safeguard their digital infrastructure, preserve patient data, and guarantee the continuation of vital healthcare services by being aware of these dangers and putting strong cybersecurity measures in place.



2.2.3 Manufacturing Sector

Due to its critical role in economic and strategic domains, manufacturing sector companies have emerged as a prime global target for cyber threats. The sheer number of data points shows how severe and sophisticated the cyber attacks the industry is facing.

Palo Alto Networks has noted the following actions that have an effect on the manufacturing industry:

- **Cyber Extortion and Ransomware:**
The Manufacturing sector tops the list of targeted industries, accounting for 20% of all cyber extortion, marking a 42% increase compared with 2022 figures.⁴ Palo Alto Networks Unit 42 assesses with high confidence that ransomware poses the most significant threat to organizations in the manufacturing industry. With 16.8% of cases, extortion-related ransomware is the most common type of investigation observed in the sector. Ransomware primarily targets the Chemicals and Specialty Materials sub-industry in Indonesia, with Squalid Scorpius (8Base) being the most common ransomware operator in this market.⁵
- **Nation-State Attacks:**
Nation-state actors frequently target this industry, driven by diverse motivations, including geopolitical ambitions and economic interests. Recent data indicates that 17.7% of nation-state attacks have been directed at the manufacturing sector.⁶ These attacks often aim to gain access to critical technologies, economic leverage, and strategic advantages essential to national goals.
- **Software Supply Chain Compromises:**
Software supply chain compromises are likely an active, increasing threat to organizations in the manufacturing industry. The targeted organization, along with its partners and clients, can be disrupted by these attacks, which can have wide-ranging impacts. It is expected that nation-state actors and hackers will continue to exploit software supply chain vulnerabilities to compromise manufacturing networks.
- **Initial Access Vectors:**
The manufacturing industry's top initial access vectors, according to data from the Palo Alto Networks Unit 42 Incident Response case survey, are software/API vulnerabilities, brute force attacks, social engineering, and insider threats. The most popular first access channels, according to reports, were phishing and vulnerabilities, underscoring the necessity of strong security protocols and staff awareness programs.⁷
- **Incident Response and Impact:**
Manufacturing accounted for 11% of all incident response instances reported in 2023, ranking it as the fourth most affected industry. In 2024, this percentage rose, highlighting the mounting danger. The ransomware that seriously disrupted operations by encrypting important data and demanding ransom payments was the subject of the most important investigations.

The soaring numbers of attacks on the manufacturing sector in Indonesia, these dynamics point to significant urgent need for enhanced cybersecurity measures, including regular vulnerability assessments, comprehensive incident response plans, and stronger collaboration between public and private sectors.

⁴ Kevin Poireault, "Manufacturing Top Targeted Industry in Record-Breaking Cyber Extortion Surge." Infosecurity Magazine, October 5, 2024. <https://www.infosecurity-magazine.com/news/manufacturing-top-targeted-orange/>

⁵ Unit 42. "Threat Actor Groups Tracked by Palo Alto Networks Unit 42." Unit 42, June 27, 2024. <https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/>

⁶ SentinelOne. "Risks Within the Factory Lines | Examining Top Threats Facing the Manufacturing Industry." SentinelOne, September 19, 2023. <https://www.sentinelone.com/blog/risks-within-the-factory-lines-examining-top-threats-facing-the-manufacturing-industry/>

⁷ Palo Alto Networks. "Incident Response 2024 Report," n.d. <https://www.paloaltonetworks.com.au/resources/research/unit-42-incident-response-report>

2.2.4 Critical Infrastructure Sector

Protecting vital assets in the critical infrastructure sector will probably require more commitment – in particular, in areas such as energy, oil, and gas sectors. Over the past decades, as this sector is a vital part of the global economy and national security, Indonesia's growing reliance on digital infrastructure within the energy, oil, and gas sectors has boosted the country's attractiveness as a main target for a range of cyber threats. Moreover, with their critical role in modern life and complex infrastructure, these sectors face complex, unique challenges.

Analysis from Palo Alto Networks Unit 42 has identified the following trends:

- **Financially Motivated Cybercrime:**
Particularly because of their dependence on continuous operations and ability to pay substantial ransoms to avoid downtime. Business email compromise (BEC) and ransomware are almost certainly the primary cyber threats facing the energy, oil, and gas sectors. And given the industry's low tolerance for downtime, cybercriminals can yield significant financial benefits from disruptive attacks.
- **Supply Chain Vulnerabilities:**
Threat actors are likely to adopt indirect targeting strategies, often initiating attacks through the supply chain. The complex and multi-faceted supply chain is becoming the most significant threat facing the energy, oil, and gas industry. If a breach in any part of this chain can happen, this would compromise the entire network, leading to significant disruptions and financial losses.
- **State-Sponsored Cyber Espionage:**
For financial and commercial gain, state-sponsored cyber espionage is likely to continue to target the energy, oil and gas industries. Confidential research, corporate planning, and trade secrets are particularly at risk from such attacks. The energy sector is expected to be a prime target for state-sponsored cyber activity due to its association with Critical Infrastructure (CI), especially during times of geopolitical crisis. State-sponsored actors typically target operational technology (OT) networks that manage key industrial assets in the sector. However, until there is a high probability of active conflict, it is highly doubtful that state-sponsored cyber attackers would intentionally disrupt or damage the infrastructure that supports the oil and gas industry.
- **High-Profile Attacks and Media Coverage:**
Attacks on the energy industry are common and cause enough damage that they are often in the headlines in various news outlets, not just tech magazines. While many perpetrators are nation-state actors, this does not exclude the possibility of cybercriminal activity or hacktivism. The criticality of energy production to nearly every facet of modern life increases the industry's vulnerability to cybercrime and nation-state actors.
- **Complex Technologies and Geopolitical Policies:**
The risks involved clearly extend beyond energy suppliers and producers. Recently, the industry's attack surface has increased dramatically due to complex technologies and the geopolitical policies that support them. Governments may be interested in conducting cyberattacks to destroy vital infrastructure, set the stage for future attacks, and find weaknesses in their adversaries' energy infrastructure for economic espionage.

In Indonesia, the country's growing reliance on digital infrastructure within energy, oil, and gas sectors continues to make them attractive targets for cybercriminals and nation-state actors alike.



2.3 Cost of Cybercrime for Indonesia

Global cybercrime continues to proliferate at alarming rates as projections indicate that damage from cyberattacks will amount to about \$10.5 trillion annually by 2025, a staggering increase from \$3 trillion in 2015 at the current growth rate.⁸ Globally, the bulk of these losses stem from ransomware and data breaches, with the financial services, healthcare, and manufacturing sectors being the hardest hit; in addition to immediate financial losses, these sectors also confront recovery expenditures, legal accountability, and injury to reputation. Furthermore, Operational disruptions also result from cyber attacks. For example, the loss of valuable intellectual property and additional expenditures required for cybersecurity measures all factors that contribute to the widening economic consequences.

Economic Impact of Cybercrime in Indonesia

As the Indonesian digital economy grows, high-profile cybercrime grows with it, and also significant financial impacts in Indonesia, amount to about \$4.79 billion annually by 2028 - a 35.7 percent increase from 2018 level.⁹ Ransomware attacks on critical infrastructure and data breaches that expose personal and sensitive Government data are some examples of common cybercrime that have occurred in Indonesia.

Estimated annual cost of cyber crime in Indonesia from 2018 to 2028 (in billion U.S dollars)

Annual cost of cyber crime Indonesia 2018 - 2028

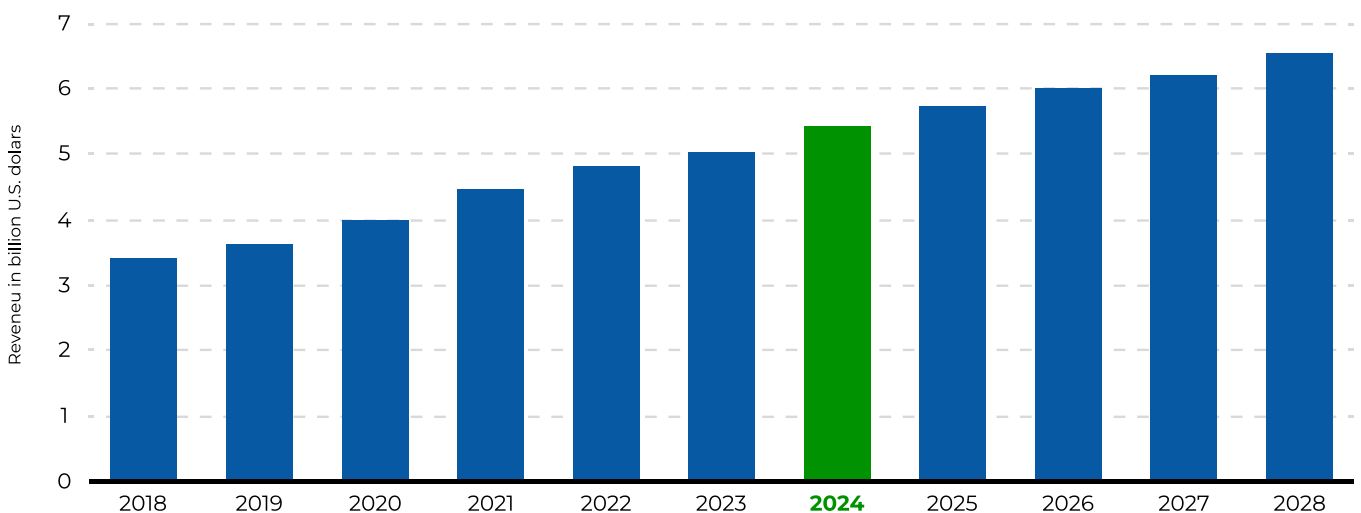


Exhibit 2.5 Projected Annual Cost of Cyber Crime in Indonesia from 2018 - 2028 (In Billion U.S dollars)

Source: Statista Technology Market Insights

Strategic Response to Mitigate Costs

Indonesia has the opportunity to substantially reduce the financial damage caused by cybercrime while also becoming more resilient against future threats. In an attempt to reduce the financial damage, we have found that it is a very demanding task to determine effective strategies to address economic costs of a lack of cybersecurity in Indonesia. Such strategies include enforcing robust cybersecurity policies, public-private sector collaborations, cybersecurity education investment, and robust incident response framework.

⁸ Mitangi Parekh, "Cybersecurity Ventures Report on Cybercrime." eSentire, August 29, 2024. <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime>.

⁹ Statista, "Annual Cost of Cyber Crime Indonesia 2018-2028," September 4, 2023. <https://www.statista.com/forecasts/1411153/indonesia-cost-of-cyber-crime#:~:text=In%202022%2C%20the%20cost%20of%20cyber%20crimes%20in,from%202018%20to%202028%20%28in%20billion%20U.S.%20dollars%29>



Chapter 

03

Strategic Pillars for Cybersecurity

As Indonesia accelerates its journey towards digitalization, it is also seeing an increasing range of cyber threats that could hinder the country's economic growth, national security, and critical infrastructure. To address these challenges, Indonesia must establish cybersecurity strategic pillars to outline a firm foundation for the national cybersecurity ecosystem that is resilient enough to confront ongoing challenges.



Exhibit 3.1 Strategic Pillars for National Cybersecurity

3.1 Pillar 1: Cyber Resilience in Critical Infrastructure

Strengthening the resilience of Indonesia's critical infrastructure sectors (such as banking, healthcare, and energy) is the aim of this pillar. In an attempt to protect these industries from cyberattacks, some key actions such as implementing periodic sector assessments, cybersecurity framework tailored to each industry, supported by an Advanced Security Operations Center (SOC) are essential to be implemented.

Critical Areas of Focus:

- Regular Cybersecurity Audits and Vulnerability Assessments**
 Provide a mechanism to conduct periodic risk assessments, penetration tests, and stress tests on infrastructure that simulates cyber attacks.
- Incident Response and Recovery Plans**
 Develop standard incident response and recovery methods for critical sectors. Each sector must have an incident management plan specific to the threat situation in that industry.
- Sector-Specific Security Operations Center** Establish a dedicated SOC for each critical sector to ensure real-time threat monitoring, analysis, and coordinated responses to cyber incidents that align with a centralized national SOC to ensure unified defense mechanisms across sectors.

3.2 Pillar 2: Enhancing Cybersecurity Governance and Regulations

Developing and enforcing a robust cybersecurity governance and regulations is the second pillar's objective. It stresses the importance of aligning national laws with international standards, strengthening existing regulations, creating cybersecurity SROs, and ensuring regular updates in response to emerging cyber threats.

Critical Areas of Focus:

- **Align with International Standards**
Adopts and adheres to global data privacy standards such as ISO/IEC 27001 and the General Data Protection Regulation (GDPR) to drive seamless integration and trust in Indonesia's cybersecurity procedures.
- **Centralized Cybersecurity Regulations**
Ensure that cybersecurity is elevated to the top levels of government, such as direct oversight by the President of Indonesia, and centrally managed by a high-capable regulatory body such as the cybersecurity agency, which would enforce policies, oversee compliance, and manage national incidents.
- **Establish Self-Regulatory Organization (SRO)** Create Indonesia's local cybersecurity self-regulatory organization (SRO) to strengthen the nation's cybersecurity posture by fostering collaboration, tailored standards, and protecting local cybersecurity providers.
- **Regular Updates and Legal Framework Enhancement**
Ensure existing cybersecurity and data protection laws evolve as new cyber threats and technologies emerge. Regulatory bodies must be empowered to update frameworks as necessary.

3.3 Pillar 3: Developing Cybersecurity Talent and Awareness

Building a pipeline of qualified cybersecurity professionals and a cybersecurity awareness culture is the third pillar's objective. It stresses the importance of increasing public awareness of cybersecurity risks and ensuring institutions have access to well-trained personnel, further supporting the development of a resilient local cybersecurity industry.

Critical Areas of Focus:

- **Cybersecurity Education Initiatives**
Collaborate with various existing academic institutions and technical centers, both domestic and foreign, to create a particular cybersecurity curriculum with an emphasis on internships, certification programs, and hands-on training.
- **Upskilling the Workforce**
Provide ongoing training and certification opportunities for existing IT professionals to sharpen their cybersecurity capabilities.
- **Public Awareness Campaigns:**
Launch a national initiative to educate companies, organizations and the general public about the importance of cybersecurity, data privacy and safe online habits.

3.4 Pillar 4: Public-Private Partnerships

In an attempt to develop a more unified and successful national cybersecurity strategy, pillar four emphasizes the necessity of cooperation between government agencies and businesses in the private sector. Public-private partnerships are crucial for exchanging resources, intelligence, and best practices.

Critical Areas of Focus:

- **Real-Time Threat Intelligence Sharing**
Provide a nationwide platform for the exchange of real-time threat intelligence between the public and private sectors. This platform need to be an AI-enhanced system that assesses new risks and plans coordinated sector-wide responses.
- **Cyber Incident Review Boards**
Create a national board including representatives from major corporations, government agencies, and local and global cybersecurity experts. This group will look at notable cyber incidents and provide suggestions for enhancements.



- **Collaborative Research and Development:** Encourage joint R&D projects between government organizations, educational institutions, and private companies to develop cutting-edge cybersecurity solutions, with a focus on cutting-edge technologies like blockchain, AI, and quantum computing.

3.5. Pillar 5: Aligning Indonesia with Standardized Cybersecurity Methodologies and Standards

Being able to apply globally accepted cybersecurity methods and standards (such as ISO and NIST) is the objective of the fifth pillar. And to achieve the seamless integration and efficient defense systems, it will require developing an integrated approach to cybersecurity across industries.

Critical Areas of Focus:

- **Adoption of Global Standards (ISO, NIST)**
Must ensure that cyber security guidelines and practices in Indonesia are in line with global standards to improve the smooth operations of companies that conduct business globally.
- **Risk Management Frameworks**
Drive the implementation of a comprehensive cybersecurity risk management framework in public and private organizations.
- **Compliance Audits and Reporting**
Require cybersecurity assessments to be conducted periodically, especially for economic sectors that depend on critical infrastructure, and require comprehensive reporting on compliance with established protocols.

3.6. Pillar 6: Strengthening Local Players in Indonesia Cybersecurity Industry Growth

The presence of a robust local cybersecurity market is fundamental to protecting Indonesia's critical infrastructure, minimizing reliance on foreign technologies, and encouraging economic development. This pillar discusses primary approaches to creating a competitive, innovative, and independent local cybersecurity ecosystem.

Critical Areas of Focus:

- **Ideal Provision**
Local companies are expected to focus on niche markets like threat intelligence and incident response and act as value-added resellers (VAR) of external technologies. Positive government incentives, such as tax holidays and grants for research and development, will encourage local development and allow them to compete globally.
- **Transition to Innovation**
It is a must for Indonesia to be able to expand its cyber security offerings and does more than just install off-the-shelf solutions. RnD will run faster if innovation centers are built and collaboration between academia and business is encouraged. This will enable solutions that better suit the unique needs of the country.
- **SRO Standardization**
To guarantee the credibility and competitiveness of local Indonesian businesses in the market, an SRO must provide certification programs and industry standards. This attempt aims to encourage equal competition and enable companies to take part in national initiatives.
- **Policy and regulatory support**
Improve regulations through local content mandates, preferential treatment, regulatory simplification, and anti-dumping laws to directly help and improve the competitiveness of local cybersecurity companies.



Chapter

04

Sector-Specific Cybersecurity Insights

As Indonesia accelerates its digital transformation, attacks on sectors such as financial services, health-care, manufacturing and energy, which are some of the main critical sectors in Indonesia, are increasingly widespread, making them vulnerable to growing cyber risks. The following sections will discuss sectoral asset mapping, attack surface management, and vulnerabilities specific to each critical sector.

4.1 Asset Mapping and Attack Surface Management

As the digital ecosystem accelerates its growth, it expands our exposure to cyber risk. It is becoming truly essential for organizations to prioritize understanding and managing their attack surface as this would help them to evaluate network infrastructure from an adversary’s perspective in an attempt to identify vulnerabilities that exist and can be exploited by adversaries as attack vectors. Furthermore, organizations begin to accelerate the modernization of their IT infrastructure—through cloud adoption, SaaS platforms, and distributed workforces—and their attack surface, thus will grow dramatically. **Effective Attack Surface Management (ASM) should thus become an integral part of their strong cyber security posture.**

The Need for Attack Surface Management (ASM)

Your Attack Surface is made up for..

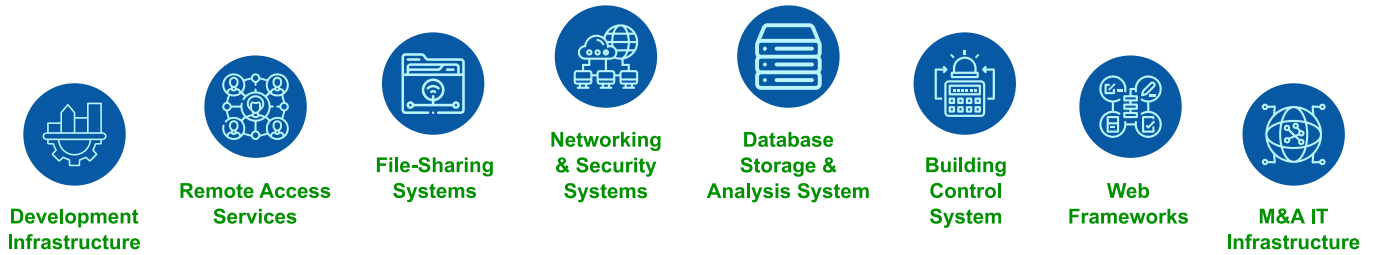


Exhibit 4.1 Attack Surface Management , Source: Palo Alto Networks Cyberpedia

Organizations are increasingly unable to manage their sprawling IT environments due to the sheer number of services added and updated. According to the Palo Alto Networks Unit 42 Threat Assessment Report, the average organization adds or updates more than 300 services monthly, contributing to 32% of new high or critical cloud exposures. This challenge is even greater in certain industries:

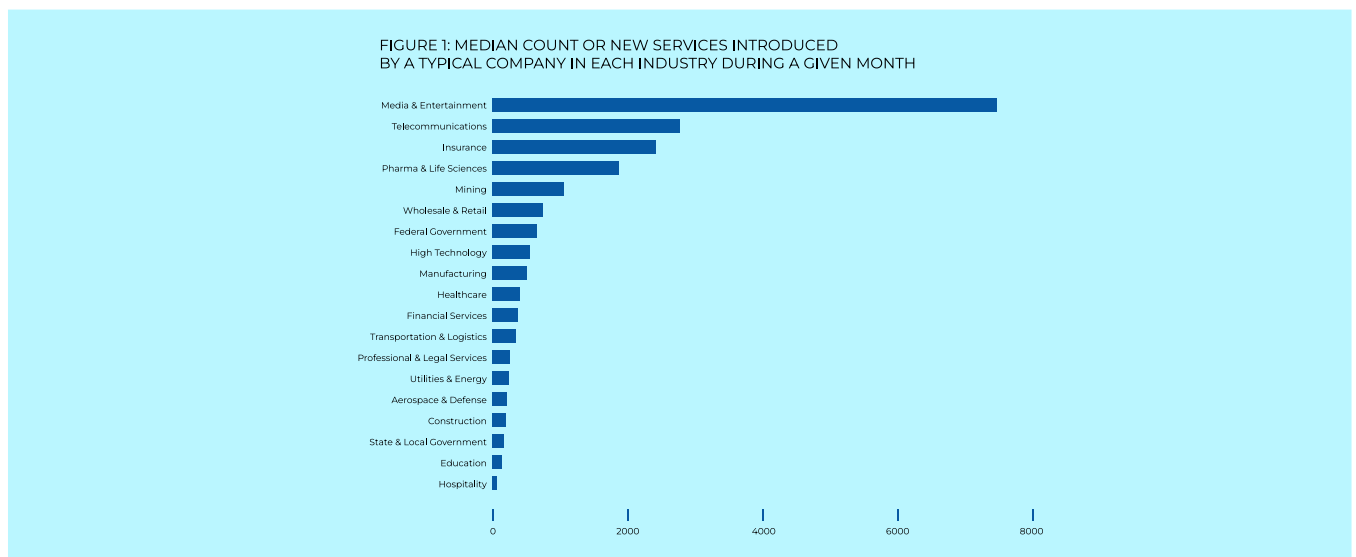


Exhibit 4.2 Indonesia’s Most Impacted Industries by Ransomware Attacks in 2023
Source: Palo Alto Networks Unit 42 Attack Surface Threat Report 2024

- It found out that the **media and entertainment industry** adds about 7,000 new services each month.
- **The life sciences, insurance, telecommunications, and pharmaceutical industries** all see significant growth; each month, more than 1,000 new services are added to their attack surfaces.
- **More than 200 new services are added to the attack surfaces of vital industries** including finance, healthcare, and manufacturing each month.

With a lack of centralized control across many public services in Indonesia, their complexity becomes increasingly challenging, increasing the risk of misconfiguration, inconsistent exposure, and data breaches. Attack Surface Management, which provides programmatic methods to detect, control, and mitigate risk through continuous observation and evaluation of an organization's exposed digital assets, is critical in this complexity.

Fundamental Principles of Attack Surface Management (ASM)

1. Visibility is Critical

- **“You cannot secure what you do not know”** is the foundational principle of ASM that needs to be adopted in an attempt to prevent cyber attack. Therefore, it becomes necessary to consistently identify all the unknown and known company's existing assets that are exposed to the internet. These may include IP addresses, domains, and cloud instances that potentially can be leveraged by attackers.
- With ASM organizations can use automated tools that are able to scan public-facing infrastructure and point out vulnerabilities in real time. This would significantly reduce the window of opportunity for attackers.

2. The ASM Process:

- ASM is a non-invasive methodology based on domain names or IP ranges, furnishing insight into exposed services, misconfigurations, and non-protected assets. With this non-invasive methodology, ASM has the ability to provide crucial visibility into the possible attack vectors, from software vulnerabilities to misconfigured cloud storage solutions.

3. Adversaries Act Fast; Organizations Must Act Faster

- When it comes to capabilities, organizations frequently come behind attackers. For instance, Palo Alto finds that if a vulnerability is disclosed, attackers begin scanning the internet for vulnerabilities within 15 minutes. Nonetheless, it might take a company up to 12 hours to find and fix problems. The 2024 Palo Alto Unit 42 Incident Response Report also finds that most large-scale campaigns begin by exploiting systems visible on the internet and that initial access is often gained through software vulnerabilities.

Rising Threats and the Importance of ASM

Organizations are exposed to a greater variety of risks as they expand, which may be divided into several device business functions. Palo Alto Networks Unit 42 identified the following key trends in attack surface exposures:

Figure 2: Distribution of Exposure Categories Across the 265 Organizations in the 12 Months

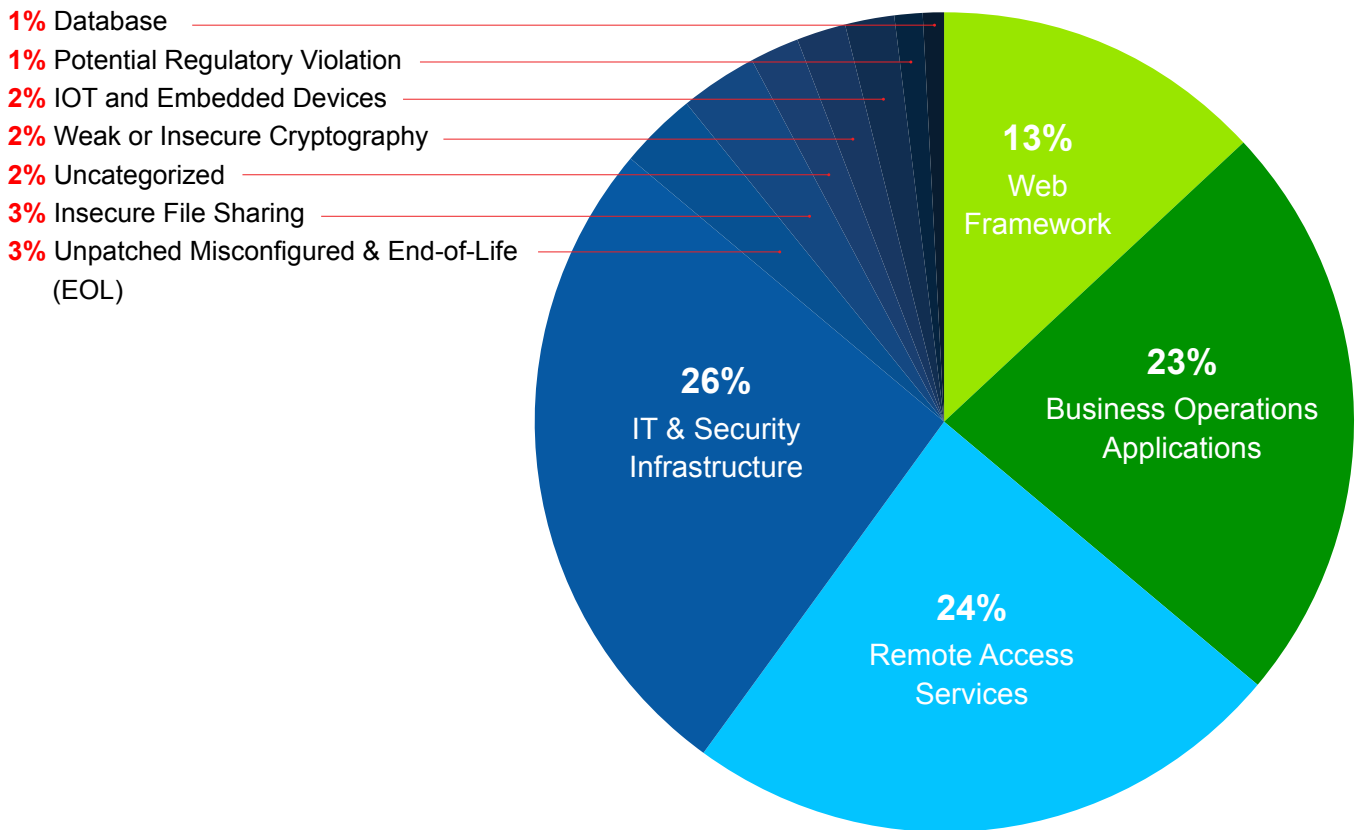


Exhibit 4.3 Distribution of Exposure Categories Observed Across Organizations in the Last 12 Months
Source: Palo Alto Networks Unit 42 Attack Surface Threat Report 2024

- IT and Networking Infrastructure (25%)**
 Systems that underpin core networking, such as routers, VPNs, and firewalls, are a source of critical vulnerabilities. Frequently, attackers attempt to breach sensitive data on these devices and disrupt core business operations.
- Remote Access Services (24%)**
 Today's remote work is possible using Virtual Network Computing (VNC), Secure Shell (SSH), and Remote Desktop Protocol (RDP). However, these components leave companies vulnerable to large-scale ransomware campaigns and brute force attacks if they are misconfigured or exposed. RDP has become one of the primary attack vectors for significant ransomware incidents.
- Business Operations Applications (23%)**
 Collaboration tools, CRMs, and project management software are vulnerable, leading to disruptions in business continuity. Such breaches in industries that handle PII and PHI pose huge regulatory and financial risks.
- Web Framework Takeovers (13%)**
 Outdated or insecure web frameworks like Apache, PHP, and jQuery are critical vulnerabilities that attackers intend to leverage. This happens because the patches are known but not applied.
- Insecure File Sharing (3%)**
 Attackers can exfiltrate public file-sharing services, poorly configured classic FTP servers, and misconfigured cloud storage. In fact, these pose a very serious risk in sectors with strict regulatory requirements for data protection.

Emerging Vulnerabilities and Critical Risks

As organizations and businesses work to modernize their IT infrastructure further, new risks pop up. Several areas need special attention over the following years:

1. Unpatched, Misconfigured, and End-of-Life (EoL) Systems:

Systems that operate with end-of-life software or those that are not correctly patched are soft targets. Using a critical vulnerability in an outdated router, an attacker can intercept network traffic, steal data, or disrupt services.

2. Weak or Insecure Cryptography:

Weak encryption protocols leave sensitive communications susceptible to decryption, compromising confidentiality and regulatory compliance. Organizations are supposed to audit and advance their encryption practices on a routine basis to avoid data interception.

3. IoT and Operational Technology (OT):

This increased integration of IoT devices and OT into corporate environments has significantly broadened the attack surface. Because many of these devices' security features are inadequate, many of them are attractive targets for DDoS and botnet recruitment, which could have an adverse effect on both business operations and individual safety.

4. Development Infrastructure:

Development environments include source code repositories, build servers, and other high-value targets for adversaries who use this position to steal intellectual property or inject malicious code. Compromising these environments could undermine trust in an organization's software and disrupt business operations.

4.2 Sector-Specific Cybersecurity Analysis

Each industry faces unique cybersecurity issues in terms of cyber risk, so different risk mitigation strategies must be implemented for different sectors. Due to their unique cybersecurity issues, in the following section, sector-specific vulnerabilities and risks (Financial services, healthcare, and manufacturing) will be examined in detail, and, in the end, develop strategic actions to strengthen cybersecurity resilience in each of the three key sectors.

4.2.1 Financial Services Sector

Due to its accessibility to sensitive financial data and other important services closely related to banking institutions and other financial organizations, the financial services industry is often becoming the main target of cyber attacks. In this sector, cybersecurity breaches can result in significant financial losses, legal fines, long-term damage to reputation, and other permanent harm.

In a recent cybersecurity evaluation by Mastercard (Appendix 1: Mastercard RiskRecon Overview), which benchmarked 10 Indonesian financial institutions against 50 in the Asia-Pacific region, found mixed cybersecurity performance across the sector, with several areas needing improvement.

Financial Sector Cybersecurity Performance Overview

Indonesia's financial institutions received an overall rate of **B**, or **8.4 out of 10**, in general cybersecurity performance, **slightly below the average regional grade of 8.8 for the Asia Pacific region**. As in the

exhibit 4.4, Indonesian financial institutions underperformed their regional peers in five of nine critical security domains.

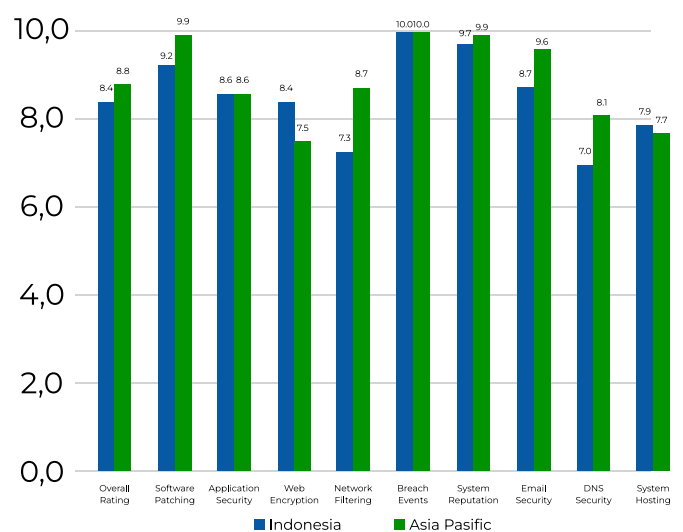


Exhibit 4.4 Financial Sector Cybersecurity Performance Comparison Between Indonesia and Asia Pacific
Source: US-ABC

Evaluating Indonesia's Financial Sector

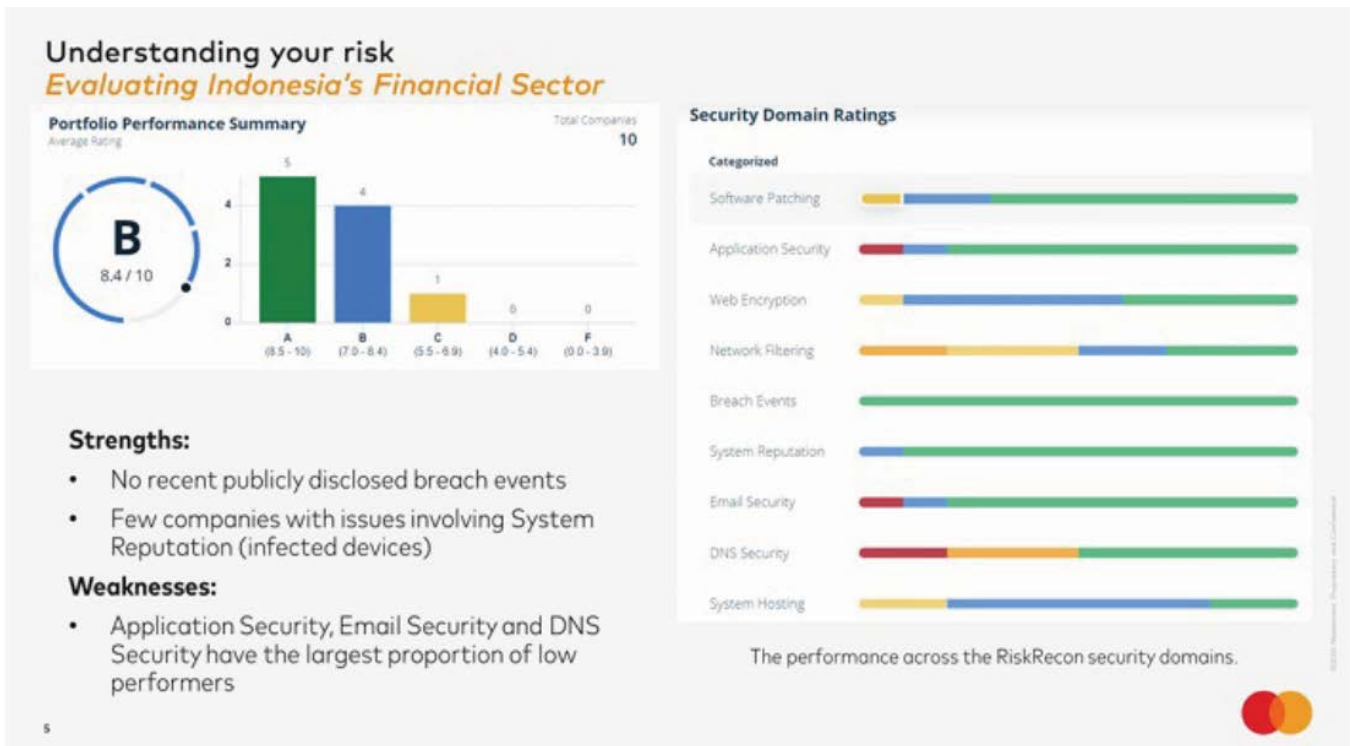


Exhibit 4.5 Indonesia's Financial Sector Security Performance, **Source:** Mastercard

The **Performance Summary** diagram by Mastercard demonstrates the following:

- **Five institutions** achieved an **A rating (8.5-10)**, indicating strong cybersecurity practices.
- **Four institutions** fell into the **B-rating range (7.0-8.4)**, this score reflecting moderate security performance.
- **One institution** scored in the lower range of **C (5.5-6.9)**, this core indicating substantial security weaknesses.

Strengths and Weaknesses

Based on the evaluation carried out by Mastercard in the **exhibit 4.5**, we identified the following areas of strength and improvement needed for Indonesia financial service sector:

Strengths:

- **No reported breach incidents:** Indonesian financial institutions have managed to avoid significant breaches in recent years.
- **System Reputation:** Few organizations showed infected devices or malware activities associated with their infrastructure, which indicates malware controls are in place.

Weaknesses:

- **Application Security, Email Security, and DNS Security** are the domains where most institutions score poorest in the Security Domain Ratings Diagram. Each of these areas presents critical vulnerabilities that should be targeted with immediate action to enhance the general cybersecurity posture in the sector.

These findings reveal that more attention needs to be paid to the security of web applications and email vulnerabilities, which are vital components in the financial sector's overall cybersecurity resilience.

Key Vulnerabilities Identified in Financial Sector

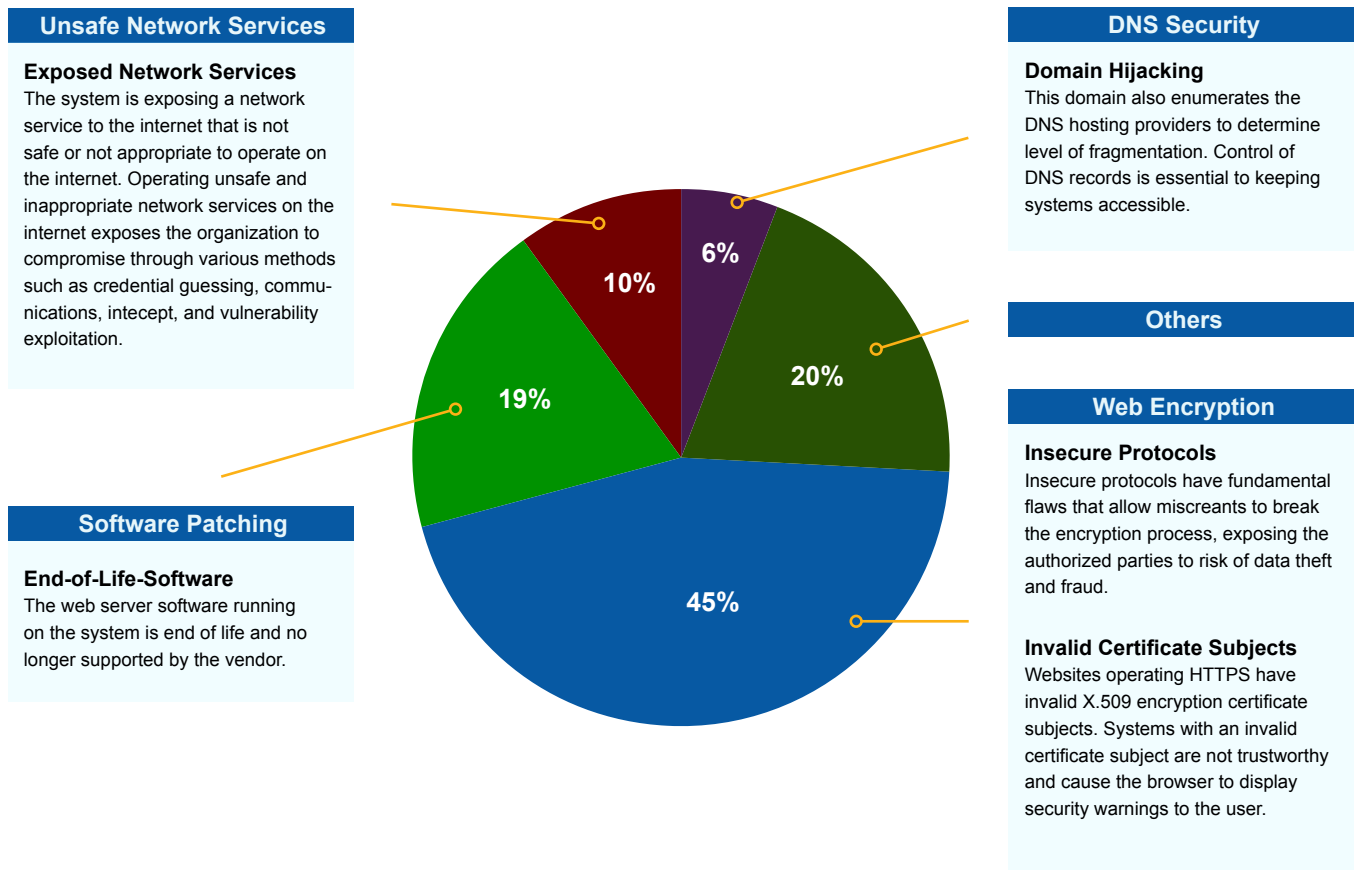


Exhibit 4.6 Security Vulnerabilities by Category in Indonesia's Financial Sector, **Source:** Mastercard

A total of **1,696 issues** within nine security domains were found, as represented in the **exhibit 4.6**. The most critical vulnerabilities identified include:

- Web Encryption (45%):**
 Weak encryption techniques and insecure protocols exposed financial data to fraud and intercepting, which was a major problem in the Indonesian banking system. This vulnerability constituted nearly half of the identified issues.
- End-of-Life Software (19%):**
 It was discovered that several financial institutions in Indonesia were still utilizing outdated software, such as PHP, Apache, and IIS, which was not receiving security upgrades. This greatly broadens the attack surface available to cybercriminals.
- Unsafe Network Services (10%):**
 Several vulnerable services, including MySQL, were found to be lacking the required security measures. These services' open ports and susceptibility to exploitation increase the likelihood of unauthorized access.

Risk Classification and Mitigation Prioritization

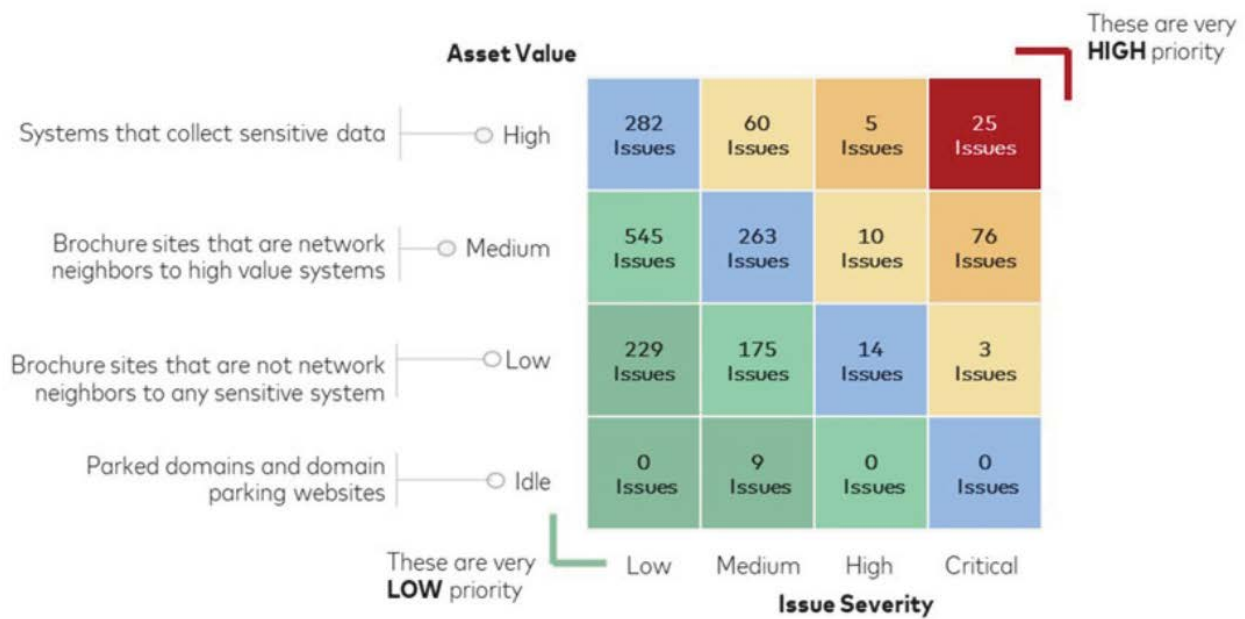


Exhibit 4.7 Indonesia's Financial Sector Risk Prioritization Matrix, **Source:** Mastercard

The **exhibit 4.7** categorizes the **1,696 vulnerabilities** by asset value and issue severity to enable institutions to prioritize remediation work efforts by risk impact. Key risk categories include:

- High Priority:**
 On critical issues, some 25 identified high-value systems, such as those dealing in sensitive financial data, were assessed. These should be immediately remediated to protect against data breaches and system compromise.
- Medium Priority:**
 Medium priority issues to systems immediately adjacent to high-value assets totaled 76. These are systems that do not handle sensitive data directly but whose exploitation could grant the attackers lateral movement onto more critical infrastructure.
- Low Priority:**
 These were the hosts of relatively low-risk systems, such as domains kept idle and non-essential services. They should not pose any imminent danger, but the vulnerabilities should be patched to avoid future hacks.

The majority of the problems are related to out-of-date software (PHP, IIS, Perl, Apache, and Nginx) that has known security vulnerabilities, as well as a system that exposes a network service (MySQL) to the Internet that is either unsafe or inappropriate to use.

4.2.2 Healthcare Sector

The healthcare industry is becoming increasingly important to Indonesia's national infrastructure as a result of the industries' massive storage of Personally Identifiable Information (PII) and Protected Health Information (PHI). Cybercriminals see healthcare facilities to be an attractive target due to these information databases. A cyberattack on this industry might endanger many lives by leaking data, interfering with hospital operations, or even affecting patient care.

In a recent cybersecurity evaluation, Mastercard evaluated 50 healthcare organizations in the Asia-Pacific area with 10 healthcare organizations in Indonesia. This study provides insight into Indonesia's health sector's current cybersecurity posture, pointing out strengths and vulnerabilities compared to regional counterparts.

Healthcare Sector Cybersecurity Performance Overview

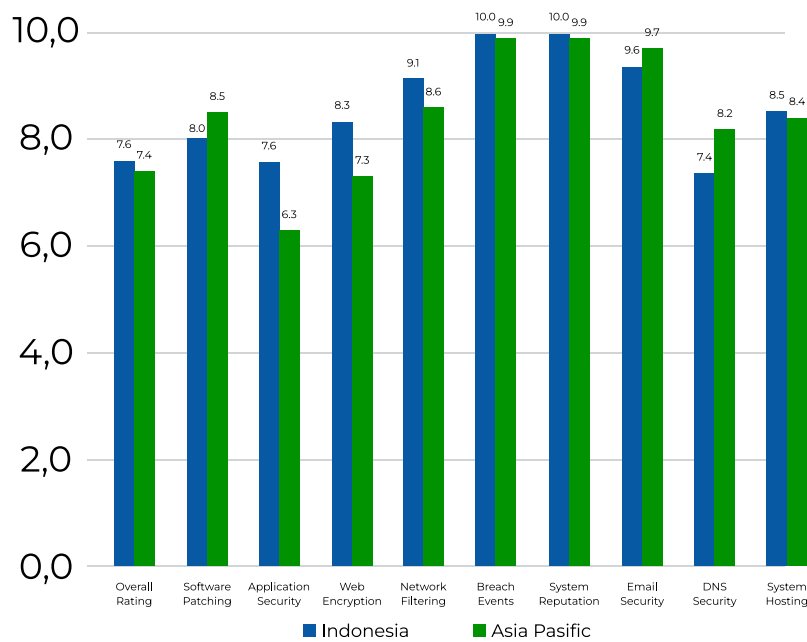


Exhibit 4.8 Healthcare Sector Cybersecurity Performance Between Indonesia and Asia Pacific, **Source:** Mastercard

Indonesian healthcare institutions' overall cybersecurity performance was rated at **B (7.6/10)**, which is slightly above the **Asia-Pacific healthcare industry average score of 7.4**. The exhibit 4.8 illustrates this comparison, revealing that Indonesian healthcare organizations performed better in six of nine critical security domains than their regional peers.

Evaluating Indonesia's Healthcare Sector

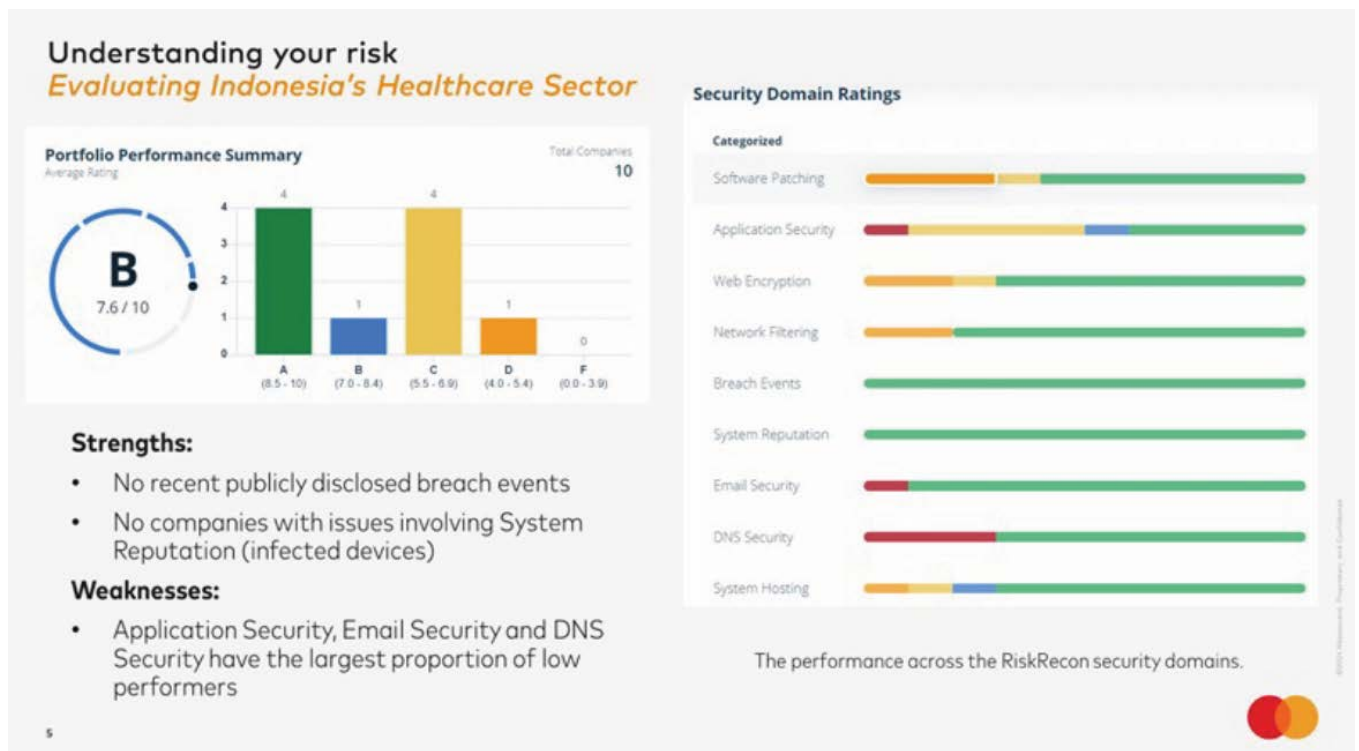


Exhibit 4.9 Indonesia's Healthcare Sector Security Performance, **Source:** Mastercard

Key points from the **Performance Summary** Diagram include:

- **Four institutions** were rated **A (8.5-10)**, reflecting a strong cybersecurity posture.
- **One institution** scored in the **C range (5.5-6.9)**, indicating areas for substantial improvement.
- **One institution** was identified with a score **below 5.5**, demonstrating critical cybersecurity vulnerabilities.

Strengths and Weaknesses

As highlighted in the **exhibit 4.9**, the key strengths and weaknesses in the Indonesian healthcare sector’s cybersecurity performance include:

Strengths:

- **No publicly disclosed breach events:** The healthcare institutions assessed have avoided significant data breaches recently, indicating adequate controls to safeguard patient information.
- **System Reputation:** Regarding system reputation, none of the institutions in the healthcare sector mentioned any severe problems, such as infected devices or malicious activities within their infrastructure.

Weaknesses:

- **Application Security, Email Security, and DNS Security** were identified as the weakest areas across the sector, highlighting a critical need for enhanced security measures in these domains. These vulnerabilities can significantly impact the confidentiality and integrity of patient data.

Key Vulnerabilities Identified in Healthcare Sector

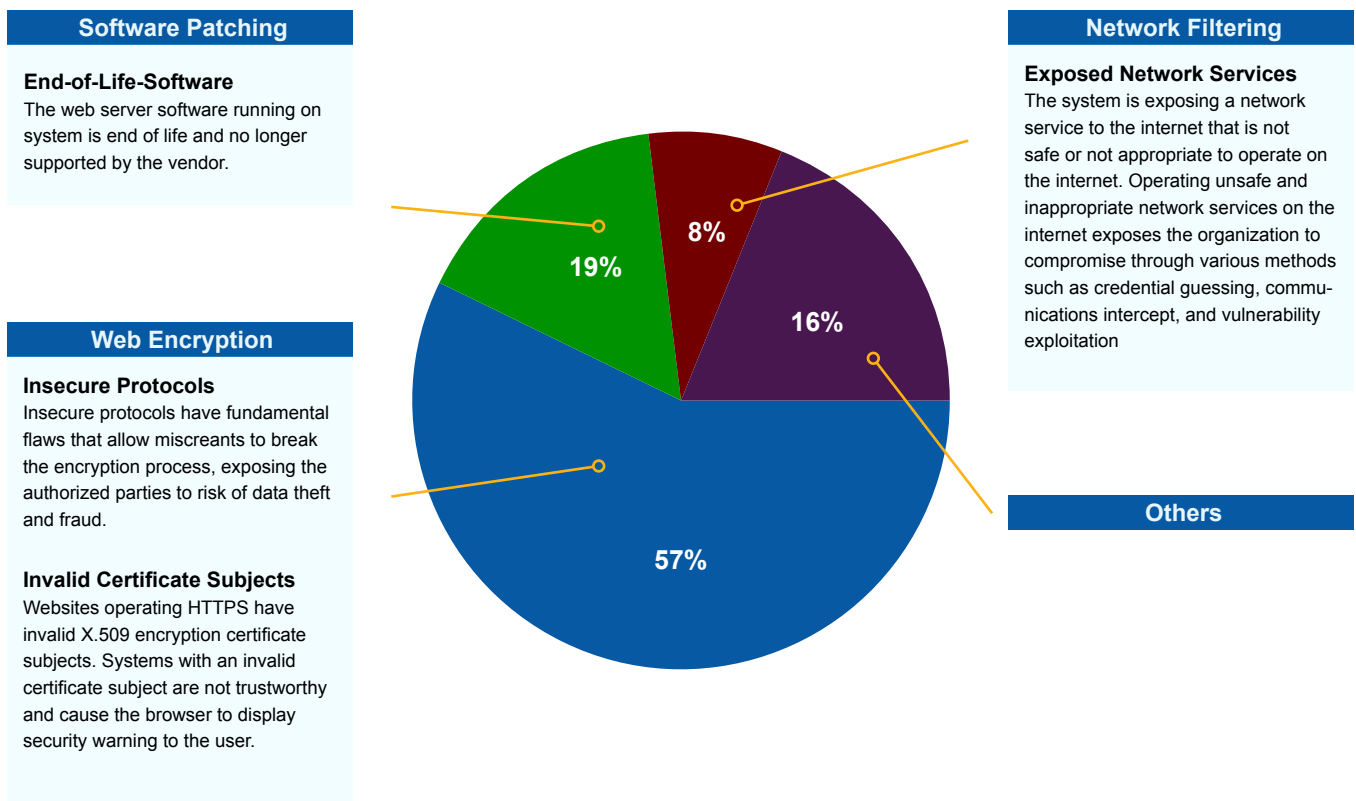


Exhibit 4.10 Breakdown of Security Vulnerabilities by Category in Indonesia’s He Sector, **Source:** Mastercard

The assessment uncovered **354 vulnerabilities** across nine security domains, as illustrated in the **exhibit 4.10**. The most critical vulnerabilities identified include:

- Web Encryption (57%):**
 Ineffective encryption techniques and expired encryption certificates were the most frequent issues jeopardizing the confidentiality of personal health information. Outdated encryption methods compromise confidentiality and regulatory compliance by making patient data susceptible to theft or fraud.
- Software Patching (19%):**
 It was discovered that many healthcare institutions were running outdated versions of Word-Press, Nginx, and PHP, among other end-of-life software. These systems are no longer supported by security updates, thus known security flaws might take advantage of them.
- Network Filtering (8%):**
 Several healthcare facilities' network services, including MySQL, are accessible to the public due to inadequate security procedures. This broad attack surface increases the likelihood of data breaches and unauthorized access.

Risk Classification and Mitigation Prioritization

Prioritizing remediation activities was achieved by classifying the 354 vulnerabilities using the Risk Prioritization Matrix based on issue severity and asset value. Healthcare facilities may concentrate their security efforts on the most important threats by following the clear route provided by the matrix.

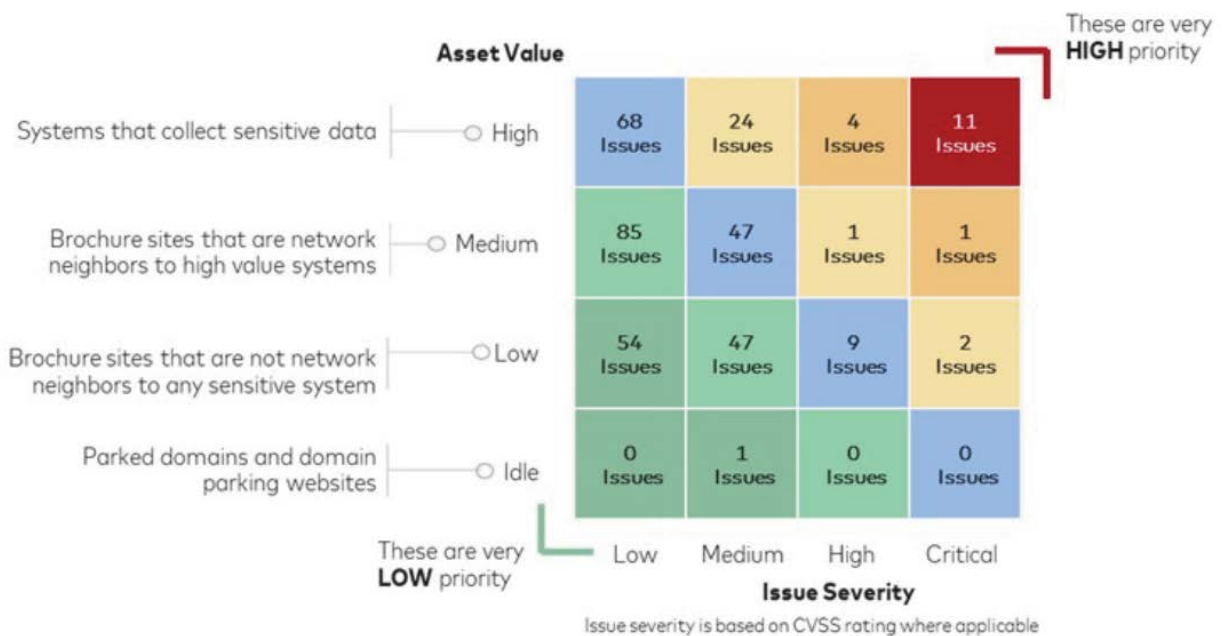


Exhibit 4.11 Indonesia's Healthcare Sector Risk Prioritization Matrix, **Source: Mastercard**

Key findings include:

- High-Priority Risks:**
 Eleven significant issues were discovered with high-value systems that oversee personal health data. These must be corrected immediately to prevent data breaches and maintain the integrity of healthcare operations.
- Medium-Priority Risks:**
 Forty-seven issues were discovered in medium-value systems that are on the same network as high-value systems but may not directly handle

sensitive data. These vulnerabilities need to be addressed very once in order to stop future exploitation and the possibility of lateral attacks.

- Low-Priority Risks:**
 The remaining issues were related to low-value systems, such as brochure websites or idle domains, which do not pose immediate security risks but should be monitored to prevent future exposures.

Most of the issues revolve around using outdated software (PHP, WordPress, Perl, Nginx) with known security vulnerabilities and exposing unsafe network services (such as MySQL) to the internet. These vulnerabilities pose significant risks to healthcare institutions' digital infrastructure integrity.

4.2.3 Manufacturing Sector

The manufacturing sector is essential to Indonesia's economy due to its significant GDP contribution and role in supporting critical infrastructure. This industry's vital role makes it a great target for cybercriminals looking to disrupt or exploit sensitive data. In a recent cybersecurity study, Mastercard compared 50 manufacturing institutions in Asia-Pacific with 10 Indonesian manufacturing firms. Compared to its regional counterparts, the evaluation provides insightful information about the industry's cybersecurity posture.

Manufacturing Sector Cybersecurity Performance Overview

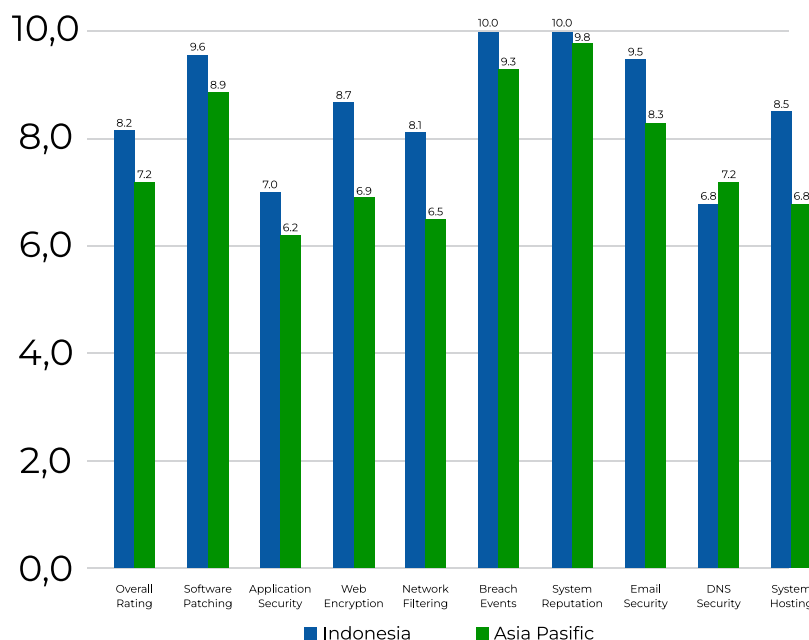


Exhibit 4.12 Manufacturing Sector Cybersecurity Performance Between Indonesia and Asia Pacific, **Source:** Mastercard

The overall cybersecurity performance of Indonesian manufacturing institutions was rated at **B (8.2/10)**, significantly higher than the **Asia-Pacific manufacturing industry average of 7.2**. As shown in the exhibit 4.12, Indonesia outperformed the regional average in eight out of nine security domains.

Evaluating Indonesia's Manufacturing Sector



Exhibit 4.13 Indonesia's Manufacturing Sector Security Performance, **Source:** Mastercard

Key takeaways from the **Performance Summary** include:

- **Five institutions** achieved an **A rating (8.5-10)**, reflecting strong cybersecurity performance.
- **Two institutions** fell into the **B-rating (7.0-8.4)** range, indicating a solid but improvable security posture.
- **Three institutions** scored in the **C-range (5.5-6.9)**, demonstrating areas for significant improvement in security practices.

Strengths and Weaknesses

As highlighted in the **Exhibit 4.13**, the key strengths and weaknesses in the Indonesian healthcare sector's cybersecurity performance include:

Strengths:

- **No recent publicly disclosed breach events:** The absence of notable data breaches announced by Indonesian manufacturing companies suggests that a strong control framework is in place to protect sensitive data.
- **No companies with issues involving System Reputation:** The well-maintained network hygiene of all the evaluated firms was demonstrated by the lack of issues pertaining to system reputation, such as infected devices or malicious activities.

Weaknesses:

- **Application Security:** The manufacturing industry has a large number of underperforming firms when it comes to application security, so there is definitely room for improvement.
- **Network Filtering:** Weaknesses in network filtering indicate that several organizations have improperly secured or misconfigured network services, increasing the risk of unauthorized access.
- **DNS Security:** DNS security is another domain where many organizations are performing poorly, which could expose their systems to attacks like DNS spoofing or man-in-the-middle attacks.

Key Vulnerabilities Identified in Manufacturing Sector

As shown in figure 4.14, the evaluation found 419 vulnerabilities spread across nine security domains. The following are the most important vulnerabilities found:

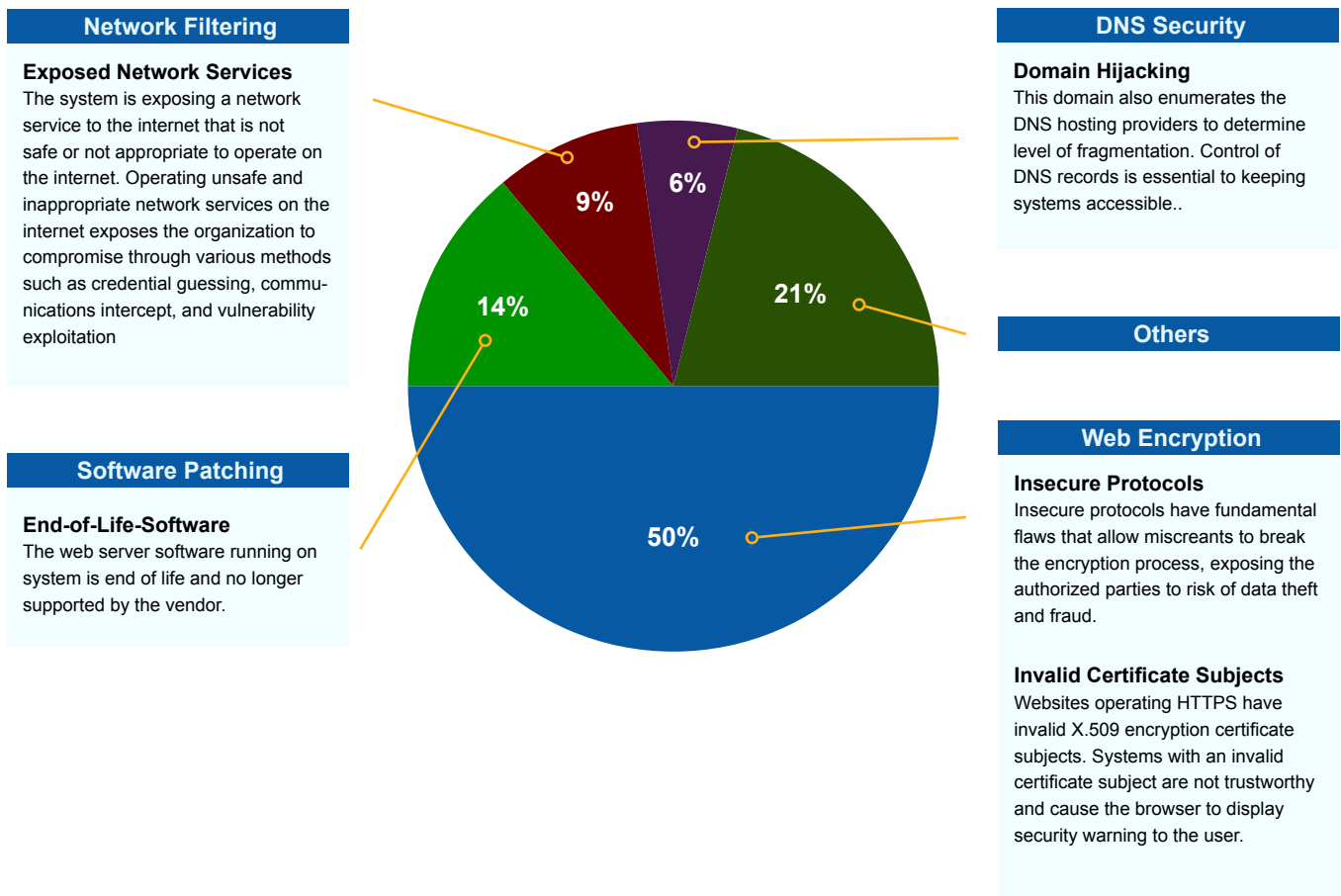


Exhibit 4.14 Security Vulnerabilities by Category in Indonesia's Manufacturing Sector, **Source:** Mastercard

1. Web Encryption (50%):

It was found that many businesses were using insecure encryption protocols and out-of-date certifications. These vulnerabilities put sensitive production data privacy at risk and increase the likelihood of data breaches.

2. Software Patching (14%):

Many companies were still utilizing outdated software, such as versions of PHP and MongoDB that were no longer receiving security updates. These outdated systems provide significant risks and are vulnerable to known assaults.

3. Network Filtering (9%):

Samba and MySQL were two examples of open and unprotected network services that were found to be of serious concern. These services increase the risk of data theft or operational disruption since they allow unauthorized access to sensitive systems when they are not adequately safeguarded.

Risk Classification and Mitigation Prioritization

Based on asset value and severity, the 419 found vulnerabilities are grouped using the Risk Prioritization Matrix to provide a focused and effective remediation process. Based on this classification, manufacturing organizations may concentrate their cybersecurity efforts where they will have the greatest impact.

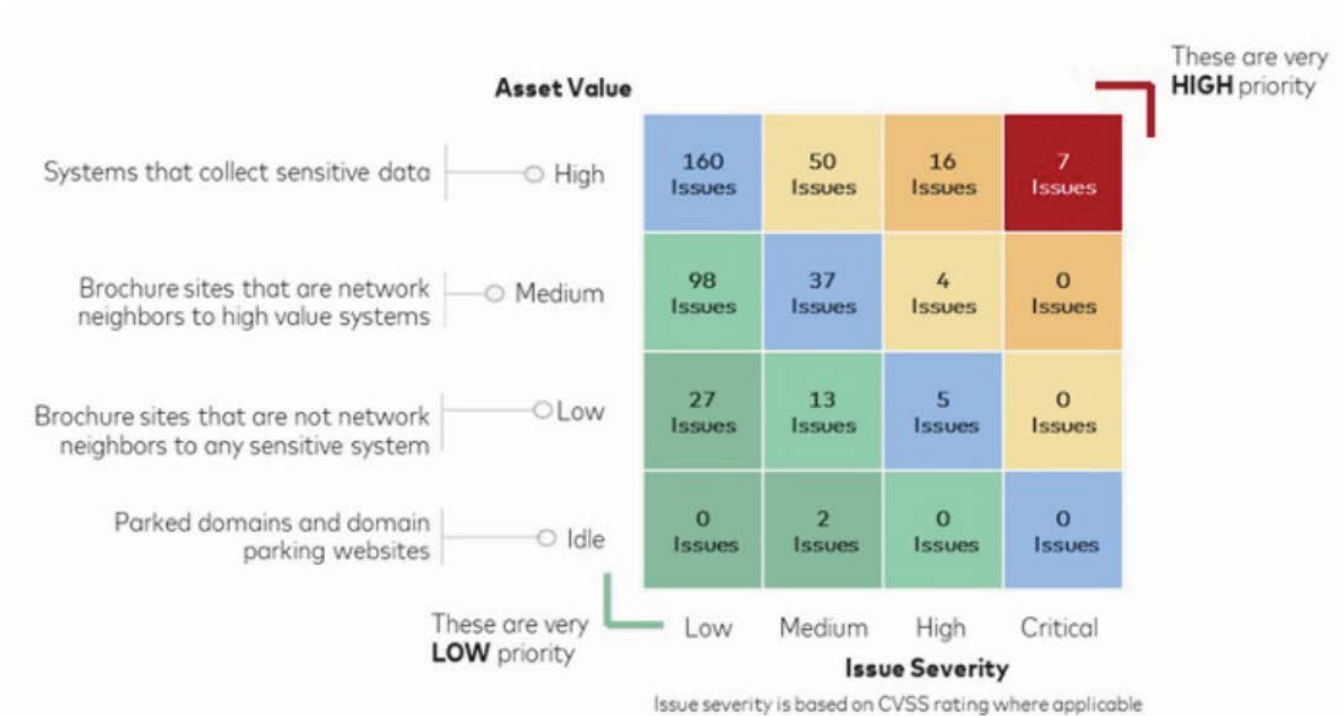


Exhibit 4.15 Indonesia's Manufacturing Sector Risk Prioritization Matrix, **Source:** Mastercard

Key findings from the matrix include:

- High-value systems that handle or store private manufacturing data have seven main problems.** Corrective action must be taken as soon as possible to avoid any operational interruptions or violations.

These systems directly handle sensitive data. These systems are susceptible to lateral movement attacks thus they must be addressed immediately to prevent unauthorized access to more crucial systems.
- Fifty high-severity issues were found in medium-value systems, which are critical assets' network neighbors, even though they do not directly handle sensitive data.** These systems are susceptible to lateral movement attacks thus they must be addressed immediately to prevent unauthorized access to more crucial systems.

Brochure sites and inactive domains with no imminent risk to vital activities were discovered to have low-priority concerns. In order to stop vulnerabilities from developing in the future, these systems still need to be observed.

Most of the problems are with software (PHP) that is getting close to the end of its life and contains known security vulnerabilities. The system exposes a network service (MySQL, MongoDB, Samba) to the internet that is not safe or appropriate to operate on the internet.



4.3 Recommendations Based on Sectoral Assessments

- 1. Maintain Persistent, Comprehensive Visibility**

Having a thorough understanding of the attack surface of your company is essential for the identification and mitigation of risks, especially those related to recognized vulnerabilities. This may be accomplished by consistently monitoring both standard and nonstandard ports while maintaining accurate fingerprints of the devices and services in your environment. This strategy will improve your capacity to recognize dangers and take preventative action.
- 2. Implement Real-Time Monitoring for Unsanctioned Services or Shadow IT**

Regular monitoring of the known perimeter assets will help distinguish between authorized assets and out-of-scope or shadow IT. The monitoring shall be further supported by common configuration baseline security on all systems. Assets not meeting these baselines are the highest risk for compromise and should be focused on for remediation.
- 3. Focus on High-Priority Vulnerabilities**

Prioritize remediation efforts on critical vulnerabilities, particularly internet-exposed ones with high severity and likelihood scores. Where necessary, Engage appropriate external experts to identify the critical areas for improvement and address them swiftly.
- 4. Remediate Critical Exposure Risks in Real-Time**

Finding internet-exposed risks due to misconfigurations and vulnerabilities is not good enough. An organization should have proper processes and technologies that empower the security operation teams to identify the service owners quickly, communicate the risk details, and track remediation progress in real-time.
- 5. Seek Expert Guidance**

Organizations new to Attack Surface Management (ASM) or wanting to advance their existing practices should consider external assessment. This would be achieved by collaborating with cybersecurity experts to identify significant vulnerabilities and thus create a custom roadmap for remediation.
- 6. Strengthen Remote Access Security**

Remote access remains among the key entry points for cyber threats. Stringent authentication protocols should be implemented for all remote access services, using multi-factor authentication (MFA) where appropriate. Monitoring systems should be installed to enable detection and response, even brute-force attempts, to unauthorized access.
- 7. Optimize Cloud Configurations**

Periodically review the cloud configuration against Industry Best Practices and perform updates to decrease the security risk. Encourage Security and Development teams to collaborate on developing secure cloud-native applications, including the correct setup and configuration of Cloud Resources for security.
- 8. Enforce Secure Data Handling Practices**

Establish and maintain strict access controls and secure file-sharing protocols regarding databases and shared resources. This will prevent unauthorized access, preserve data integrity, and support compliance with related regulatory frameworks, including data privacy laws.
- 9. Stay Informed About Emerging Threats**

Create a more formal process to stay abreast of emerging vulnerabilities, exploits, and threat actors. Due to the ever-evolving threat landscape, periodically reassess your organization's attack surface to ensure the efficiency of your security postures.
- 10. Adopt a Risk-Based Approach Aligned with Leading International Standards**

A risk-based approach, aligned with international standards like SNI/ISO/IEC 27001 and SOC2, is critical for building a resilient cybersecurity framework. Implement essential controls, such as:

 - Timely patching of applications and operating systems
 - Use of strong passwords and multi-factor authentication
 - Restricting administrative privileges
 - Application control
 - Regular backups
 - Protection against brute force credential attacks - such as lockouts after a maximum number of attempts

11. Drive Digital Transformation by Retiring Legacy Equipment

To counter growing threats, Indonesian companies need to proactively migrate from outdated cybersecurity solutions. They have to start by identifying which legacy system risks are critical for business operations and then rank those risks appropriately. Then continued by developing a detailed transition plan that includes data migration, integration, testing, and phased migration to modern solutions like cloud-based security and advanced threat detection systems. Furthermore, acquiring the required funds via grants, budgetary allotment, cost-benefit analysis, or cybersecurity insurance is also crucial. Afterwards, allocate funds for employee training to close skill gaps and ensure employees are knowledgeable about emerging technologies and incident response procedures. Continuous monitoring, vulnerability management, and a strong incident response plan are necessary for maintaining security.

Collaboration with stakeholders, vendor support, and a phased approach will facilitate a smooth transition and strengthen defenses against cyberattacks. Fully retiring the legacy system also can save environmental and financial costs. Several things should be considered when decommissioning legacy systems. Maintaining outdated systems up and running forever has security issues that can allow hackers to breach a company's firewall and expose its sensitive data to potential threats.¹⁰ There's also a chance that maintaining an outdated system may violate data privacy laws, which might result in fines, penalties, and other legal issues.¹¹

¹⁰ TJC Group. "Decommissioning Legacy Systems for Better Cybersecurity," July 26, 2024. <https://www.tjc-group.com/blogs/the-strategic-imperative-decommissioning-legacy-systems-for-better-cybersecurity/>.

¹¹ *Ibid.*



Chapter

05

Regulatory and Governance Framework

For Indonesia’s national cybersecurity measures to be successful, strong governance and regulations are essential. This chapter examines the current regulatory environment in Indonesia, providing suggestions for improvements, offering a framework for coordination, governance and ongoing monitoring across the sector.

5.1. Overview of Indonesia’s Current Cybersecurity Regulations

| Level | Regulation |
|---|---|
| Law/Act/Government Regulation in Lieu of Law | <ul style="list-style-type: none"> • Electronic Information and Transactions (EIT) Law No. 11 of 2008, Amended by Law No. 19 of 2016 • Personal Data Protection (PDP) Law No. 27 of 2022 • Criminal Code (KUHP) • National Police Law 2022, Amended in 2024 |
| Government Regulation | <ul style="list-style-type: none"> • Government Regulation No. 71 of 2019 |
| Presidential Regulation | <ul style="list-style-type: none"> • Presidential Regulation No. 82 of 2022 • Presidential Regulation No. 47 of 2023 |
| Specific Regulation | <ul style="list-style-type: none"> • BSSN Regulation No. 1 of 2024 • BSSN Regulation No. 2 of 2024 • BSSN Regulation No. 5 of 2024 |

Exhibit 5.1 Glimpse Hierarchy of Indonesian Cybersecurity Regulations

Indonesia has made considerable progress in establishing a national cybersecurity framework, enacting several laws and regulations to enhance cyber resilience across critical sectors. The following are vital regulations that form the foundation of Indonesia’s cybersecurity governance:

- Criminal Code (KUHP)**
 Cybercrime cases can be brought under the provisions of the Criminal Code (KUHP). However, there are difficulties in applying the KUHP to cybercrime cases because of its nature as general criminal regulation. Therefore, one of the main challenges is that the Criminal Code was not designed to address the special characteristics of cybercrime. Another challenge is that the status of the Criminal Code as a national law means that cybercrimes committed outside Indonesia cannot be prosecuted under the law, so this creates other difficulties.¹²
- Electronic Information and Transactions Law (EIT Law) No. 11 of 2008, Amended by Law No. 19 of 2016:)**
 This law controls E-Transactions, E-information, and cybercrime in Indonesia. It provides a legal framework to address cyber crimes and ensure integrity within electronic systems.¹³
- Government Regulation No. 71 of 2019**
 Provides for the implementation of electronic systems and transactions, including specific cybersecurity requirements to be implemented by all relevant parties operating within Indonesia’s jurisdiction, including the public and private sectors.¹⁴
- Personal Data Protection (PDP) Law No. 27 of 2022**
 The PDP Law harmonized Indonesia’s national data privacy law with internationally accepted best practices. This law demands explicit consent for access, correction, or deletion of personal data and provides strict penalties for disobedience.¹⁵
- Indonesia’s Presidential Regulation No. 82 of 2022**
 Strengthens cybersecurity by protecting Vital Information Infrastructure (VII) in critical sectors like Government and finance. It tasks the National Cyber and Crypto Agency (BSSN) with coordinat-

ing these efforts, assigning clear roles to stakeholders, and creating Computer Security Incident Response Teams (CSIRTs) at various levels to handle cyber threats.¹⁶

- **Formed a Unique Cross-Departmental Team in 2022**

In 2022, President Jokowi formed a unique cross-departmental team to investigate and handle data leaks. The team included representatives from the State Cyber and Crypto Agency (BSSN), the Ministry of Communications and Informatics, the Indonesian National Police (Polri), and the State Intelligence Agency (BIN).¹⁷

- **Presidential Regulation No. 47 of 2023**

This is the establishment of the National Cybersecurity Strategy and Framework for Cyber Crisis Management, which mentions governance structures, risk management protocols, and incident response procedures, all aimed at increasing the national cybersecurity resilience level.¹⁸

- **Regulation of the Deputy for Cybersecurity and Encryption (BSSN) in the Economic Sector No. 1 of 2023**

Deputy Regulation's primary objective is to establish a structured roadmap to develop and nurture Indonesia's local cybersecurity industry over the next five years (2024 -2028). This roadmap is planned to guide the Government, business sector, and other stakeholders in fostering the industry's growth and encouraging collaboration between the public and private sectors.¹⁹

- **Revision of Indonesian National Police Law in 2024**

This revision allows the police to slow down, block, and monitor cyberspace for national security purposes. The Law has been revised and authorized by the parliament. This consent was granted on Tuesday, 28 May 2024, during the 18th parliament plenary meeting for the 5th period of the 2023–2024 session year.²⁰

- **BSSN Regulation No. 1 of 2024**

This regulation focuses on incident management and crisis response, particularly for Vital Information Infrastructure Providers. It aims to provide a comprehensive framework, improve coordination or chain of command, and minimize the adverse impact of cyber incidents. This applies to Electronic System Operators (ESOs), Sectoral Computer Security Incident Response Teams (CSIRTs), and National CSIRT. There are several key provisions within this regulation including establishment of CSIRTs, incident reporting, incident response, and information sharing.²¹

- **BSSN Regulation No. 2 of 2024**

This regulation outlines the framework for cyber crisis management. There are three phases of crisis management which emphasized in the document which are pre crisis (cyber incident response, early warning, and contingency planning), crisis (declaration, management, and information dissemination), and post-crisis (recovery, evaluation, and lesson learned) through well-established procedure, coordinated action, and adequate preparedness.²²

- **BSSN Regulation No. 5 of 2024**

This regulation focuses on the establishment of a cybersecurity national action plan 2024-2028 which encompasses policy direction, challenges, strategic objectives, activities, indicator of success, achievement targets, roles and responsibilities as well as related institutions which should be involved. The national action plan itself outlines four priority projects which must be executed within a certain period of time such as establishment and enhancement of the cybersecurity response team; strengthening cybersecurity infrastructure, human resources and regulations; preventing cybercrime and increasing international cooperation; and solving the cybercrimes itself.²³

¹² Undang-undang (UU) Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Pemerintah Pusat. (2023)

¹³ Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Pemerintah Pusat. (2016)

¹⁴ Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pemerintah Pusat. (2019)

¹⁵ Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pemerintah Pusat. (2022)

¹⁶ Peraturan Presiden (Perpres) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Pemerintah Pusat. (2022)

Currently, the primary reference for Indonesia's cybersecurity regulatory framework is Presidential Regulation No. 47 of 2023. This regulation provides the basic guidelines for guiding the national cybersecurity Strategy and the framework for cyber crisis management, then explained further through BSSN Regulation No. 5 of 2024. This regulation outlines several key focus areas. These focus areas are as follows:

1. Governance
2. Risk Management
3. Preparedness and Resilience
4. Strengthening the Protection of Vital Information Infrastructure
5. National Cryptographic Independence
6. Enhancing Capability, Capacity, and Quality
7. Cybersecurity Policy
8. International Cooperation

Additional Regulations

Several other essential laws and regulations play a role in shaping Indonesia's cybersecurity landscape:

- **Law No. 3 of 2002 on National Defence**
- **Ministry of Defence (MOD) Regulation No. 82 of 2014 on Cyber Defense Guidelines**
- **Presidential Regulation Number 95 of 2018 on Electronic-Based Government System**
- **Ministry of Communication and Information (MOCI) Regulation No. 5 of 2020**
- **BSSN Regulation No. 10 of 2020 on Cyber Incident Response Team**
- **BSSN Regulation Number 4 of 2021 on Guidelines for Information Security Management of Electronic-Based Government Systems**
- **Indonesia Central Bank Regulation No. 23 of 2021 on Payment Service Providers**
- **OJK Regulation (POJK) No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks**
- **Law No. 7 of 1992 on Banking and OJK Regulation No. 22 of 2023**
- **Law No. 17 of 2023 on Health**
- **OJK Regulation No. 3 of 2024 on Organization of Financial Sector Technological Innovations Challenges and the Need for Continuous Improvement**
- **And others.**

¹⁷ Kementerian Komunikasi dan Informatika Republik Indonesia, "Presiden Instruksikan Jajarannya Tindaklanjuti Kebocoran Data Pemerintahan", Kementerian Komunikasi dan Informatika Republik Indonesia, September 14th, 2022, <https://www.kominfo.go.id/berita/berita-pemerintahan/detail/presiden-instruksikan-jajarannya-tindak-lanjuti-dugaan-kebocoran-data-pemerintah>

¹⁸ Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Pemerintah Pusat. (2023)

¹⁹ Peraturan Deputi Bidang Keamanan Siber dan Sandi Perekonomian Nomor 1 Tahun 2023 tentang Peta Jalan Pembinaan Industri Keamanan Siber Tahun 2024-2028, BSSN. (2023)

²⁰ Sari, Amelia Rahima, "Revisi UU Polri Bikin Polisi Bisa Awasi Ruang Siber hingga Blokir Internet, Pengamat: Jadi Dilema", Tempo.co, May 30th, 2024, <https://nasional.tempo.co/read/1873786/revisi-uu-polri-bikin-polisi-bisa-awasi-ruang-siber-hingga-blokir-internet-pengamat-jadi-dilema>

²¹ Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber, BSSN. (2024)

²² Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber, BSSN. (2024)

²³ Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 Tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028, BSSN. (2024)

Regulatory Gap

The Need to Have Unified Regulation: Cybersecurity Law

Although Indonesia has several regulations which serve as the foundation for the cybersecurity landscape, the country remains scrappy, lacking substantial depth, and clarity in terms of a solid regulatory framework.²⁴

There is a need to create and enforce unified cybersecurity law which is reflected through how the current parliament still has an ongoing discussion about cybersecurity and resilience although it has stalled since 2019. The cybersecurity and resilience law is expected to have more depth on cybersecurity threats, protection of critical infrastructure, data, information, and cybersecurity talent. The lack of unified and solid cybersecurity law also posed an adverse impact towards the private sector where most companies should adhere with complex yet different laws that are handled by different stakeholders.

The absence of a clear and overarching cybersecurity law and strategy creates ambiguity and overlaps in authority among government agencies. The complex compliance bureaucracy could hinder the potential economic value and investment opportunities. Other than that, the presence of regulation is also expected to further create good governance in cybersecurity while also encouraging public-private partnership to facilitate collaboration in strengthening cybersecurity and improving local cybersecurity talents.²⁵

Lack of Coordinated Authority and Oversight and Divergent Threat Perceptions

The lack of a central coordinating agency manifests in the limited authority given to the cybersecurity agency. Due to its lack of legal authority, the cybersecurity agency cannot position itself as a leading body in cybersecurity governance, creating gaps between sectors in terms of regulation and enforcement.²⁶

While awareness of cyberattacks is on the rise, stakeholders in Indonesia hold diverging views on the nature and severity of cyber threats. This discrepancy leads to inconsistencies in risk assessment and mitigation strategies, undermining a unified approach to national cybersecurity defense.²⁷

Severe Underfunding and Resource Limitations

The cybersecurity agency and other cybersecurity units face chronic underfunding and lack the necessary human capital to respond effectively to cyber threats. This resource deficit limits their capacity to combat evolving cyber risks and proactively protect critical infrastructure and sensitive data.²⁸

²⁴ Dr. Kartina Sury, "Indonesia's Cyber Resilience: At the Epicenter of ASEAN Digital Economy Growth" Tech for Good Institute, May 13th, 2024. <https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/>.

²⁵ Raihan Zahirah & Theo Gerald, "Digitalisasi, Teknologi, dan Inovasi" in *Visi dan Peta Jalan Indonesia Emas 2045 Milik Pemuda*, ed. Reza Edriawan et al. (Jakarta: Indonesian Youth Diplomacy, 2024) 84, https://iyd.or.id/wp-content/uploads/2024/09/05092024_IYD_Report_All-Content.pdf

²⁶ Gatra Priyandita, "Indonesia's Cybersecurity Woes: Reflections for the Next Government", CSIS, CSISCOM00624 (2024): 2-6, <https://csis.or.id/publication/indonesias-cybersecurity-woes-reflections-for-the-next-government/>

²⁷ *Ibid.*

²⁸ *Ibid.*

5.2. Proposed Regulatory Enhancements

Due to the increasingly complex nature of the cyber threat landscape, Indonesia's regulatory framework must be continually updated to close regulatory gaps and achieve cyber resilience. Therefore, we will discuss several important recommendations for regulatory improvement in this section.

5.2.1 Alignment with International Best Practices

The main action that must be taken to achieve cyber resilience is harmonizing national regulation with international standards. Harmonizing the regulation will encourage international cooperation, increase competitiveness, and provide strong protection for organizations and individuals. Therefore, harmonization of cyber laws with existing frameworks, such as the European Union's General Data Protection Regulation (GDPR), will be beneficial for cybersecurity governance and the digital economy in Indonesia.

Benefit of Aligning with International Best Practices

- **Global Standard for Data Protection**
The GDPR serves as a global benchmark in data protection, emphasizing transparency of information flow, consent of users, and tight security measures regarding personal information. Compliance with these types of regulations thus may go on to further develop Indonesia's cybersecurity framework in ways that will help foster public confidence in digital services while improving their defenses against cyber threats.
- **Improving Trust and Confidence**
Strict regulations that protect personal information will increase public and company confidence in national data security that will lead to better utilization of digital services and more economic activity in the digital economy.
- **Facilitating International Trade and Commerce**
Harmonizing data protection laws like GDPR will enable Indonesian businesses to conduct seamless activities with the international market. More importantly, since cross-border data flows underpin most of the global commerce and collaboration that happens today, a lack of harmonization will only raise the risks to which businesses are exposed.
- **Attracting Foreign Investment**
Strong data privacy regulations that comply with international standards will increase Indonesia's recognition as a secure and reliable business environment. This may attract more foreign investment, especially from companies that want to operate data-driven businesses in technology, finance, and e-commerce.

Strategic Path to Alignment

The international best practices in the Laws of Indonesia could be aligned by considering the following steps:

- 1. Incorporate Key GDPR Principles into Indonesian Legislation**
Several important GDPR principles, such as openness, user consent, data minimization, rights of access, correction and deletion, must be implemented by the Indonesian government and make these important principles the basis for the regulatory framework.
- 2. Establish Data Protection Authorities (DPAs)**
Give the DPAs the resources and enforcement powers to ensure that the new privacy regulation is adhered to. DPAs should be able to investigate data breaches, impose penalties, and give businesses guidance on data protection matters. The cybersecurity agency may adopt this DPA role.
- 3. Encourage International Data Transfers**
We should develop mechanisms aligning with global standards to facilitate international data transfers. This may be by adopting Binding Corporate Rules (BCRs) or even joining international agreements on data privacy and protection so Indonesian businesses are fully involved in the global digital economy.
- 4. Continuous Monitoring and Updates**
For privacy regulations to keep up with changing global standards and new advances in technological development, they must be regularly evaluated and updated. Indonesia will benefit from increased competitiveness and ease of adaptation to changes in international regulations.

5. Risk-Based Approach

Governments should implement risk-based laws and regulations and align them with existing regulations to prevent contention and fragmentation. This key action will provide a safe yet creative technology environment. This methodology recognizes that not all systems require the maximum level of security and instead advocates proportion-

ality and flexibility in responding to specific settings and risk profiles. Regulations can efficiently protect society and promote economic progress by striking a balance between risk management and the need to support technical progress, and by prioritizing existing international standards over those that have not yet been created.

5.2.2 Regularly Review Cyber, Data, and Privacy Laws

Indonesia needs to do regular and ongoing examinations of the law, and this will be necessary to ensure that the national data, privacy, and cyber law framework is up to date and functional in the face of evolving technological environments, shifting cyber threat landscapes, and rising social expectations. Technological innovation gives rise to new threats and weaknesses. Therefore, the legal framework must be updated regularly to protect society, the business world, and national security. Outdated laws may seriously weaken defenses against data breaches, privacy violations, and cybercrime. The existence of a regulatory gap could jeopardize the legitimacy of the public for stronger protection and transparency. To address this regulatory gap, the Government must regularly update the legislation to ensure that the legal basis and standards remain effective, responsive, and relevant in addressing the complex modern challenges and keep it aligned with international best practices.

Critical Areas for Legislative Review

1. Data Breach Notification Laws and Penalties

One critical review area is data breach notification laws and their associated penalties. Indonesia must ensure the penalties for non-compliance are significant and severe enough to incentivize good cybersecurity practices, which are critical in preserving trust and accountability in the digital world.

Study Case:

Australia's **Notifiable Data Breaches Act** introduced a maximum of AUD 2 million for severe breaches as a penalty, but this penalty was much less than it would have cost organizations in Australia to implement appropriate cybersecurity measures. However, after significant breaches, the Australian Government introduced the **Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022**, allowing increased maximum penalties to the greater of AUD 50 million, three times the value of any benefit obtained through misuse of information or 30% of the company's adjusted turnover during the relevant period. This legislative amendment ensures that penalties reflect the severity of data breaches and that consumer protection is of paramount interest.

Focus for Indonesia:

- Review and improve **data breach notification laws** to ensure timely reporting of cyber incidents by private organizations, including non-Critical Information Infrastructure (non-CII) operators.

- Ensure penalties for severe or repeated data breaches reflect public expectations, foster trust, and ensure accountability.

2. Incident Reporting Framework

The existing incident reporting framework should also put an obligation on all private organizations in the critical sectors to report cyber incidents promptly to the national Computer Security Incident Response Team (CSIRT), not just public or critical infrastructure operators. This would further enhance the national incident response and increase transparency at all levels.

3. Legislation on Emerging Technologies and Vulnerable Populations

The legislation will move toward the specific risks from emerging technologies, such as artificial intelligence (AI), blockchain, and the Internet of Things (IoT), that are integral to digital ecosystems. Additionally, we should improve online protection legislation for children, consumer, and intellectual property, where this should be reviewed regularly to ensure its compatibility with evolving international standards and for the safe adoption of new technologies.

Recommendations for the Legislative Review Process:

1. Adopt a Continuous Review Cycle

Create a regular cycle for examining and amending cyber, data, and privacy regulations in order to stay responsive to changing threats, technological advancements, and public expectations.

2. Consultation with Stakeholders

Engage a wide range of stakeholders, including the private sector, civil society, organizations, and international experts, in a review of the legal framework to ensure that the legislative update follows best global practices while reacting to sector-specific difficulties.

3. Benchmarking Against International Standards

Conduct regular benchmarking of Indonesian laws against global frameworks such as the GDPR, NIST, and other international standards to ensure compliance with global data protection rules and cross-border collaboration.

5.2.3 Ensuring Effective Compliance Monitoring Across Sectors

- **Enforce Mandatory Incident Reporting and Regular Audits:**

The cybersecurity agency or certified third-party auditors may undertake recurring cybersecurity audits and assessments of organizations, especially those in important industries. These audits assess if regulations are being followed, find weak points, and suggest fixes.²⁹

- **Impose Sanctions for Non-Compliance:**

The cybersecurity agency and sectoral regulators have the power to apply administrative consequences, such as warnings, fines, and license suspensions should there be any violation towards cybersecurity regulations. These penalties serve as a disincentive and motivate businesses to give cybersecurity a priority.³⁰

- **Promote Public Disclosure:**

To promote awareness and better practices

across industries, the cybersecurity agency may occasionally make information regarding cybersecurity incidents or non-compliance publicly available.

- **Facilitate Threat Intelligence Sharing:**

The cybersecurity agency will create channels for exchanging cybersecurity best practices and threat intelligence across many industries and stakeholders so companies can keep up with new threats and proactively strengthen their cybersecurity system.

- **Deploy Automated Monitoring and Detection Tools**

Automated technologies can be used by sectoral authorities and the cybersecurity agency to track network traffic, spot anomalies, and quickly identify possible cyber threats.

5.2.4 Enhancing ICT Supply Chain Security in Government Procurement

ICT hardware and software are the core component yet foundational backbone for Indonesia's national and economic cybersecurity. This underpins the critical infrastructure, comprising energy grids, telecommunications networks, healthcare systems, and defense platforms. The era of growing digitization and global interconnectivity has significantly increased the risks related to cyberattacks on ICT supply chains. Compromises in these supply chains can provide adversaries with undetected access to networks or systems, posing severe threats to national security and sovereignty.

²⁹ Hukumonline, "Strengthening the National Cybersecurity Ecosystem: Unveiling New BSSN Frameworks on Cyber Incidents and Cyber-Crisis Management" hukumonline.com, 868 (2024), <https://pro.hukumonline.com/alt66165fd50830/strengthening-the-national-cybersecurity-ecosystem--unveiling-new-bssn-frameworks-on-cyber-incidents-and-cyber-crisis-management>.

³⁰ Denny Rahmansyah, "Data Protection and Cybersecurity in Indonesia: Enforcement and Litigation", SSEK, December 12th, 2019, <https://www.ssek.com/blog/data-protection-and-cybersecurity-in-indonesia-enforcement-and-litigation/>

Rising Threat of ICT Supply Chain Attacks

Cyber attackers are increasingly targeting hardware and software development activities. By embedding malicious code or vulnerabilities (often referred to as “backdoors”). They exploit this vulnerability for espionage, sabotage, or other malicious activities. This threat is posed as a critical issue in the defense and national security sectors that might disrupt critical activities, where software plays a critical role in data analytics, intelligence operations, and security functions.

Prominent and high-profile incidents such as the SolarWinds attack (also known as SolarStorm) and NotPetya (a devastating cyber attack on Ukraine in 2017) have brought attention to the growing sophistication and impact of supply chain threats. These attacks have accelerated efforts around the world to intensify their cyber defense by identifying and mitigating risks within their ICT supply chains.

Procurement Policies to Emphasize Cybersecurity and Supply Chain Integrity

Government procurement officials, especially those tasked with technology purchases, have to consider more than the economic value a product is given. The procurement must be carried out with consideration of cybersecurity and supply chain integrity to ensure national security. Appropriate procurement rules and policies can be done by stating clearly that government agencies are responsible for ensuring cybersecurity and supply chain risks during procurement while ensuring economic value.

Key areas to consider when updating procurement policies include:

- **Product Security and Integrity**

Government procurement processes should require technology vendors to demonstrate adherence to secure development practices, including supply chain risk management. This should be treated as a prerequisite before allowing the vendors to participate in the next stage of procurement processes.

- **Non-Financial Benefits**

Beyond cost, procurement of the technology should account for the security of the product and the vendor’s exposure to supply chain risks.

- **Global Best Practices**

Indonesia can take the US Executive Order on ICT supply chain security from March 2021 that requires US government agencies to purchase only software that was created by secure development standards. These standards lead the government agencies to acquire adequate information from the vendors of the software for informed, risk-based decisions about the security of the merchandise under purchase.

Strategic Recommendations for Government Procurement

- **Adopt Secure Development Standards**

Procurement policy should be aligned with international best practices, such as the US Executive Order on secure software development, to ensure that all government software purchases meet strict cybersecurity standards.

- **Require Vendor Transparency**

In the procurement process, require vendors to provide information on their product integrity practices, including compliance with frameworks like **NIST’s Secure Software Development** and secure supply chain standards.

- **Incorporate Cybersecurity into Procurement Policies**

Improving government procurement policies to explicitly emphasize the importance of cybersecurity and supply chain security in order to ensure all purchased ICT products meet stringent security standards.

- **Conduct Regular Audits and Assessments**

Implement continuous audits and assessments to ensure security in the software development lifecycle of vendors, right from development to the deployment phase.

5.2.5 Government Policies Emphasize the Procurement of Commercial Off the Shelf (COTS) Products

The term Commercial off-the-shelf (COTS) products refers to the software or hardware solutions that are available in the commercial marketplace which are designed specifically tailored to fulfill predetermined needs. COTS products offer standardized functionality that can be swiftly deployed to all users.. In government procurement, especially in cybersecurity, COTS solutions allow agencies to seamlessly adopt established technologies without the delays and expenses associated with developing custom systems.

Advantages of COTS Solutions

- COTS products are supported by **high vendor R&D efforts**, ensuring that these solutions remain relevant with the latest technological innovation.
- It is critical to allocate the government's finite cybersecurity resources efficiently. COTS solutions procurement will enable the government to gain **resource efficiency** by directing its cybersecurity personnel to focus on essential functions, such as protecting critical infrastructure, rather than building and maintaining custom-built systems.
- COTS solutions help address the **global challenges** of the shortage of skilled cybersecurity professionals by reducing the need for internal development expertise. Government agencies can focus their skilled staff on high-impact cybersecurity tasks, leaving routine system updates and maintenance to external vendors.

5.3. Enhance the Governance Model and Institutional Roles

To guarantee an efficient cybersecurity management throughout Indonesia, a well-defined and well-coordinated cybersecurity governance framework is essential. In this section, we outline the necessary steps to improve the governance model of national cybersecurity architecture and define the roles of key institutions involved.

Elevate Cyber Security to the Highest Levels of Government

The President of Indonesia should have direct control for cybersecurity in Indonesia, and it should be brought to the highest echelons of government. This strategic move acknowledges the reality that cybersecurity is no longer merely a technical issue but a national security priority affecting critical infrastructure, economic stability, and public safety.

Key Actions:

- **Appoint a Special Advisor to the President on Cybersecurity**
This role will ensure cybersecurity is integrated into all aspects of national strategy, offering professional advice to the government, facilitating interagency cooperation, and fostering international partnerships to enhance national strategy.
- **Make Cybersecurity a Top Agenda Item**
Elevating the cybersecurity agenda as a major focus will facilitate better coordination, resource allocation, and policy implementation to address evolving cyber threats.

Prioritize and Increase Funding for Cybersecurity Uplift in Government

There is a need for the government to step up and demonstrate its commitment in safeguarding sensitive data and critical national functions by significantly increasing expenditure on national cybersecurity is crucial to protect and defend government systems from sophisticated cyber threats.

Key Actions:

- **Increase Budget for Cybersecurity Initiatives**
Invest more for education in talent development, public awareness campaigns, and modernizing cybersecurity infrastructure.
- **Allocate Resources for Critical Functions**
Prioritize securing payment processes, national security systems, and defense platforms against cyber threats.



Review Organizational Cyber Roles and Responsibilities

To ensure effective cybersecurity, organizations need to clearly define who is responsible for online security within their structure while ensuring that the leadership, board of directors, and financial officers understand the importance of cyber risk management.

Key Actions:

- **Establish Clear Cybersecurity Accountability:** Every organization should have a Chief Information Security Officer (CISO) or equivalent role, directly reporting to the CEO or Head of the organization, to manage cyber risks effectively.
- **Separate CISO from CIO Functions:** The CISO should not be the same person as the Chief Information Officer (CIO) or Chief Operating Officer (COO) to avoid conflicts of interest between data accessibility and data security priorities.
- **Launch Cyber Security Review Board:** Encourage public-private collaboration and open information sharing on incidents and investigations to strengthen overall cybersecurity resilience. Board members can consist of telecommunication companies, technology companies, the Attorney General, and law enforcement bodies.

Define Government Policy and Operational Roles, and Responsibilities

To enhance Indonesia's national cybersecurity framework, there is a need for a clear role of the cybersecurity agency and ID-SIRTII (National CSIRT); they are key in defending Indonesia from cyber threats, responding to incidents, and fostering international cooperation. The following actions are crucial to improve their capabilities:

Key Actions:

- **Conduct comprehensive reviews and regular updates** of internal policies to ensure roles, responsibilities, and operations are aligned with evolving cybersecurity threats and best practices.
- **Conduct frequent cybersecurity drills** to test coordination and response capabilities, ensuring readiness for real-world incidents, financial resilience, and seamless stakeholder collaboration.
- **Invest in the ongoing training for all staff levels** with clear metrics to measure the effectiveness of these programs, ensuring skills and knowledge stay sharp to handle complex cyber threats.
- **Develop tracking tools and analyze** key cybersecurity metrics, including incident response times and threat management efficiency. Regular evaluations will help make informed decisions and optimize resources.
- **Strengthen the technical capabilities** of cybersecurity agency and ID-SIRTII in threat intelligence, digital forensics, and international operations. This should be supported by legislation that expands their roles and functions.
- **Ensure proper allocation** of human, financial, and technological resources, along with updated awareness programs, to keep pace with emerging threats and trends.

5.3.1 Role of Indonesian Chamber of Commerce and Industry (Kadin) in Cybersecurity Governance

As the Indonesian government's strategic partner, the Indonesian Chamber of Commerce and Industry (Kadin) can play a role as a bridge between the private and government sectors in shaping the national cybersecurity agenda. Through its extensive network, Kadin could align business interests with national security objectives, ensuring the private sector actively participates in building a strong cybersecurity ecosystem. The approach will help Indonesia to create consistent cybersecurity policies, harmonize its cybersecurity policies across industries, and support broader national objectives, including protection of critical infrastructure and digital transformation.

Key Roles of Kadin



Exhibit 5.2 Key Roles of Kadin

1. Public-Private Partnership (PPP) Leader

Kadin will lead the development of a structured Public-Private Partnership (PPP) model that facilitates and incentivizes businesses to participate actively in cybersecurity initiatives. The collaboration with the government would enable Kadin to facilitate information sharing, cyber incident coordination, and policy discussions. Such a model has been successfully implemented in other ASEAN countries like Singapore, where they enable business and government collaboration under the Cybersecurity Act of 2018 to enhance critical infrastructure protection.

2. Cybersecurity Awareness and Advocacy

Kadin will drive industry-wide cybersecurity awareness campaigns focusing on fostering a security-first culture within the business community. Kadin can encourage and promote internationally recognized best practices such as SNI/ISO/IEC 27001 and the well-known NIST Cybersecurity Framework. This helps Indonesian businesses align with global standards. Additionally, Kadin can advocate for better cyber regulations by facilitating continuous dialogue between business leaders and policymakers.

3. Cybersecurity Talent Development Collaborator

A major challenge for Indonesia is the shortage of skilled cybersecurity professionals. Kadin's initiatives will initiate the collaboration effort with educational institutions, training centers, and cybersecurity agency to create a pipeline of

cybersecurity talent. Then facilitate the internships, apprenticeships, and certification programs that integrate real-world industry needs with academic training. In addition, Kadin can foster collaboration with global tech companies to bring world-class expertise to Indonesia.

4. Standards and Regulatory Compliance Facilitator

Kadin should help businesses navigate the increasingly complex regulatory environment around cybersecurity by providing the resources they need to meet both national and international cybersecurity standards. This facilitator role includes offering guidance on data privacy laws (such as Indonesia's Personal Data Protection Law), cybersecurity risk assessments, and audit frameworks. Imagine Kadin creating an online platform where businesses can access information on complying with cybersecurity laws, conduct self-assessments, and even get advice from cybersecurity experts.

5. Incident Response and Crisis Management Coordinator

Given the extensive network and influence of Kadin, it can play a central role in coordinating responses to sophisticated cyber incidents. By acting as an intermediary between businesses and government cybersecurity bodies (like cybersecurity agency and CSIRT), ensuring a faster and more effective response to incidents.

By taking on these roles, Kadin can significantly strengthen Indonesia's cybersecurity, build trust between the private sector and the government, and ensure that businesses actively contribute to national cybersecurity resilience. This is not only important for protecting businesses but also for strengthening Indonesia's digital economy against cyber threats.

5.3.2 Role of the Cybersecurity Agency

The cybersecurity agency plays a role as the primary authority in developing and implementing Indonesia's cybersecurity governance. The agency plays a very crucial role in developing a cohesive framework that ensures the integrity, security, and resilience of the nation's digital infrastructure. The mandate of the cybersecurity agency includes capacity building, regulatory enforcement, coordination of incident response, and facilitating public-private sector collaboration.

Strategic Roles of Cybersecurity Agency in Cybersecurity Governance



Exhibit 5.3 Key Roles of Cybersecurity Agency

1. Lead Architect of National Cybersecurity Policy

The cybersecurity agency should also lead the development and continually update Indonesia's national cybersecurity initiatives. This will involve aligning the national framework with international best practices and standards, including but not limited to ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), the Risk Management Framework (RMF), and other relevant cybersecurity and privacy frameworks. The agency's primary objective is to make Indonesia's cybersecurity policies adaptive to the new emerging threats and comprehensive in its approach to deal with risks from all sectors.

2. Coordinator of National Incident Response

As the central entity for cybersecurity crisis management, the cybersecurity agency must establish a comprehensive, nationwide incident response framework. This will involve managing the establishment and coordination of sectoral Computer Security Incident Response Teams (CSIRTs) and integrating these into a national CSIRT. It should be implemented centrally to ensure good communication and utilization of resources in cases of cyber security incidents, especially those regarding critical infrastructure sectors. Also, consider forming a public - private advisory or consultation board to get advice from a broad set of stakeholders. Hitherto, cybersecurity agency has ID-SIRTII

which stands for Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center which responsible for improving the whole Indonesia's cybersecurity landscape, assisting both public and private sector in providing security system, conducting series of works (early monitoring, detection, and warning), managing laboratory facilities, supporting law enforcement, acting as the central point of contact for the domestic and international cybersecurity initiatives as well as carrying out research and development initiatives.³¹

3. Regulator and Enforcer of Cybersecurity Compliance

The cybersecurity agency is responsible for the implementation of national regulations in the field of cybersecurity across industries, including the enforcement of the Personal Data Protection (PDP) Law and other relevant cybersecurity laws. Regular audits, vulnerability assessments, and compliance checks are necessary to ensure adherence to these standards, especially in sectors critical to national security and economic stability.

4. Capacity Builder for National Cybersecurity Talent

In addressing the national need to develop a robust workforce for cybersecurity, the agency must take a leading role through coordination with relevant educational institutions, industry players, and international partners. This includes designing cyber education via formal and informal avenues. This involves creating training programs, certification pathways, and awareness on cybersecurity for capability development in the public-private sector.

5. Facilitator of Public-Private Collaboration

The cybersecurity agency plays a pivotal role in fostering collaboration between the public and private sectors. The cybersecurity agency needs to facilitate knowledge sharing, best practice dissemination, and coordination of collective cybersecurity defenses through formalized partnerships.

6. Promoter of Cybersecurity Innovation and Technology Adoption

The cybersecurity agency should actively encourage active adoption and the promotion of innovation in cybersecurity with advanced technologies within the national cybersecurity ecosystem. The cybersecurity agency also must be involved in encouraging collaboration between technology providers, academia, and research institutions to ensure that the cybersecurity agency drives the creation of solutions to suit Indonesia's needs. It also needs to protect personnel and infrastructure with cutting-edge technologies like artificial intelligence; save the most important resources, such as AI and the models, training data, and real-time learning that it depends on; exchange knowledge and skills to safeguard the AI technologies that keep everyone safe.³² The cybersecurity agency and the overall country's systems must prioritize security by implementing technologies that adhere to best practices. This can be achieved through three key recommendations: procuring secure-by-design systems and products, ensuring security considerations are central to the procurement process, and mitigating concentration risk to avoid over-reliance on single vendors or technologies.³³ By embracing these recommendations, governments can strengthen their defenses against cyber threats and safeguard sensitive information.

These roles will solidify the cybersecurity agency position as the leading authority for cybersecurity governance in Indonesia. Its leadership will ensure a structured system to maintain compliance and effectively handle incidents, and at the same time will enable various stakeholders both from the public and private sectors to further develop a resilient and secure digital ecosystem. By focusing on developing skilled professionals, encouraging innovation, and collaborating internationally, the cybersecurity agency will help establish Indonesia as a key player in global cybersecurity.

³¹ ID-SIRTII, "History Id-SIRTII/CC", ID-SIRTII, <https://www.idsirtii.or.id/en/page/history-id-sirtii-cc.html>

³² Google, "How AI Can Reverse the Defender's Dilemma", Secure Empower Advance, February (2024):12, <https://services.google.com/fh/files/misc/how-ai-can-reverse-defenders-dilemma.pdf>

³³ Royal Hansen & Christoph Kern, "Tackling cybersecurity vulnerabilities through Secure by Design", Google, March 4th, 2024, <https://blog.google/technology/safety-security/tackling-cybersecurity-vulnerabilities-through-secure-by-design/>

5.3.3 Establishing Self Regulatory Organization (SRO) for Critical Sectors

To bolster Indonesia's cybersecurity against rising threats, creating industry-led Self-Regulatory Organizations (SROs) is crucial to develop and enforce cybersecurity standards and best practices within a specific sector. These organizations would set industry-specific frameworks and guidelines, promoting knowledge sharing and collaboration, monitoring compliance with established standards, facilitating incident response and information sharing about cyber threats, and advocating for cybersecurity interests within their sector through training and educational resources. Establishing a successful SRO in Indonesia can pose us to several potential challenges, primarily in building trust and cooperation among diverse stakeholders, securing adequate resources like funding, personnel, and technology for effective operation, and striking the right balance between self-regulation and government oversight. However, these challenges can be effectively addressed through strong partnerships and a shared commitment to cybersecurity from all stakeholders, paving the way for a robust and resilient SRO in Indonesia.

As we are facing the plethora of cyber threats targeting critical infrastructure, businesses, and individuals, establishing SROs for cybersecurity in Indonesia would be significantly beneficial to strengthen the nation's cybersecurity posture. An SRO can strengthen the nation's overall cybersecurity posture by tailoring standards and best practices to the unique needs of each critical and non-critical sector. Furthermore, an SRO can facilitate crucial collaboration and information sharing among stakeholders, including government agencies, businesses, and cybersecurity experts, while also drawing upon international best practices for optimal implementation. An SRO can play a pivotal role in driving the growth and development of the cybersecurity industry in Indonesia while also contributing to a safer and more secure digital environment for all. It can facilitate collaboration and knowledge sharing through networking, information exchange, and joint research initiatives that can foster innovation and growth while also accelerating the development of new cybersecurity solutions. Furthermore, an SRO can advocate for supportive policies and promote the industry domestically and internationally to potential investors,

so it can boost trust and confidence. In addition, it can also provide incubation and mentorship for emerging and local cybersecurity businesses by helping them to grow and succeed, also enhancing their credibility and marketability. This contributes to stronger growth for cybersecurity businesses in the country.

There are few examples of SRO that have existed in some countries. For instance, Indonesia itself has specific SRO within the financial industry, which are the Indonesia Stock Exchange, Indonesian Securities Underwriting Clearing (KPEI), and Indonesian Central Securities Depository (KSEI). Similarly, the United States also has the New York Stock Exchange (NYSE) and Financial Industry Regulatory Authority (FINRA), which also serve as SRO. Another example specifically related to cybersecurity would be the United States, where both the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Information Sharing and Analysis Center for the Electricity Subsector (E-ISAC) in the US exemplify the SRO model, with the former focusing on cybersecurity within the financial sector and the latter dedicated to protecting the electricity sector. The Institute of Nuclear Power Operations (INPO) in the US focuses on safety and reliability in the nuclear sector, demonstrating an SRO dedicated to critical infrastructure. The UK's Advertising Standards Authority (ASA) tackles online safety and misleading content, showcasing an SRO addressing broader trust issues within its sector. Another example would be that Canada's CRTC collaborates with broadcasting and telecommunications providers to implement security measures, illustrating a model where a government agency partners with industry to achieve SRO-like outcomes. Finally, the European Telecommunications Standards Institute (ETSI) develops globally applicable cybersecurity standards, playing a crucial role in setting baseline security requirements. These varied examples offer valuable insights for Indonesia as it considers which SRO model best suits its unique needs and priorities, highlighting the potential for sector-specific approaches, public-private partnerships, and the development of both broad and targeted cybersecurity standards. These organizations highlight the sector-specific approach that SROs can adopt to address unique cybersecurity challenges.

5.3.4 Industry Self Regulation (ISR) for Non-Critical Sectors

Instead of strict regulations, Industry Self-Regulation (ISR) in cybersecurity empowers businesses within the non-critical sector to proactively enhance their collective cybersecurity posture through voluntary collaboration, information sharing, and the development of tailored standards and best practices. This approach is particularly beneficial for non-critical sectors in Indonesia, allowing for tailored solutions that address each sector's unique challenges and reduces the burden of following one-size-fits-all rules. Furthermore, ISR can enhance industry reputation, build trust with customers, and establish a minimum cybersecurity baseline across the sector, preventing vulnerabilities caused by uneven security practices. To foster successful ISR in non-critical sectors, Indonesia can encourage industry associations to lead the development of cybersecurity standards while the government provides support, resources, and incentives for participation. Promoting awareness and collaboration among businesses is crucial, and learning from international best practices can offer valuable guidance. While challenges like ensuring widespread participation and consistent enforcement exist, a strong commitment from all stakeholders can enable effective ISR implementation, ultimately strengthening Indonesia's overall cybersecurity resilience.

Industry Self-Regulation (ISR) is used in many different ways across the globe. For instance, the Direct Selling Association Consumer Code in the United Kingdom which focuses on setting the ethical standards for consumer protection. Similarly, in New Zealand, the Advertising Standards Authority Advertising Codes of Practice ensures responsible advertising across all media.³⁴ In Denmark, the Framework

Agreement for Mobile Content and Payment Services safeguards consumer interests in mobile content and payments.³⁵ Other examples include the Entertainment Software Rating Board in the United States, which provides age and content ratings for video games. In addition, the Electricity and Gas Complaints Commission in New Zealand, resolves consumer complaints in the energy sector.³⁶ Furthermore, initiatives like the Code of Marketing of Food and Non-alcoholic Beverages to Children in Mexico and the Children's Food and Beverage Advertising Initiative in the United States demonstrate ISR's role in promoting responsible food marketing to children.³⁷ These examples underline how ISR can be implemented across various sectors for a wide range of purposes starting from to protect consumers, ensure fair practices, and promote ethical standards, offering valuable insights for strengthening cybersecurity in Indonesia's non-critical sectors.

For this to be successful and impactful, self-regulation initiatives must be carefully designed, adopted broadly, and monitored effectively to ensure compliance and demonstrable results. To build trust and accountability, independent verification is key.³⁸ Furthermore, self-regulation requires continuous adaptation and improvement through ongoing monitoring, evaluation, and adaptation to remain relevant and effective in achieving its desired outcomes. These takeaways underscore the importance of designing and implementing self-regulation initiatives carefully, with a focus on transparency, accountability, and demonstrable results. There is also a need for collaboration among industry players, regulators, and independent verifiers to ensure that self-regulation truly serves its intended purpose.

³⁴ OECD, "Industry self regulation", OECD Digital Economy Papers, 247 (2015): 40-63, <https://doi.org/10.1787/5js4k1fjqkwh-en>.

³⁵ *Ibid.*

³⁶ *Ibid.*

³⁷ *Ibid.*

³⁸ Martha Lagace, "Industry Self-Regulation: What's Working (and What's Not)?", Harvard Business School, April 9th, 2007, <https://hbswk.hbs.edu/item/industry-self-regulation-whats-working-and-whats-not>

5.3.5 Setting up a Cybersecurity Security Operations Center (SOC)

Security Operations Centers (SOCs) are fundamental for monitoring, detecting, and responding to security incidents. This section outlines the strategic approach to establishing Indonesia’s SOC and sector-specific SOC, ensuring strong cybersecurity across Indonesia’s critical sectors. A Security Operations Center (SOC) is a centralized facility for continuously monitoring an organization’s digital infrastructure to detect and respond to cybersecurity threats. An SOC performs the functions of real-time monitoring, rapid incident response, and forensic analysis after the incident.

Responsibilities of National SOC

| National SOC | | | |
|--------------------------------|-----------------------------|-------------------------------|-------------------------------|
| Incident Response Coordination | Threat Intelligence Sharing | Proactive Security Approaches | Policy and Regulation Support |

Exhibit 5.4 Responsibilities of National SOC

1. Incident Response Coordination:

- **Acts as the main point of contact** for cybersecurity incidents nationwide.
- **Leads the response to major incidents**, from detection, analysis, containment, eradication, and recovery.
- **Works with organizations and international partners** to manage and mitigate the impact of cyber incidents.

2. Threat Intelligence Sharing:

- **Collects, analyzes, and shares** threat information to stakeholders.
- **Facilitate the exchange of threat intelligence** between government, critical infrastructure, and the private sector.

3. Proactive Security Approaches:

- **Identify and manage vulnerabilities** within national critical infrastructure.
- **Conduct regular cybersecurity awareness campaigns and training** programs to strengthen the cybersecurity posture of organizations and the public.

4. Policy and Regulation Support:

- **Advise policymakers** on cybersecurity matters and support the development of relevant policies and regulations.
- **Ensure Indonesian organizations comply** with all international and national cybersecurity laws and standards.

Importance of CSIRT/SOC

Having a Computer Security Incident Response Team (CSIRT) or Security Operations Center (SOC) is really important for Indonesia's cybersecurity because:

- **Enhanced Cyber Resilience:** By providing a coordinated and efficient response to cyber incidents, CSIRTs and SOCs enhance the overall resilience of the country's critical infrastructure and digital assets.
- **Improved Situational Awareness:** Continuous monitoring and threat intelligence sharing improve situational awareness, enabling proactive measures to mitigate potential threats before they materialize.
- **Public Trust and Confidence:** Effective incident response and transparent communication during cyber crises build public confidence in the nation's ability to protect its digital environment.
- **International Collaboration:** Both CSIRTs and SOCs facilitate international collaboration in cybersecurity, contributing to the worldwide efforts to combat cyber threats.

Establishment of Sectoral SOCs

Concept of Sectoral SOCs:

- **Each sector (finance, energy, healthcare, etc.)** should establish its own SOC for industry-specific threat intelligence and response, possessing specialized knowledge about their technologies and regulations.

Coordination with the National SOC:

- **Information Flow:** Sectoral SOCs should maintain continuous communication with the national SOC, ensuring coordinated efforts.
- **Unified Response:** Sectoral SOCs should maintain continuous communication with the national SOC, ensuring coordinated efforts.

Phased Approach to Implementing a National SOC for Government Agencies

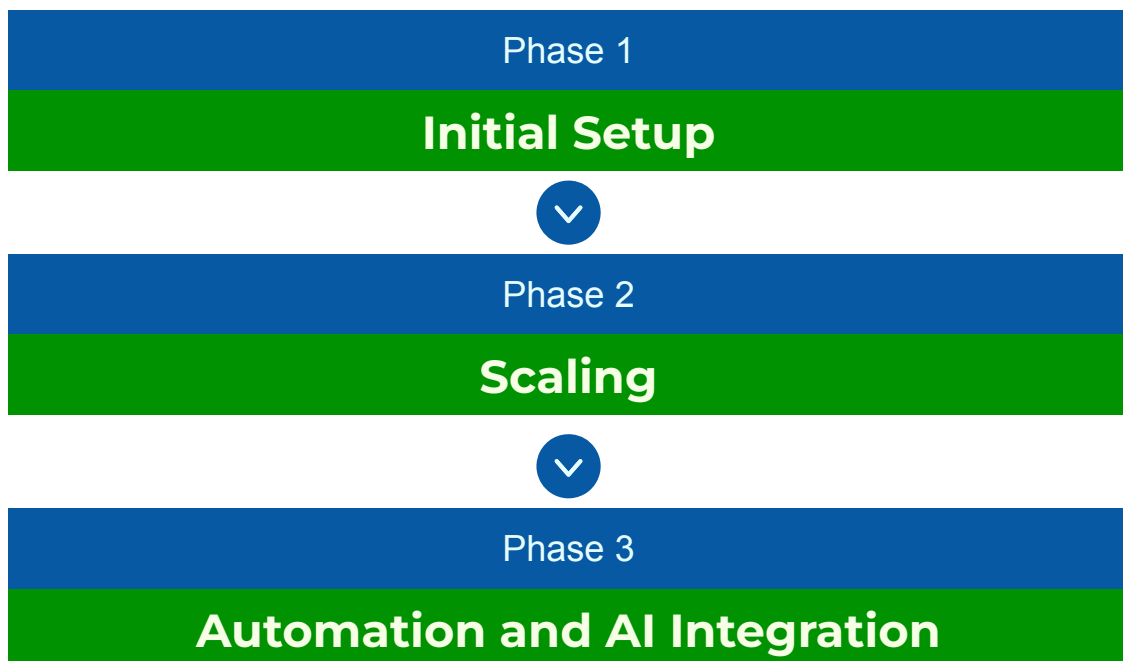


Exhibit 5.5 Phased implementation approach of national SOC



Phase 1: Initial Setup

- **Core Agencies:** Begin with key agencies like cyber-security agency and ID-SIRTII to establish a central hub for detecting and responding to threats.
- **Data Sources:** Deploy tools like endpoint detection and response (EDR) and firewalls to collect the data needed for analysis.

Phase 2: Scaling

- **Extend to Critical Sectors:** Expand the SOC's capabilities to cover important sectors like finance, healthcare, and energy.

- **Implement Sector-Specific SOCs:** Develop SOCs for each sector, which report back to the national SOC.

Phase 3: Automation and AI Integration

- **Embrace Advanced Technologies:** Incorporate AI and automation to boost the SOC's ability to quickly detect and respond to threats.
- **Improve Efficiency:** Automation will reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), threat detection and response times, making the SOC more efficient overall.

Encourage Uptake of AI-Driven, Automated Security Tools in SOCs

Incorporating AI-driven automation in SOCs is essential for addressing the inefficiencies of manual security processes, which often result in delayed responses and missed vulnerabilities.

Key Benefits of AI-Driven SOCs:

- **Reduced Overwhelming Alert Volumes:** AI-driven SOCs can process massive amounts of security events daily, distilling them into a manageable number of actionable alerts that require human analysis.
- **Faster Incident Response:** AI tools have been proven to reduce Mean Time to Respond (MTTR) from days to under two hours, significantly enhancing threat containment speed.
- **Resource Optimization:** By automating low-level alerts, AI enables cybersecurity professionals to focus on critical, sophisticated threats, increasing incident closure rates and expanding the amount of security data analyzed daily.

Proven Results:

- **Reduction of Response Time:** From 2–3 days to under 2 hours.
- **Increased Incident Closure Rate:** By five times.
- **Expanded Security Data Analysis:** By four times.

Policy Recommendations:

- **Incentivize AI Adoption:** Provide incentives, such as tax breaks or subsidies, for organizations adopting AI-driven SOC tools.
- **Set Performance Standards:** Require organizations to include MTTD and MTTR in their cybersecurity strategies to promote faster threat resolution.

Adopting AI-driven automation will significantly improve the efficiency and resilience of Indonesia's SOCs, enabling faster detection, better resource allocation, and a stronger overall cybersecurity framework.

5.3.6 SOC Intervention Criteria

This outlines when Indonesia's national SOC (Security Operations Center) should step in to handle cybersecurity incidents, and how they would provide support.

1. National SOC Intervention Scenarios::

- **State-Sponsored Attacks:**
Incidents involving attackers with state-level capabilities and interests.
- **Cross-Sectoral/Pandemic Events:**
Large-scale incidents affecting multiple sectors or resembling a cyber pandemic.
- **Critical Infrastructure Attacks:**
Incidents targeting entities defined as national critical infrastructure.

2. Coordination and Support:

- **Resource Allocation:**
The national SOC will allocate resources and expertise to support affected entities.
- **Incident Command:**
Establish an incident command structure to coordinate response efforts across sectors.
- **Information Sharing:**
Facilitate real-time information sharing between affected entities and relevant stakeholders to ensure a unified and cohesive response



Chapter

06

Public-Private Partnerships & Industry Collaboration

6.1 Developing a National Public-Private Partnership Program

Building a resilient and collaborative cybersecurity ecosystem requires strong partnerships between the public and private sectors. A structured multi-tiered cyber public-private partnership (PPP) program is essential to Indonesia’s national cybersecurity resilience. This program will facilitate formal engagement between the government and industry stakeholders, ensuring aligned cybersecurity strategies, timely threat intelligence sharing, and strengthened coordinated responses to cyber incidents.

Multi-Tiered Engagement Structures

The Indonesian government should establish multi-tiered engagement structures that categorize industry partners based on their cybersecurity sophistication and relationship with the government. This approach ensures targeted communication and appropriate engagement aligned with each organization’s capabilities and role.

Industry Partners Category

| | Unidirectional Communication (Tier 1) | Bidirectional Communication (Tier 2) |
|-------------------------------|---|---|
| Organizational Types | Small and medium-sized enterprises (SMEs). | Sophisticated organizations in critical infrastructure, technology, and cybersecurity sectors. |
| Focus | Receiving tailored threat intelligence and guidance from the government. | Two-way communication for sharing and receiving threat intelligence. |
| Purpose | Provide actionable information to bolster cybersecurity defenses, acknowledging that these organizations may lack resources to contribute significantly to threat intelligence. | Contribute valuable insights to the government, enhancing the national threat intelligence landscape, and receive detailed technical threat data aligned with their response capabilities. |
| Tailored Communication | <p>Provide detailed explanations of threat significance and potential impacts.</p> <p>Offer concrete steps to mitigate vulnerabilities, ensuring guidance is accessible and actionable.</p> | <p>Deliver granular data and actionable intelligence suited to their advanced capabilities.</p> <p>Encourage contributions that enrich the government’s understanding of the evolving threat landscape.</p> |

Outcomes of the Multi-Tiered Public-Private Partnership (PPP) Program

By creating a partnership program with different levels of engagement for various organizations, Indonesia can achieve the following:

- **Enhanced Threat Intelligence Sharing:**
Enables timely sharing of actionable threat intelligence and vital information between the government and private sector, allowing everyone to be prepared.
- **Strategic Alignment:**
Creates a unified national cybersecurity strategy by aligning efforts across sectors, reducing fragmentation and duplication.
- **Support for National Awareness Initiatives:**
Amplifies national cybersecurity awareness campaigns, ensuring businesses of all sizes understand the threats they face and the necessary actions to take.

6.2 Developing a Real-Time Threat Intelligence Sharing Platform

An effective framework for cyber threat intelligence sharing is essential for detecting, deterring, and responding to cyber threats in real time. Since the government and private businesses each have unique knowledge about these threats, combining their insights gives Indonesia a complete picture and strengthens its defenses.

Key Features of the Threat Intelligence Sharing Platform

1. Real-Time Intelligence Sharing

- Facilitates rapid and quick sharing of threat intelligence, enabling swift responses to emerging threats.
- Provides customized guidance suited to the needs of different organizations, from large enterprises to SMEs.

2. Bi-Directional Flow of Information

- Encourages both government and private sector entities to share insights, ensuring a two-way exchange of information.
- Allows SMEs to benefit from the advanced threat intelligence contributed by larger organizations.

- Both the government and private businesses share what they know, creating a complete understanding of the threat landscape

3. Collaborative Response Options

- Enables members to collaborate on response strategies and share best practices.
- Strengthens collective response capabilities and improves incident management across industries.

Benefits of the Threat Intelligence Sharing Platform

- **Faster Detection and Response:**
Equips organizations to detect and respond to threats more effectively, reducing the time between vulnerability identification and mitigation.
- **Broader Participation:**
Engages organizations of all sizes, ensuring that even smaller businesses benefit from high-quality threat intelligence.
- **Enhanced Cybersecurity Resilience:**
Fosters collaboration and real-time intelligence sharing, improving Indonesia's overall cybersecurity posture.

6.3 Establish a Cyber Incident Review Board or Similar Forum

As part of the Public-Private Partnership (PPP) Program, Indonesia should establish a Cyber Incident Review Board to enhance its ability to analyze and learn from major cyber incidents. This board, composed of government officials and trusted industry experts in cybersecurity and incident response, is responsible for:

1. Reviewing major cyber events

- **Detailed Analysis:**

Conduct comprehensive evaluations of significant incidents, including causes, impacts, and contributing factors.

- **Lessons Learned:**

Identify incidents and recommend measures to prevent recurrence.

2. Offering concrete recommendations:

- **Improvement Strategies:**

Provide actionable recommendations for enhancements across the public and private sectors.

- **Policy Development:**

Inform national cybersecurity policies and practices with insights from incident analyses.

By establishing this formal incident review forum, it will enable Indonesia to enhance its cybersecurity posture and foster stronger collaboration between government agencies and private sector partners, thereby strengthening the strategic response to ensure a safer digital environment.

6.4 Strengthening International Collaboration in Cybersecurity

In order to tackle the growing complexity and transnational character of cyber threats, Indonesia acknowledges the crucial need for international collaboration in cybersecurity. To improve its cybersecurity posture, Indonesia should actively participate in alliances and cooperative projects with other nations and international organizations.

Regionally, Indonesia is committed to further bolstering the role of regional organizations in the cybersecurity landscape through Confidence Building Measure (CBMs) and the development of regional capacity.³⁹ An important part of ASEAN's cybersecurity efforts is Indonesia's participation in the ASEAN Regional Forum (ARF), ASEAN Political-Security Community, ASEAN Cyber Capacity Program (ACCP), ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC), and the ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC). These programs put a strong emphasis on member

state capacity building, incident response, and information sharing. Furthermore, Indonesia is also actively involved in Asia-Pacific Economic Cooperation to fight cybercrime and contribute to building international norms on cybersecurity.⁴⁰

Globally, Indonesia is dedicated to promoting peace and strengthening the development of cyber norms.⁴¹ Indonesia has actively participated in UN Security Council, UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace, UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, International Telecommunication Union (ITU), United Nations Office on Drugs and Crime (UNODC), Organization of Islamic Cooperation (OIC), Global Commission on the Stability of Cyberspace (GCSC), and G20.⁴²

Bilaterally, Indonesia cooperates and collaborates on the cybersecurity landscape with the European Union, Australia, the United States, China, Japan, South Korea, etc. The scope of cooperation encompasses security dialogue, workshops, incident management, cybercrime investigations, capacity building programs, cybersecurity strategy, joint exercises, cyber defense capabilities, information sharing, combating cybercrime, protecting critical infrastructure, and promoting cyber norms.

³⁹ MoFA Indonesia, "Indonesia Voices Cyber Stability in the UN", MoFA ID, May 23rd, 2020, <https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un>

⁴⁰ IISS, "Indonesia", *Cyber Capabilities and National Power: A Net Assessment*, (2021): 143-147, <https://www.iiss.org/globalassets/media-library---content-migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---indonesia.pdf>

⁴¹ MoFA Indonesia, "Indonesia Voices Cyber Stability in the UN", MoFA ID, May 23rd, 2020, <https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un>

⁴² *Ibid.*

Several areas that can be explored for future collaborations would be:

- **Information sharing mechanism** to facilitate early warning of cyber threats, exchange threat intelligence, and improve incident response capabilities
- **Joint exercise** to improve coordination, test incident response plans, and building practical skills in handling cyberattacks
- **Capacity building** through training programs, scholarships, exchange programs, knowledge transfer, mentorships, workshops, and knowledge sharing to develop local expertise in cybersecurity, incident response, and digital forensics
- Promote and encourage the development of **cyber norms and responsible state** behavior in cyberspace

Key diplomatic agenda items that should be prioritized:

- **Promoting Cyber Norms:**
In order to promote responsible state behavior and avert cyber conflict, Indonesia must emphasize the significance of creating and upholding international cyber rules, thereby encouraging the peaceful resolution of conflicts and supporting the application of international law to cyberspace.
- **Enhancing International Cooperation:**
Indonesia should actively and closely work to enhance global cybersecurity cooperation through information exchange, cooperative training, and capacity building to highlight the necessity of working together to combat the transnational nature.
- **Bridging the Digital Divide:**
Indonesia has to emphasize how critical it is to close the digital gap, provide equal access to technology, and help developing nations strengthen their cybersecurity capabilities to promote international assistance to improve less developed countries' cybersecurity capacities.
- **Protecting Critical Infrastructure:**
Indonesia needs to emphasize how important it is for nations to work together to defend vital infrastructure against cyberattacks to encourage the exchange of best practices and the creation of global guidelines for the defense of vital infrastructure.
- **Involving Non-State Diplomatic Actors:**
As the global issue is getting complex, it is important for Indonesia to also have substantial and practical leadership in international forums. To support this, Indonesia needs to harmonize the involvement of non-state diplomatic actors that have expertise in the cybersecurity landscape, such as think tanks and the private sector.⁴³ This ensures a more comprehensive and inclusive approach to cybersecurity diplomacy, incorporating diverse perspectives and expertise. Non-state actors possess specialized knowledge and innovative solutions that can contribute significantly to addressing cyber threats. Indonesia can explore this avenue by creating a specific cybersecurity working group or task force that can be managed under the Ministry of Foreign Affairs.

⁴³ Abdurrahman Al-Fatih Ifdal & Kenzie Sultan Ryvantya, "Ketangguhan Diplomasi Internasional" in *Visi dan Peta Jalan Indonesia Emas 2045 Milik Pemuda*, ed. Reza Edriawan et al. (Jakarta: Indonesian Youth Diplomacy, 2024) 58, https://iyd.or.id/wp-content/uploads/2024/09/05092024_IYD_Report_All-Content.pdf



Chapter

07

Cybersecurity Education and Talent Development



Indonesia must address its cybersecurity awareness and talent shortage through comprehensive education reform, professional certification programs, and practical training initiatives. This means promoting certifications, launching national awareness campaigns, and creating hands-on learning opportunities to bridge the gap in cybersecurity knowledge and skills. Developing a skilled workforce is crucial to protect the country's critical infrastructure from cyber threats. By investing in cybersecurity, supporting government initiatives, and improving digital literacy, Indonesia can reduce its losses from cybercrime by IDR 1,365 trillion by 2030.⁴⁴

The cybersecurity agency and Kadin (Indonesian Chamber of Commerce and Industry) will lead these efforts, ensuring that cybersecurity education and awareness reach everyone. By partnering with the private sector, industry groups, and schools, Indonesia can build a strong cybersecurity foundation.

7.1. Current Challenges in Cybersecurity Talent and Awareness

The world is facing a growing shortage of cybersecurity experts. Indonesia is also facing a significant shortage of cybersecurity professionals and a general lack of awareness about cybersecurity best practices. These gaps hinder the nation's ability to effectively respond to cyber threats and adopt cybersecurity measures across industries.

Key challenges include:

- **Cybersecurity Professional Shortage:**
Indonesia faces a cybersecurity professional shortage, especially in critical sectors like finance, healthcare, and energy.
- **Limited Awareness and Training:**
A significant portion of the general workforce, particularly in SMEs, lacks basic cybersecurity awareness, which increases the risk of human error leading to cyber incidents.
- **Lack of Formal Cybersecurity Education Programs:**
Most universities and technical schools in Indonesia do not yet offer comprehensive degree programs or training pathways dedicated to cybersecurity.

To solve this, both the public and private sectors need to invest in training and supporting these professionals. It's also important to maximize the effectiveness of the existing cybersecurity workforce. Building a robust pipeline of skilled professionals, including those from unconventional backgrounds, will benefit the entire cybersecurity ecosystem. Governments should prioritize recruiting diverse talent and reconsider traditional hiring criteria, such as rigid degree requirements and certifications, which often exclude capable individuals like hackers, veterans, and those from underrepresented groups. Addressing challenges like cybersecurity knowledge and talent gaps in Indonesia requires a multi-faceted strategy focused on educational reform, professional certification, and continuous learning. Such an effort has to be performed comprehensively through collaboration between government, private sector, and educational institutions in building a skilled cybersecurity workforce.

⁴⁴ Access Partnership, "Google's role in helping Indonesia build a safe and productive society through digital tools", Economic Impact Report, October (2023): 5, <https://cdn.accesspartnership.com/wp-content/uploads/2023/10/ID-EN-FA-OnScn.pdf?hsCtaTracking=be48563c-9c59-4f6c-9b6e-65c517502ef5%7C087a5bf8-c39f-4fb3-9c18-2aaf7af92354>

7.2 Designating a Lead Agency for Cyber Education and Awareness

Indonesia needs a multi-pronged approach to raise cybersecurity awareness and knowledge across all levels of society. A critical step towards enhancing Indonesia's national cybersecurity framework is to designate a central authority responsible for coordinating, developing, and delivering cybersecurity awareness programs. This lead agency, ideally the cybersecurity agency) or the national **CSIRT (or another designated body)**, would be the key driver of all cyber education and awareness efforts, working across both the public and private sectors. The designated agency would have several strategic responsibilities to ensure effective nationwide engagement and alignment across stakeholders.

Key Responsibilities of the Lead Agency



Exhibit 7.1 Key Responsibilities of the Lead Agency

1. Coordinate and Develop Awareness Programs

- **Stakeholder Engagement:**

Collaborate with public institutions, private businesses, critical infrastructure providers, and academia to create comprehensive awareness programs.

- **Tailored Content:**

Design programs that address both general and sector-specific cybersecurity threats, tailored to Indonesia's diverse industries.

2. Establish a Centralized Online Portal

- **Primary Platform:**

Create and maintain a centralized online portal consolidating all relevant cybersecurity information and resources.

Portal Features:

- **Audience Segmentation:**

Provide information tailored to different audiences, from SMEs to large corporations and critical infrastructure operators.

- **Timely Updates:**

Provide up-to-date best practices, threat alerts, and practical guidance

- **Resource Library:**

Include training materials like video tutorials, toolkits, and self-assessment tools.

This platform would be distinct from a broader threat information-sharing portal and would serve the specific purpose of public education and cyber resilience awareness.



3. Launch a Whole-of-Nation Cybersecurity Education Campaign

- **Collaborative Effort:**

The Indonesian government partners with leading industry associations such as USABC and Kadin to launch a national cybersecurity awareness campaign. This initiative will be pivotal in educating the broader public on how to protect themselves against cybercrime, with messaging tailored to all levels of society.

- **Campaign Scope:**

- **National Messaging:**

Develop messaging that resonates with everyone from business executives to students.

- **Multiple Channels:**

Utilize social media, television, and radio to ensure broad reach.

- **Educational Content:**

Cover basic cybersecurity hygiene, including phishing detection, data safeguarding, and secure communication practices.

- **Targeted Audiences:**

- **Business Leaders:**

Ensure top-level awareness and investment in cybersecurity.

- **Employees:**

Instill daily cybersecurity practices across the workforce.

- **Students and Young Professionals:**

Foster the next generation of cybersecurity experts.

4. Implement Evaluation Metrics for Awareness Programs

- **Performance Indicators:**

Establish clear metrics to assess the effectiveness of awareness campaigns, such as participation rates and reductions in incidents linked to poor awareness.

- **Continuous Improvement:**

Use evaluation data to refine content and distribution methods, keeping programs responsive to the dynamic cyber landscape.

5. Develop Executive-Level Awareness Programs

- **Tailored Training:**

Create specialized programs for executive managers in both the public and private sectors, focusing on the unique cyber risks their organizations face and the strategic countermeasures required.

- **Special Focus:**

Address the financial, operational, and reputational impacts of cybersecurity incidents, enabling executives to make informed decisions on investments and policies.

6. Coordinate Existing Awareness Campaigns

- **Strategic Alignment:**

Align and coordinate existing cybersecurity awareness initiatives to avoid duplication, maximize resource utilization, and present a unified and consistent national message.

- **Regular Communication:**

Facilitate ongoing dialogue between stakeholders running these campaigns to ensure consistency and reinforce key messages.

7.3 Comprehensive Cyber Security Employee Training

To combat the ever-changing cyber threats, every organization in Indonesia needs to prioritize cybersecurity training for all employees. While many businesses have incorporated cybersecurity into their training programs, there is a need for a more unified, mandatory approach, especially within government institutions and state-owned enterprises.

Key Recommendations for an Effective Cybersecurity Training Program

1. Inclusive Training for All Business Areas

Cybersecurity training should be mandatory for all employees, from entry-level staff to senior executives and CFOs. This ensures everyone understands the risks and can act as the first line of defense.

2. Incentivize Positive Security Behavior

Instead of solely penalizing mistakes, organizations should reward employees for reporting phishing attempts and other cyber threats. Positive reinforcement encourages vigilance and proactive engagement, fostering a security-conscious culture.

3. Tailor Training Based on Behavior Analysis

To improve the effectiveness of training, organizations should analyze why employees engage with phishing emails or other security threats. This analysis should move beyond simple metrics like “click-through rates” and delve into behavioral factors such as the content or urgency of the email. Tailored training that addresses the root causes of risky behavior will be far more effective in fostering strong cybersecurity practices.

4. Provide Specialized Training for Executives and CFOs

Executives and CFOs must receive specialized training that addresses their unique roles in

shaping an organization’s cybersecurity strategy and investments. This training should ensure they are aware of the financial and operational risks posed by cyber threats, enabling informed decision-making regarding cybersecurity expenditure and strategic initiatives.

5. Foster a Culture of Security

Building a culture where employees feel safe reporting cybersecurity incidents or mistakes is critical to an organization’s defense posture. Encouraging openness and continuous learning reduces the likelihood of repeated errors and strengthens the organization’s ability to adapt to new threats. A culture that prioritizes security from the top down fosters a sense of shared responsibility across the workforce.

6. Develop a Comprehensive Cyber Strategy

Cybersecurity strategies must acknowledge the inevitability of human error and include preventive measures and real-time threat responses, leveraging automation where possible. Organizations should maintain a clear understanding of their cybersecurity posture from the perspective of potential adversaries, ensuring that their defenses evolve in response to changing threats.

By implementing these recommendations, government institutions and businesses across Indonesia will significantly enhance their cybersecurity posture. Extensive employee training programs that engage all levels of the workforce—from frontline staff to senior executives—will help organizations mitigate risks more effectively. This holistic approach to cybersecurity training not only strengthens defenses but also cultivates a culture that prioritizes security at every level, which is fundamental for sustaining organizational and national cyber resilience.

7.4 Growing Cybersecurity Talent in Indonesia

Addressing the shortage of cybersecurity professionals is crucial for Indonesia’s national security and digital economy. A comprehensive strategy spanning all education levels is required to develop a robust pipeline of skilled professionals. This talent pipeline will support both the public and private sectors, ensuring the country has the expertise needed to counter evolving cyber threats.

Key recommendations for growing Indonesia's cybersecurity talent:

1. Align Government Entities on Shared Objectives

The cybersecurity agency, the Ministry of Education, and other relevant entities should collaborate to define clear cybersecurity education priorities. This will ensure a unified national approach and efficient use of resources.

Actionable Initiatives:

- Develop a **national cybersecurity education roadmap** as part of the National Cybersecurity Strategy (NCSS).
- Ensure that a **dedicated national budget** is allocated to fund cybersecurity education initiatives, infrastructure development, and talent programs across all education levels.

2. Implement Comprehensive Cyber Education

To ensure that Indonesia can meet its growing need for cybersecurity professionals, **cybersecurity education** must be integrated across **primary, secondary, and tertiary** education levels. This includes creating specialized cybersecurity courses and embedding cybersecurity content within existing **ICT** and **STEM** curricula. Early exposure cultivates interest and foundational knowledge, while advanced programs at universities develop specialized skills.

Actionable Initiatives:

- **Teacher Training:**
Provide educators with training and resources to deliver current and industry-relevant cybersecurity courses
- **Curriculum Expansion:**
Embed cybersecurity modules across various university programs, including non-technical fields like law and business, to promote cross-disciplinary expertise.
- **Public Access and Informal Education:**
Support seminars, MOOCs, mentorship, workshops, and lectures on cybersecurity topics accessible to non-specialists, fostering widespread awareness.
- **Cyber Clinics:**
The cyber clinics offer a valuable opportunity to address the cybersecurity skills gap. By providing hands-on experience for students while assisting under resourced organizations, they strengthen

the overall security posture of local communities. Furthermore, innovative training programs leveraging technologies like generative AI can personalize the learning experience and efficiently expand the pool of qualified cybersecurity professionals.

● **Cyber Year of Service:**

To bolster the cybersecurity workforce, we need both broader and deeper expertise. Mandating standardized cybersecurity content in all computer science programs through certification requirements can significantly increase baseline knowledge. Furthermore, initiatives like a "Cyber Year of Service" can provide valuable experience and a direct pathway to government cybersecurity roles for graduates. These diverse training avenues, coupled with equipping professionals with advanced tools like AI and leveraging cloud-based security solutions, will maximize their effectiveness and efficiency in combating cyber threats.

Further Developments:

- Regularly review and update the IT and cybersecurity content taught in schools and universities to align with current best practices.
- Allocate additional funding to public universities to expand their cybersecurity infrastructure, including labs and technical facilities, ensuring they are equipped to meet the demands of increasing enrollment in cybersecurity courses.

3. Incentivize ICT and STEM Courses

Encouraging students to pursue **ICT and STEM** fields is key to fostering a steady flow of talent into the cybersecurity workforce. Providing **financial incentives** like grants and scholarships, can make these programs more attractive and accessible to a broader range of students. Additionally, we also need to provide financial incentives for institutions and educators to promote and enhance ICT and cybersecurity education.

4. Develop Cyber Internships and Apprenticeship Programs

Providing hands-on learning opportunities through **internships and apprenticeship** programs is critical to bridging the gap between academic education and practical cybersecurity experience. These programs allow students and professionals to gain real-world experience in cybersecurity, improving their skills and employability.

Actionable Initiatives:

Partner with the private sector to offer internships and apprenticeships, providing hands-on experience that bridges academic learning and practical application.

5. Promote Micro-credentials in Cybersecurity

Encourage the development and recognition of short, focused qualifications in areas like cloud security and incident response. Micro-credentials allow professionals to upskill rapidly and specialize according to industry needs.

Actionable Initiatives:

- Promote micro-credentials that focus on emerging areas such as cloud security, threat intelligence, incident response, and forensic analysis.
- Collaborate with industry leaders to ensure Micro-credential programs are relevant and meet current cybersecurity demands.

6. Enhance Diversity and Inclusion

A diverse cybersecurity workforce is essential for bringing different perspectives and skills to the table. Programs aimed at increasing diversity, particularly in underrepresented groups, are key to building an inclusive cybersecurity talent pipeline.

Key Recommendations:

- Develop mentorship programs and outreach initiatives targeting underrepresented groups in

cybersecurity, including women, minorities, and those from disadvantaged backgrounds.

- Create partnerships with organizations that promote diversity in STEM fields to increase participation from all segments of society in cybersecurity roles.

7. Host a National Cyber Challenge

Organize Capture the Flag (CTF) competitions and other cybersecurity challenges to engage students and professionals. These events stimulate interest, encourage skill development, and identify promising talent.

Actionable Initiatives:

- Collaborate with universities, Kadin, and international organizations to provide sponsorships and prizes, enhancing participation.
- Establish pathways from competition participation to internships and employment opportunities within the cybersecurity sector.

8. Cybersecurity Talent Retention Strategy

Retaining skilled cybersecurity professionals is crucial. Their expertise grows with time, making them invaluable assets. Cultivating a supportive environment where they feel empowered to question, innovate, and adapt ensures job satisfaction and encourages long-term commitment to the organization.

7.5 Career Path and Occupation Mapping for Cybersecurity Talents

To further grow the cybersecurity talents and create labor market symmetry, there is a need for the public and private sector to have a synergy in terms of how to properly channel these talents into the right occupation through proper career path and occupation mapping. In 2019, BSSN partnered with Kadin, Ministry of Manpower, Ministry of Communication and Informatics, Ministry of National Development Planning, and BNSP launched “National Occupational Map in the Indonesian National Qualification Framework in the Area of Cybersecurity Function” that outlines cybersecurity job roles, skills, competencies, and career paths while also serves as the guidelines for individuals, educational institutions, and private sectors. The purpose of this document is also to provide standardization, skills development, career planning, workforce development, and industry growth. There are approximately 30 occupations and four key components for each occupation such as job roles, competencies, career path, and certification or training which are already synchronized with Indonesian National Work Competency Standards (SKKNI) (see appendix N).⁴⁵

7.6 Certification Programs and Standards

In the context of Indonesia’s evolving cybersecurity landscape, certification and standards play a critical role in ensuring that both professionals and organizations are equipped to meet the growing demands for cybersecurity resilience. This chapter will detail the professional and organizational certification programs necessary to foster a robust cybersecurity environment, building on existing initiatives from the cybersecurity agency, MOCI, and Kadin while incorporating best practices from global frameworks.

7.6.1 Professional Certification Programs

To ensure that Indonesia develops a skilled and certified cybersecurity workforce capable of addressing complex threats across sectors. Professional certification programs will focus on closing the cybersecurity skills gap by providing globally recognized credentials and practical expertise.

Existing Certification Landscape:

- **Cybersecurity Competency Certification:**
In collaboration with the **Indonesian Certification Body**, it currently offers professional certifications that address specific competencies, such as network security and incident management.
- **MOCI's Digital Literacy and Cybersecurity Training:**
MOCI has initiated several programs aimed at enhancing digital skills and cybersecurity awareness among professionals across industries, focusing on areas such as data privacy, cloud security, and threat detection.

Role of Kadin:

Kadin (the Indonesian Chamber of Commerce and Industry) is planning to expand and introduce cybersecurity certification programs for professionals in collaboration with the **cybersecurity agency, MOCI**, and international certification bodies. Kadin will act as the key facilitator, working to ensure that certification programs are aligned with industry needs and cover the latest technologies.

Key Focus Areas:

- **Expansion of Certification Programs:**
Offer a wide range of certifications like CompTIA Security+, CISSP, and CEH, and collaborate with international bodies such as ISC2 and ISACA to offer certifications tailored to Indonesia's specific needs. Focus on high-demand areas like incident response, penetration testing, cloud security, and critical infrastructure protection.
- **Cybersecurity Talent Pipeline:**
Kadin will collaborate with universities, vocational training institutions, and global tech companies to create a pipeline of skilled cybersecurity professionals. This will include integrating cybersecurity training into academic curricula and offering internships and on-the-job training.

Implementation Plan



Exhibit 7.2 Implementation Plan

7.6.2 Organizational Certification Programs

The organizational certification program aims to ensure that organizations across Indonesia, especially those operating in critical infrastructure sectors, meet internationally recognized cybersecurity standards. This will help reduce risks and protect important national assets.

Current Initiatives:

- **KAMI Index Assessment:**
This facilitates assessment for organizations in sectors handling sensitive information, including finance, government, and telecommunications which follows the SNI/ISO/IEC 27001.
- **MOCI's Data Protection Certification:**
This program focuses on ensuring compliance with Indonesia's Personal Data Protection Law (PDP), requiring organizations to safeguard personal data in alignment with global standards.

Role of Kadin:

Kadin, the Indonesian Chamber of Commerce and Industry, will expand these certification efforts to include more organizations, especially small and medium-sized enterprises (SMEs). Kadin will facilitate compliance with both national and international cybersecurity standards, such as **ISO/IEC 27001** and/or the **NIST Cybersecurity Framework**.

Key Focus Areas:

- 1. Mandatory Certifications:**
 - Promote mandatory certification for critical sectors, including energy, finance, and healthcare, to meet ISO/IEC 27001 standards.
 - Facilitate workshops and training sessions to help organizations prepare for certification.
- 2. SME Cybersecurity Certification:**
 - Develop a tiered certification program for SMEs that gradually introduces them to cybersecurity best practices. This would include basic compliance with NIST, with a path toward more advanced certifications like ISO/IEC 27001.
 - Provide financial support for certification programs aimed at smaller organizations, offering tax incentives and government-backed grants to encourage compliance.

Implementation Plan



Exhibit 7.3 Implementation Plan



By leveraging the collective efforts of Cybersecurity Agency: MOCI, this ensures the development of a highly skilled cybersecurity workforce and encourages organizations, particularly in critical sectors, to achieve and maintain global cybersecurity standards. Kadin's role as a facilitator for SMEs and its collaboration with government bodies will be key to achieving national cybersecurity goals.

7.7 Case Studies: Industry Support for Cybersecurity Education

Case Study 1: Google's Extensive Collaboration and Initiatives

The United States

Google is committed to making cybersecurity careers accessible to everyone, regardless of their background. Google is taking a multi-pronged approach to improve cybersecurity globally, with specific initiatives in Southeast Asia and Indonesia. To close the cybersecurity talent gap, they're investing in hands-on learning through cybersecurity clinics at 20 universities, the Google Cybersecurity Certificate for entry-level training, and industry partnerships to create new career pathways. By combining these efforts, Google aims to empower individuals and strengthen the overall cybersecurity workforce to better protect against cyber threats.⁴⁶

Southeast Asia

In Southeast Asia, Google's charitable arm, Google.org, is giving \$15 million to The Asia Foundation to start the APAC Cyber Security Fund. They're working with CyberPeace Institute and Global Cyber Alliance to improve the online security of 300,000 small businesses, nonprofits, and social enterprises in 12 Asian countries. This involves partnering with organizations and universities to provide training and support to local communities and students.⁴⁷

Indonesia

Indonesia faces a growing number of cyber threats, including data breaches and ransomware attacks, which can disrupt essential services and harm the digital economy. In Indonesia, Google is addressing the growing cyber threats by providing scholarships for BSSN officials to earn the Google Cybersecurity Certificate, sharing threat intelligence with BSSN through Mandiant, and collaborating with BSSN on using AI to enhance cybersecurity. There is a need to improve cybersecurity capabilities in the public sector and among small and medium-sized enterprises (SMEs) in Indonesia. On the other hand, policymakers in Indonesia need support in understanding and harnessing the potential of AI for cybersecurity while mitigating its risks.

• Training cybersecurity specialists:

Google is providing 1,000 scholarships for BSSN officials to earn the Google Cybersecurity Certificate. This will equip them with the skills to protect networks, devices, and data from cyber threats.

• Sharing threat intelligence:

Mandiant, a Google Cloud company, will share its industry-leading threat intelligence with BSSN. This will help BSSN understand the latest tactics used by cybercriminals and nation-state actors.

• Enhancing cybersecurity with AI:

BSSN and Google Cloud will collaborate on using AI to improve cybersecurity. This includes developing and implementing solutions that use automation, analytics, intelligence, and AI to quickly detect, investigate, and prevent cyberattacks on critical infrastructure.

This partnership is expected to strengthen Indonesia's cybersecurity workforce, improve threat detection and response, and raise cybersecurity awareness. By proactively investing in these capabilities, Indonesia aims to safeguard its digital landscape and protect its citizens from the growing threat of cyberattacks. This involves bolstering cybersecurity in the public sector and among SMEs, enabling them to better detect, prevent, and respond to cyber threats using AI-powered tools.⁴⁸

What's Next

Looking ahead, Google continues its commitment to strengthen Indonesia's cybersecurity across all levels. In addition to their partnership with BSSN, Google.org is supporting The Asia Foundation to empower 70,000

micro, small, and medium-sized enterprises (MSMEs) with crucial cybersecurity skills. This initiative, implemented with local partners like PPSW, PUPUK, and Majelis Ekonomi dan Kewirausahaan Muhammadiyah, will provide training and AI-powered security tools to help MSMEs defend against cyber threats.

Furthermore, Google Cloud offers free cybersecurity and AI training resources through its Skills Boost program, accessible to all Indonesians. These resources include courses like the Cloud Digital Leader Learning Path and the Introduction to Generative AI Learning Path, along with gamified learning experiences through The Arcade. By providing these opportunities, Google aims to equip Indonesians with valuable skills in cybersecurity and AI, enabling them to contribute to a safer and more resilient digital Indonesia.

Case Study 2: Palo Alto Networks CyberFit Nation

Initiative

Palo Alto Networks launched the CyberFit Nation program to address cybersecurity education gaps in Indonesia. The initiative offers free workshops tailored to diverse audiences, including SMEs, corporate leaders, and students.

Impact

By equipping different sectors with the knowledge and skills needed to protect their digital environments, CyberFit Nation enhances overall cybersecurity resilience. Participants gain practical insights into threat prevention and response strategies.

Case Study 3: Cisco Networking Academy

Collaboration

The Cisco Networking Academy partners with universities, vocational schools, and government agencies to provide free training in cybersecurity, networking, and IT skills.

Impact

Over 442,000 students in Indonesia have been trained through this program, earning globally recognized certifications. This enhances individual career prospects and also contributes to a more skilled national workforce capable of addressing cybersecurity challenges.

⁴⁵ BSSN et al., *National Occupational Map in the Indonesian National Qualification Framework in the Area of Cybersecurity Function*. (Jakarta: BSSN, 2019).

⁴⁶ Lisa Gevelber & Phil Venables, “New cybersecurity training to help build a safer world”, Google, May 4th, 2024, <https://blog.google/outreach-initiatives/grow-with-google/google-cybersecurity-career-certificate/>

⁴⁷ The Asia Foundation, “APAC Cybersecurity Fund”, The Asia Foundation, October 10th, 2023 <https://asiafoundation.org/apac-cybersecurity-fund/>

⁴⁸ Google Indonesia, “Google Bekerja Sama dengan BSSN dan Ekosistem Digital Indonesia untuk Memperkuat Pertahanan dan Keamanan Siber Nasional Berteknologi AI”, Google, March 5th, 2024, https://blog.google/intl/id-id/company-news/technology/2024_03_google-bekerja-sama-dengan-bssn-dan/

Chapter

08

Cybersecurity Methodologies and Risk Management Frameworks

Effective cybersecurity management requires adopting well-defined methodologies and risk management frameworks that provide organizations with clear guidelines for identifying, mitigating, and responding to cyber threats. Indonesia should prioritize the implementation of international best practices while also tailoring them to fit the specific needs of important sectors like finance, healthcare, and energy. This chapter explores how adopting well-defined cybersecurity methodologies and risk management frameworks provides clear guidelines for identifying, mitigating, and responding to cyber threats, ensuring organizational resilience.

8.1 Adopting a Standardized Cybersecurity Methodology

A standardized cybersecurity methodology or framework is essential for organizations to systematically manage their cyber risks. Adopting a recognized framework ensures that all cybersecurity activities—from identifying vulnerabilities to responding to incidents—are carried out in a structured and consistent way. It is crucial for the Indonesian government to utilize existing industry-led, globally harmonized Information and Communication Technology (ICT) standards, both in terms of setting standards for industry to meet in their own environments and also in terms of the standards that vendor ICT products should meet. Drawing on these established standards for both industry practices and vendor ICT products ensures alignment with global best practices and avoids the pitfalls of creating country-specific standards that may inadvertently hinder innovation and security.

Key cybersecurity methodologies that Indonesia should consider adopting include:

- **The Risk Management Framework:**
The Risk Management Framework (RMF) is a set of guidelines, standards, and processes developed by the U.S. National Institute of Standards and Technology (NIST) to help organizations manage information security risks. It offers a comprehensive and flexible approach that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.
- **NIST Cybersecurity Framework (CSF):**
A widely accepted framework focusing on identifying, assessing, and managing cyber risks. The NIST CSF organizes cybersecurity efforts into five key functions: identify, protect, detect, respond, and recover.
- **ISO/IEC 27001:**
This international standard focuses on establishing a comprehensive Information Security Management System (ISMS). It helps organizations protect data by ensuring confidentiality, integrity, and availability.
- **ASEAN CyberSecurity Framework:**
For regional harmonization, Indonesia should ensure alignment with ASEAN's cybersecurity initiatives, which focus on securing the region's critical infrastructure.
- **Cybersecurity Maturity Model Certification (CMMC):**
This framework offers tiered cybersecurity levels to ensure that organizations in sensitive industries like energy and defense meet stringent cybersecurity standards.

By adopting these frameworks, Indonesia can establish consistent and standardized approaches to cybersecurity across sectors, enabling organizations to better protect their assets and manage risks.

8.2 Security Controls Based on NIST Cybersecurity Framework

The NIST CSF is a widely accepted framework that provides a comprehensive set of security controls. Understanding its five core functions helps organizations implement a structured approach to cybersecurity.

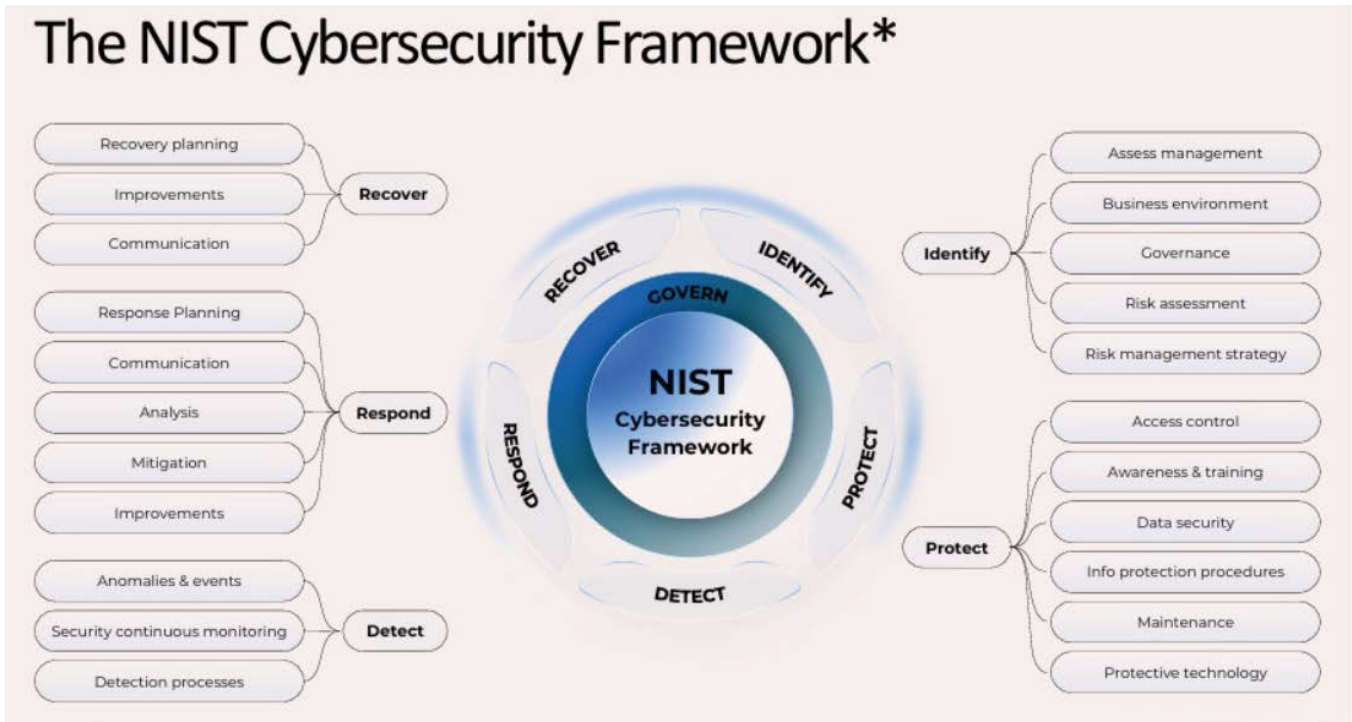


Exhibit 8.1 The NIST Cybersecurity Framework

To ensure effective cybersecurity risk management, the NIST Cybersecurity Framework provides a comprehensive set of security controls across five core functions:

1. **Identify**
2. **Protect**
3. **Detect**
4. **Respond, and**
5. **Recover.**

These functions create a structured approach for securing digital environments and responding to cyber incidents. The NIST framework's flexibility allows for adaptation to various sectors and organizations, from SMEs to critical infrastructure operators.

8.2.1 Identify

The **identify** function helps organizations understand cybersecurity risks to their systems, assets, and data. By identifying critical assets and assessing potential threats, organizations can prioritize the implementation of security measures that align with their risk profile.

Key Activities:

- **Asset management:**
Catalog all IT assets, including hardware, software, and cloud environments.
 - **Risk assessment:**
Identify vulnerabilities and threats through continuous risk assessments.
 - **Governance:**
Establish governance structures to assign accountability for cybersecurity.
- For a detailed breakdown of control steps under the NIST's identify function, refer to Appendix B.

8.2.2 Protect

The **protect** function focuses on implementing safeguards to ensure service continuity and the protection of assets. This function prioritizes proactive measures to minimize the potential impact of cybersecurity events.

Key Activities:

- **Access Control:**
Use multi-factor authentication (MFA) and role-based access control to ensure that only authorized personnel have access to sensitive systems and data.
- **Data Security:**
Encrypt data at rest and in transit, and ensure that data backups are secure and regularly updated.
- **Information Protection Processes:**
Establish policies for secure data handling and storage, and regularly audit compliance with security standards like ISO/IEC 27001.

For a detailed breakdown of control steps under the Identify function, refer to Appendix C.

8.2.3 Detect

The **detect** function focuses on monitoring systems to detect cybersecurity events in real time. Early detection of malicious activity is crucial for mitigating damage and preventing data breaches.

Key Activities:

- **Continuous Monitoring:**
Implement tools such as Security Information and Event Management (SIEM) systems to monitor networks, endpoints, and applications for suspicious activities.
- **Detection Processes:**
Set up automatic alerts for anomalies and events, and ensure that detection rules are regularly updated to reflect new threats.

Detailed methodologies for detection processes and controls are provided in Appendix D.

8.2.5 Recover

The **Recover** function ensures organizations can restore services and operations after a cybersecurity incident. This function emphasizes resilience and continuous improvement in recovery processes.

Key Activities:

- **Recovery Planning:**
Develop recovery plans to restore systems and services quickly.
- **Post-Incident Reviews:**
Conduct thorough assessments of the incident response process to identify lessons learned and improve future responses.

Further details on implementing recovery controls can be found in Appendix F.

8.3 Tailoring Cybersecurity Methodologies to Organizational Categories

Organizations come in all shapes and sizes, with different resources and levels of risk. They vary significantly in their resources, risk exposure, and digital environments. Therefore, Indonesia's cybersecurity framework must provide tailored methodologies that align with the specific needs of different organizations. To ensure that cybersecurity efforts are proportional and effective, organizations are categorized into two distinct groups, category A and category B, based on the potential damage a cyber incident could cause.

8.3.1 Category A Organizations

These include small to medium-sized enterprises (SMEs), which may not have the resources to invest heavily in cybersecurity infrastructure. For these organizations, a simplified methodology should be implemented, focusing on basic cyber hygiene and low-cost security measures.

Key Actions:

- **Basic Control Families:**

Implement approximately ten foundational control families (Appendice) that address fundamental security needs. These basic cybersecurity controls can ensure SMEs have a foundational level of security even with limited resources. (Detail on Appendix G).

Implementation Guidance:

The implementation process for Category A organizations should be straightforward and focused on practical steps:

- **Secure Network Configurations:**
Use firewalls, secure routers, and network segmentation to prevent unauthorized access.
- **Basic Access Controls:**
Implement multi-factor authentication (MFA) and ensure users have appropriate access based on their roles.
- **Regular Patch Management:**
Keep software up to date to reduce the risk of vulnerabilities being exploited.
- **Data Protection:**
Encrypt sensitive data both at rest and in transit to prevent unauthorized access.
- **Compliance and Monitoring:**
Employ simple compliance verification and basic monitoring techniques to maintain adequate cybersecurity.

Additional requirements:

Category A organizations may be subject to additional regulatory obligations if they handle sensitive information or work with third-party vendors. In such cases, they may be reclassified as Category B organizations, requiring them to adopt more advanced cybersecurity measures. Similarly, suppliers to Category B organizations may need to comply with higher security standards to protect the supply chain.

Attention:

In cyber and data security, it is common to assess potential impact based on three categories:

- **Data Confidentiality:**
For example, a cyberattack intended to leak customers' details to the internet.
- **Data Integrity:**
For example, a cyberattack intended to falsify a company's financial reports.
- **Data Availability:**
For example, a cyberattack denying information from the company or its customers (e.g., shutting down a website, locking files, or deploying ransomware).

8.3.2 Category B Organizations

Category B organizations, such as large enterprises and critical infrastructure operators, face more significant cybersecurity risks due to the complexity of their digital environments and the potential damage that cyber incidents can cause. As a result, they must adopt more sophisticated cybersecurity frameworks and advanced risk management processes.

Advanced Risk Assessment and Management Process:

Category B organizations need comprehensive risk management processes that include advanced models like PASTA (Process for Attack Simulation and Threat Analysis) and FAIR (Factor Analysis of Information Risk). These models allow organizations to quantify risks, prioritize investments, and develop mitigation strategies based on a clear understanding of potential threats.

Introduction to Advanced Models:

1. PASTA (Process for Attack Simulation and Threat Analysis):

This model helps organizations simulate potential attacks, identify vulnerabilities, and develop appropriate responses.

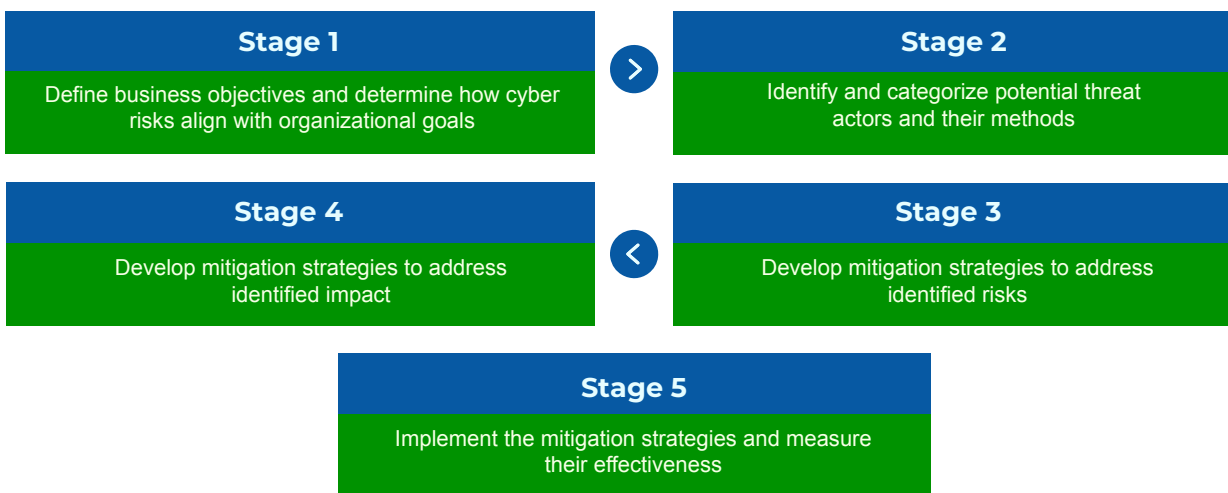


Exhibit 8.2 PASTA Processes

2. FAIR (Factor Analysis of Information Risk):

This model focuses on quantifying risks and providing a financial assessment of potential impacts.



Exhibit 8.3 Key stages of the FAIR methodology

Control Implementation Based on Risk Assessment:

Organizations should implement controls based on the outcomes of their risk assessments. Controls should be prioritized using a Control Complexity Scoring System, which ranks controls from Level 1 to Level 4 according to their complexity and cost-benefit value.

• Control Complexity Scoring

| | |
|----------------|---|
| LEVEL 1 | Basic controls that are easy to implement and involve minimal costs. Suitable for protecting assets or for organizations with limited cybersecurity budgets. |
| LEVEL 2 | Controls offering a moderate level of security, requiring some investment in resources and time to implement effectively. |
| LEVEL 3 | More complex controls that provide higher security but require significant resources and expertise to deploy. Suitable for protecting valuable organizational assets that, while not critical, still carry significant risk if compromised. |
| LEVEL 4 | The most complex controls, designed for assets considered crown jewels or of national/regulatory interest. These controls involve substantial investment and are critical for assets where the highest level of security is non-negotiable. |

Exhibit 8.4 Control Complexity Scoring

• Key Implementation Guidelines for Category B:

- **Identify Critical Assets:** Classify assets based on their importance and the potential impact of their compromise.
- **Conduct Risk Assessment:** Perform a comprehensive risk assessment to understand the threats and vulnerabilities associated with each asset.
- **Map Controls to Assets:** Based on the risk assessment and the control complexity score, assign appropriate controls to each asset. Reserve Level 4 controls for the most critical assets.
- **Resource Allocation:** Allocate resources according to the complexity scores, directing more resources toward controls critical for the organization's cybersecurity posture.
- **Monitoring and Adjustment:** Continuously monitor the effectiveness of the implemented controls and adjust as needed based on evolving threats and organizational changes.

Continuous Monitoring and Improvement

Cybersecurity is a dynamic field, and Category B organizations must continuously adapt to emerging threats. Regular audits, vulnerability assessments, and penetration tests are essential to ensure that security controls remain effective and up-to-date. Continuous review and improvement are necessary to address new risks and changes in the threat landscape.

Integration with Organizational Processes

In addition to implementing advanced cybersecurity efforts, they must be integrated with business continuity and crisis management frameworks. This ensures that cybersecurity is not treated as a standalone issue but is embedded in the organization's overall strategy.

8.4. Advanced Cybersecurity Enhancement Recommendations

8.4.1 Continuous Visibility, Audits and Proactive Security Measures

In today's rapidly evolving cyber threat landscape, maintaining continuous visibility and real-time monitoring of an organization's security posture is critical. Continuous visibility enables organizations to detect anomalies, identify vulnerabilities, and respond swiftly to threats before they escalate. Regular penetration testing, red teaming, and cyber exercises further bolster defenses by simulating real-world attacks, uncovering weaknesses, and preparing teams for actual incidents. Proactive measures such as purple teaming, where offensive and defensive teams collaborate, enhance the organization's ability to anticipate and mitigate risks. Regular audits of compliance with key security standards like ISO/IEC 27001 are also essential. By combining these strategies, organizations can build a resilient cybersecurity posture that adapts to new threats and withstands the dynamic nature of the digital environment.

8.4.2 Incentivize Attack Surface Management (ASM) Adoption

Entities of all sizes have historically struggled to understand and manage their digital infrastructure, including devices and applications exposed to the internet. Studies have found that even sophisticated enterprises may have twice the number of systems exposed on the internet than they are internally monitoring—a visibility gap that gives adversaries an advantage. Attackers regularly scan the internet for vulnerabilities in public-facing infrastructure to exploit them. Adversary scanning can occur every 15 minutes or less following vulnerability disclosures. Meanwhile, global enterprises may need an average of 12 hours to find vulnerable systems, assuming they are aware of all assets on their network.

Recommendations:

- The Indonesian government should incentivize each State-Owned Enterprise (SOE) and other organizations to implement technologies that improve real-time discovery and visibility over their network attack surfaces, particularly internet-facing assets and assets held in cloud environments.
- The cybersecurity agency may consider leveraging ASM capabilities to create a 'cyber weather' map of government and SOE entities, providing broad, near real-time visibility into each entity's cyber posture.

This approach aligns with global best practices, where entities in regions like the EU, the US, and Australia are mandated to have real-time visibility into their internet-facing infrastructure.

8.4.3 Develop Guidance/Policies on Zero Trust

The Zero Trust model is essential in eliminating implicit trust within networks and validating all user interactions. Instead of automatically trusting users and devices within a network, the Zero Trust model requires verification at every access point. By continuously authenticating every access point, Zero Trust improves the resilience of IT environments and reduces attack vectors. This strategic approach has been popularized by initiatives such as President Biden's Executive Order on Improving the Nation's Cybersecurity and is being adopted by countries like Australia to enhance governmental cybersecurity postures.

Recommendation:

The Indonesian government should develop and implement Zero Trust security guidance across both the public and private sectors. This framework will ensure that all sectors adopt policies that reduce implicit trust, continuously authenticate access, and improve overall security.

8.4.4 Develop a Plan for Secure Transition to the Cloud

Cloud adoption provides substantial benefits, including cost savings, scalability, and flexibility. However, transitioning to cloud environments must be handled securely, as cloud services are not inherently secure by default. With the rise of multi-cloud environments, organizations may face visibility challenges, increasing exposure to vulnerabilities.

Recommendation:

The Indonesian government should create a secure cloud transition plan for public and private entities. This plan must ensure comprehensive visibility and governance across all cloud environments, emphasizing automation and continuous monitoring.

Key Security Pillars for Cloud Transition:

- 1. Cloud Security Posture Management (CSPM):**
Provides continuous visibility and compliance across all cloud environments, including monitoring for misconfigurations and prioritizing risks.
- 2. Threat Detection:**
Utilizes User and Entity Behavior Analytics (UEBA) and network anomaly detection for real-time identification of threats.
- 3. Cloud Infrastructure Entitlement Management (CIEM):**
Manages access permissions and roles within the cloud to prevent security risks from excessive permissions.
- 4. Code Security:**
Incorporates supply chain security and Software Bill of Materials (SBOM) analysis to ensure secure coding practices and vulnerability management.

8.5 Enhancing Critical Infrastructure Protection

The protection of Critical Information Infrastructure (CII) is a top priority for Indonesia's national cybersecurity strategy. Critical infrastructure sectors such as energy, telecommunications, and healthcare are highly vulnerable to cyberattacks, and robust security measures must be implemented to mitigate these risks.

8.5.1 Prioritize and Invest in Critical Infrastructure Protection

Sector-specific cybersecurity guidelines, aligned with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, should be developed and enforced across all critical sectors. These guidelines will provide detailed protocols for incident response, risk management, and the implementation of advanced security controls.

8.5.2 Centralized Cybersecurity Services

Critical infrastructure sectors should centralize their cybersecurity services within sector-specific Security Operations Centers (SOCs). Centralizing services such as monitoring, incident response, and threat detection will improve the efficiency and coordination of cybersecurity efforts across critical infrastructure sectors.

8.5.3 Regular Audits and Vulnerability Assessments

To maintain compliance with regulatory standards, all critical infrastructure sectors must be subject to regular audits and vulnerability assessments. These audits will help identify areas where improvements can be made, ensuring that cybersecurity measures remain effective in protecting critical infrastructure.



Chapter

09

Strengthening Local Players in Cybersecurity Industry Growth

A robust and resilient local industry is essential to achieve Indonesia’s national cybersecurity goals. Developing a competitive local cybersecurity sector is necessary to safeguard the nation’s critical infrastructure, achieve technological independence, and foster economic growth. This chapter outlines a focused strategy to build a solid local cybersecurity ecosystem that is capable of competing globally while ensuring national security.

By empowering local firms, promoting indigenous innovation, and ensuring fair competition with foreign enterprises, Indonesia can position itself as a leader in the cybersecurity field both regionally and internationally. Three major foundations that Indonesia should consider **are ideal provision, transition, and SRO standardization.**

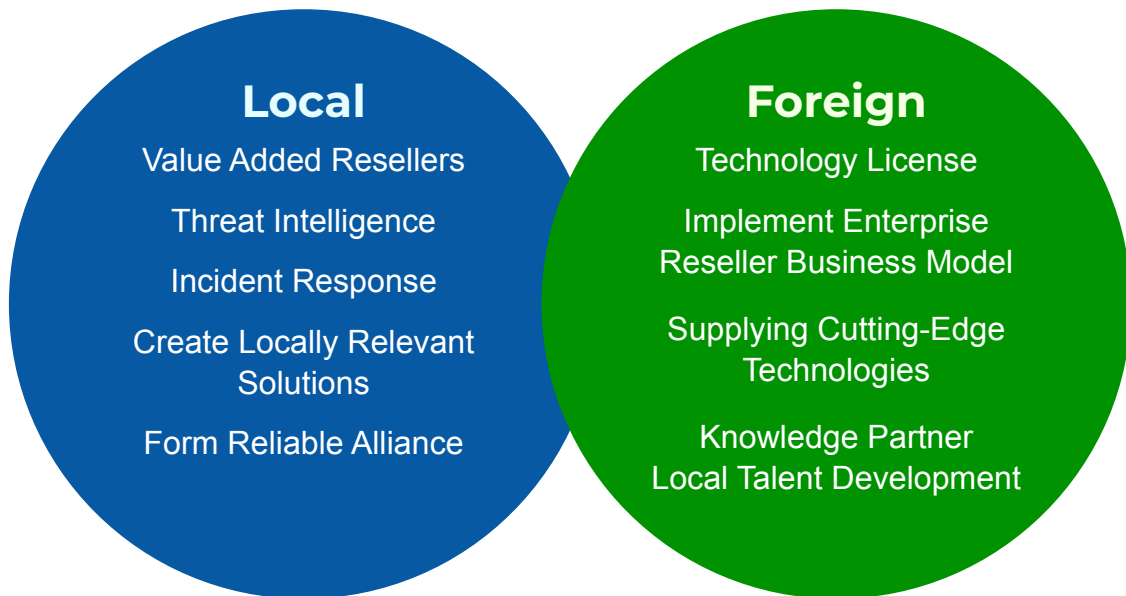


Exhibit 9.1 Ideal Provision

Ideal Provision

Increased digitization is propelling Indonesia’s cybersecurity sector’s explosive expansion, but it also confronts obstacles like a lack of qualified workers, little R&D, and a dependency on foreign solutions. Local businesses should concentrate on specialty markets like threat intelligence and incident response, create locally relevant solutions, and form reliable alliances to support a flourishing local industry while also still being able to become Value-Added Resellers (VARs). As the VARs, local companies play their role as high-end security assessors, integrators, consultants, customer success accelerators, consolidators, optimizers, managed security service providers (MSSPs), managed detection and response services (MDRs), and SOC-as-a-Service Partners.⁴⁹ International businesses may help by licensing their technology, allowing enterprise reseller business models to be applied, sharing best practices worldwide, investing in local talent development, and supplying cutting-edge technologies. Local innovation should be encouraged by the Government through incentives and policies.⁵⁰ To create a workforce of qualified cybersecurity professionals, the Government must also support cooperation between regional and international actors and invest in education and training to develop a skilled cybersecurity workforce.⁵¹

Transition from Technological Perspective

If Indonesia wants to compete at a high level, it needs to concentrate on promoting innovation rather than merely implementing current technologies. This entails creating domestic cybersecurity solutions that are suited to Indonesia’s particular problems, boosting R&D spending to spur innovation and provide a competitive edge, and fostering a cybersecurity culture by incorporating best practices and awareness into educational and professional development initiatives.⁵²

SRO Standardization

As mentioned in Chapter 5, establishing a Self-Regulatory Organization (SRO) for cybersecurity in Indonesia can help to upscale the playing field for local and international companies. SRO can create industry standards by establishing clear guidelines and best practices for cybersecurity products and services. Furthermore, it can also promote certification and accreditation by creating a framework to assess and recognize cybersecurity providers' capabilities, which will eventually positively impact local talents' capacity and capability. By ensuring fair competition based on merit and capability rather than brand recognition, the SRO can foster a more competitive and robust cybersecurity landscape in Indonesia.

9.1 Strengthening Policy and Regulatory Support for Local Industry

In Chapter 5, we discussed the broader regulatory landscape required to secure Indonesia's digital future. Building upon those foundations, Indonesia can build a self-reliant cybersecurity ecosystem by ensuring that local firms are protected from unfair foreign competition while also fostering innovation.

Key Actions:

- **Local Content Mandates**

The Indonesian Government can implement regulations requiring a minimum proportion of local content in cybersecurity procurement for Government agencies and vital infrastructure projects to promote a thriving local cybersecurity sector. Clear definitions of "local" goods and services, including incorporating standards like Indonesian ownership and domestic R&D, can help achieve this. Local businesses could progressively increase their capacity to satisfy demand using a phased deployment strategy. A method for auditing and confirming compliance should also be implemented with the help of independent certifying organizations. For instance, the Government may require all agencies to purchase at least 40% of services or goods that they need from local suppliers.⁵³

- **Preferential Treatment in Procurement**

The Indonesian Government can modify regulations related to procurement to grant preferential treatment to empower and support the growth of local cybersecurity companies, especially SMEs. This can be achieved by providing price benefits during the procurement bidding process. Furthermore, some governments, either in municipal or provincial level contracts, might only be awarded to regional suppliers, particularly for initiatives that deal with sensitive data or local needs. Encouragement of joint ventures between domestic and foreign businesses will also help local businesses

meet local content standards while gaining access to cutting-edge technologies and invaluable experience. For instance, local cybersecurity SMEs could receive a 10% pricing preference in Government tenders during the procurement process. One example would be India, which has imposed preferential treatment in procurement for cybersecurity products, which is expected to foster income and employment growth.⁵⁴

- **Regulatory Simplification**

The Indonesian Government needs to expedite yet streamline the bureaucratic hurdles of licensing and regulation processes for the establishment of local cybersecurity businesses where businesses can quickly acquire licenses, permits, and certificates, streamlining the compliance procedure. It would ensure that local businesses fully comply with the criteria and can comply efficiently if clear and concise guidance on cybersecurity standards and regulations were provided through the eligibility assessment process, exclusion of tenderers with poor track records, and cyber integrity of prospective tender, goods, and procurement procedure. Additionally, tax incentives for regional cybersecurity SMEs and startups would also promote investment and industry expansion.

- **Anti-Dumping Laws**

Introduce measures to prevent foreign companies from using predatory pricing strategies that undermine local firms' competitiveness.

⁴⁹ Emily Real, "Rethinking Cyber Security Strategies: The Role of VARs", Veeam, December 27th, 2023, <https://www.veeam.com/blog/cyber-security-resellers-veeam.html>

⁵⁰ International Trade Administration, "Indonesia Digital Economy", International Trade Administration, September 19th, 2024, <https://www.trade.gov/country-commercial-guides/indonesia-digital-economy>



Impact:

- Increase opportunities for local companies, giving local cybersecurity firms greater access to national projects and enabling them to scale and grow.
- Reduce reliance on foreign solutions, decreasing Indonesia's dependence on foreign technologies and fostering technological sovereignty.
- Enhance competitiveness of local startups and SMEs, allowing them to innovate, compete internationally, and strengthen Indonesia's cybersecurity resilience.

9.2 Fostering a Competitive and Resilient Local Industry

Every successful industry is built on innovation, and Indonesia's cybersecurity market is no different. This section explores the particular mechanisms that stimulate innovation in the community's cybersecurity ecosystem. By supporting R&D, public-private collaborations, and intellectual property protection, Indonesia can lessen its need for foreign technologies and create a competitive, self-sustaining cybersecurity economy.

Key Actions:

• R&D Grants and Incentives

The Government must introduce R&D grants and tax incentives for local firms investing in cybersecurity technologies to stimulate local innovation. R&D grants are expected to cultivate the culture of science and innovation further. By offering direct funding and tax breaks, the Government can lower the cost barriers for local firms, enabling them to explore new and advanced cybersecurity solutions. The Government of the United States has done this through its R&D Tax Credit.⁵⁵

• Innovation Hubs

The establishment of cybersecurity innovation hubs will provide a collaborative environment where startups, research institutions, and corporations can co-create solutions. These hubs will serve as incubators for new technologies and business models, supporting the growth of local talent and companies. Each hub will focus on Indonesia's unique cybersecurity needs, such as securing critical infrastructure and protecting digital identities while fostering a culture of continuous innovation. For instance, in Europe, an innovation hub for cybersecurity called European Digital Innovation Hubs (EDIHs) - Cybersecurity Innovation Hub provides a wide range of programs, including pre-investment testing, networking, skilling, and networking.⁵⁶

• Research Collaborations

Local cybersecurity firms should be encouraged

to partner with academic institutions to co-develop technologies tailored to Indonesia's specific challenges. Several promising academic institutions in Indonesia are ready to support the initiatives. This model will facilitate knowledge transfer and information exchange between academia and industry, ensuring that research is science-backed and grounded in practical applications. Some case study examples are the UK Research Institute in Secure Hardware and Embedded Systems (RISE), Cyber NYC, and Stanford Cyber Initiative (SCI).⁵⁷ By combining both strengths, Indonesia can further accelerate the development of local cybersecurity solutions.

• Intellectual Property (IP) Protection and Commercialization

Protecting local innovation is crucial to ensuring that Indonesian firms benefit from their investments in R&D by strengthening the regulations and related ruling institutions in enforcing IP protection.⁵⁸ The Government should enhance IP protection laws, ensuring local firms can secure patents for their innovations, especially for digital products.⁵⁹ Moreover, support mechanisms for commercialization need to be introduced, helping local firms bring their technologies to market domestically and internationally. This will drive competitiveness and incentivize further investments in R&D. It is highly recommended that the government of Indonesia also learn from WIPO about the protection of IP.

⁵¹ edX Enterprise, "Indonesia Cyber Education Institute case study: Supporting students in building in-demand skills", edX Enterprise, March 7th, 2024, <https://business.edx.org/case-study/indonesia-cyber-education-institute-case-study-supporting-students-in-building-in-demand-skills>

Impact:

- Increase R&D investment in the local cybersecurity sector, leading to the development of local solutions tailored to national needs.
- Stronger local industry's competitiveness can reduce our reliance on foreign products and technologies.
- The cultivation of innovation culture can drive technological advancement across the industry.

Through these series of actions, it is expected that the growth of the local cybersecurity industry can be boosted, human capital can be harnessed, and the ecosystem can be harmonized. This is aligned with the blueprint's proposal to foster a competitive and resilient local cybersecurity industry.

9.3 Supporting Local Firms' Participation in Government Projects

For Indonesia's local cybersecurity industry to thrive, they must be provided meaningful opportunities to participate in national projects. By creating designated procurement set-asides, offering capacity-building programs, and facilitating mentorships, the Government can ensure that local firms gain experience and build the credibility needed to grow.

Key Actions:

- **Designate Procurement Set-Asides for Local Companies**
Designate a portion of Government cybersecurity projects exclusively for local companies, providing them with opportunities to secure national contracts and gain valuable experience.⁶⁰
- **Capacity Building and Standardization for Local Companies**
Offer training programs and technical assistance to help local firms meet the standards for participating in large-scale national projects.
- **Mentoring Program**
Facilitate mentorship programs where international cybersecurity firms mentor local companies, helping them develop the expertise needed to compete in the market. These programs can take the form of hackathons, workshops, and boot camps to nurture emerging local talent.
- **Pilot Programs for Local Firms**
Launch pilot projects to allow local firms to demonstrate their capabilities in Government projects, building a track record to bid for larger contracts.
- **Business Incubation**
Grow and nurture local cybersecurity firms by partnering with accelerators, incubators, enablers, venture capital, and angel investors to unleash the economic opportunity further. One example is Italy, where the Incubator of Politecnico di Torino partnered with the Italian Agency for National Cybersecurity (ACN) to provide a cybersecurity incubation program for cybersecurity startups.⁶¹

Impact:

- Increase participation of local companies in national cybersecurity projects can drive business maturity, growth, and experience.
- Strengthened capabilities among local firms can enhance their ability to take on larger projects and compete with international players.
- Providing equal opportunity for local companies

⁵² Indosec, "What should be Indonesia's national cybersecurity strategy in 2024?", Indosec, July 25th, 2024, <https://indosecsummit.com/indonesia-national-cybersecurity-strategy-2024/>

⁵³ Sekretariat Kabinet, "Pengadaan Barang dan Jasa Pemerintah, Wapres: 40 Persen Alokasi untuk UMKM", Sekretariat Kabinet, June 18th, 2021, <https://setkab.go.id/pengadaan-barang-dan-jasa-pemerintah-wapres-40-persen-alokasi-untuk-umkm/>

⁵⁴ ET Bureau, "Government to introduce preferential public procurement for cybersecurity products", The Economic Times, Sep 26, 2017, <https://economictimes.indiatimes.com/tech/software/government-to-introduce-preferential-public-procurement-for-cybersecurity-products/articleshow/60843739.cms?from=mdr>

9.4 Encouraging Technology Transfer and Fair Competition

As Indonesia continues attracting foreign investment in its growing digital economy, partnerships developed with foreign players must be linked to empower local cybersecurity companies. Therefore, structuring foreign partnerships to benefit local companies and putting measures in place to safeguard national interests can ensure that Indonesia's cybersecurity industry develops in a competitive and sustainable way.

Key Actions:

- **Licensing, Value Added Resellers (VARs), and Enterprise Reseller Business Model**
Local firms should be able to get licensing and decide to become resellers of foreign firms' cybersecurity products and services.⁶²
- **Technology Transfer Agreements**
Foreign firms are required to engage in technology transfer when entering the Indonesian market, ensuring that local companies benefit from access to advanced technologies.
- **Equity Restrictions in Key Sectors**
Implement ownership restrictions in critical cybersecurity areas, ensuring local companies retain control over key projects and infrastructure.
- **Joint Ventures and Strategic Alliances**
Encourage partnerships between foreign and local firms to combine international expertise with local knowledge.
- **Knowledge Sharing Initiatives**
Establish knowledge-sharing platforms where foreign companies provide training and technical expertise to local professionals, ensuring the transfer of valuable skills.

Impact:

- Strengthen local industry capabilities through knowledge sharing and access to advanced technologies.
- Increase collaboration between local and foreign firms, fostering innovation and growth.
- Protection of national interests by ensuring local companies control critical infrastructure.

⁵⁵ Omar Assoudi, "Leveraging the R&D Tax Credit: Cybersecurity Innovation", Leyton, February 8th, 2024, <https://leyton.com/us/insights/articles/leveraging-the-rd-tax-credit-cybersecurity-innovation/>

⁵⁶ European Commission, "European Digital Innovation Hubs (EDIHs) - Cybersecurity Innovation Hub", https://commission.europa.eu/projects/european-digital-innovation-hubs-edihs-cybersecurity-innovation-hub_en

⁵⁷ European Commission, "European Digital Innovation Hubs (EDIHs) - Cybersecurity Innovation Hub", https://commission.europa.eu/projects/european-digital-innovation-hubs-edihs-cybersecurity-innovation-hub_en

⁵⁸ Raihan Zahirah & Theo Gerald, "Digitalisasi, Teknologi, dan Inovasi" in *Visi dan Peta Jalan Indonesia Emas 2045 Milik Pemuda*, ed. Reza Edriawan et al. (Jakarta: Indonesian Youth Diplomacy, 2024) 84, https://iyd.or.id/wp-content/uploads/2024/09/05092024_IYD_Report_All-Content.pdf

⁵⁹ Thales Group, "Software Intellectual Property: What It Is & How to Protect It", Thales Group, <https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property>

⁶⁰ OECD, "Intervening to support SMEs in public procurement" in *SMEs in Public Procurement: Practices and Strategies for Shared Benefits*. OECD. (Paris: OECD, 2018), 84-86.

⁶¹ i3P, "i3P launches the Cybersecurity Incubation Program, promoted with ACN and in collaboration with Leonardo and C*Sparks", i3P, February 5th, 2024, <https://www.i3p.it/en/news/i3p-launches-cybersecurity-incubation-program-acn-leonardo-c-sparks>

⁶² Emily Real, "Rethinking Cyber Security Strategies: The Role of VARs", Veeam, December 27th, 2023, <https://www.veeam.com/blog/cyber-security-resellers-veeam.html>



Chapter

10

Implementation Roadmap

To transform Indonesia into a cybersecurity-resilient nation, the implementation of cybersecurity measures must be systematically and meticulously planned, phased, and monitored. This roadmap sets forth a strategic path to build Indonesia’s cybersecurity capabilities incrementally, addressing both immediate needs and long-term goals. By aligning with global best practices and adapting to the local context, this roadmap provides a clear, actionable framework for government agencies, businesses, and critical infrastructure operators.

10.1 Periodical Target

Implementation Roadmap for Indonesia’s Cybersecurity Resilience

| I. Short Term Target (by 2030) | II. Medium Term Target (by 2035) | III. Long Term Target (by 2040) |
|---|---|--|
| <p>Foundation Building & Early Strengthening</p> <ul style="list-style-type: none"> • Establish National Cyber Defense Infrastructure: Form National CERT, develop incident response frameworks. • Cybersecurity Education & Talent Programs: Integrate basic cybersecurity curriculum in schools and universities. • Critical Sector Protection: Secure financial services, and critical infrastructure with international-standard protocols. • Strengthen Legal & Regulatory Framework: Implement strict data protection laws, incident reporting standards, and cybersecurity regulations. | <p>Advanced Capabilities & Ecosystem Growth</p> <ul style="list-style-type: none"> • Advanced Threat Management: Capabilities to address APTs, disinformation, infrastructure outages, and sophisticated cyber threats. • Adoption of Emerging Technologies: AI integration for surveillance, automation of threat detection and incident response. • Build a Cybersecurity Ecosystem: Promote startups, invest in R&D, and enhance the skilled cybersecurity workforce. • Regional & Global Engagement: Establish international threat intelligence sharing, cyber treaties, and a rapid response team for cross-border security. | <p>Full Resilience & Global Leadership</p> <ul style="list-style-type: none"> • Achieve Maximum Cyber Resilience: Attain robust cyber defense capabilities across all sectors to predict, withstand, and recover from cyber incidents. • Become a Global Cybersecurity Leader: Lead in specific cybersecurity domains, acting as an enabler for best practices and innovations. • Influence Global Norms & Policies: Actively contribute to the creation of international standards for responsible behavior and collaboration in cyberspace. |

Exhibit 10.1 Short, Medium, and Long-Term Target

10.1.1 Short term target 2030

- Indonesia should develop essential cybersecurity capabilities, including a national Computer Security Incident Response Team (CSIRT), incident response plans, basic cybersecurity education in schools, and a skilled cybersecurity workforce. Furthermore, the country should strengthen cyber infrastructure and implement strong data protection measures and establish early cybersecurity regulations for important sectors. Indonesia also must enhance the capacity of law enforcement agencies to handle cybercrime, clarifying their roles, responsibilities, and organizational structure. This will streamline the process for citizens to report cybercrime and ensure a swift response from law enforcement.
- Indonesia needs to prioritize critical sectors such as financial services, healthcare, manufacturing, and critical infrastructure to be protected from cybercrime, bolster trust, and facilitate growth. This includes international-standard security protocols, establishing early detection and monitoring systems, and conducting regular security checks and audits.
- Indonesia must enhance law enforcement capacity and international collaboration to tackle complex cyber threats including malware, social engineering, network-based attacks, web application attacks until AI powered attacks. Indonesia also needs to develop comprehensive regulations to address cyber security issues, including data protection, privacy, incident reporting, and security standards for digital products and services. These regulations will guide the handling of cyberattacks, prevention, detection, response, and recovery procedures.

10.1.2 Medium term target 2035

- Indonesia should be able to have advanced threat management to handle more sophisticated threats such as APT attacks, disinformation operations, and major infrastructure outages. In addition, Indonesia also should adopting latest high-capability technology, which include integrating artificial intelligence to improve surveillance, automating threat detection and response, and enhancing the capacity of the Computer Security Incident Response Team (NCSIRT)
- Indonesia needs to build a strong local cybersecurity industry ecosystem and growth by supporting the creation of startups, investing in research and development, and developing a skilled workforce.
- Indonesia must take a more active role in regional and international information sharing, cybersecurity cooperation, and capacity building. This includes exchanging cyber threat intelligence, developing digital extradition treaties, and forming an international rapid response team for cross-border security.

10.1.3 Long term target 2040

- Indonesia must attain the highest cyber resiliency level across all sectors, including the ability to anticipate, withstand, mitigate, respond, and recover from major cyber incidents.
- Indonesia should be able to become cybersecurity leader and enabler in specific domain.
- Indonesia needs to actively participate in creating global norms and guidelines for cyberspace, encouraging responsible behavior and collaboration between countries.

| Policy Area | | Key Stakeholders |
|---|--|--|
| 1st Pillar Strengthening Cybersecurity Infrastructure | | |
| Immediate Action | Conduct cybersecurity audits and vulnerability assessments across critical infrastructure. | Kadin |
| | Establish incident response and recovery plans tailored to critical sectors (energy, healthcare, etc.). | Coord. Ministry of Politics, Law, and Security |
| | Establish SOC for continuous monitoring of government and SOE networks. | MOCI |
| Medium-term Action | Implement regular penetration testing, red teaming, and cyber exercises for critical infrastructure sectors. | MOD Cybersecurity Agency SOE |
| | Expand SOC capabilities with AI-driven monitoring and response systems | Indonesia National Police Indonesia National Army House of Representatives |

| | | |
|---|--|---|
| Long-term Action | Fully integrate SOC across all sectors to enable real-time threat intelligence and response coordination. | State Intelligence Agency Private sector Academia Research Institutions Industry association IGO |
| | Upgrade SOC with next-gen technologies like AI and machine learning. | |
| 2nd Pillar Enhancing Cybersecurity Regulatory and Legal Framework | | |
| Immediate Action | Review and enhance cybersecurity laws aligning with global standards (e.g., SNI/ISO/IEC 27001, GDPR). | Kadin Coord. Ministry of Politics, Law, and Security MOCI MOD MOHA MSABR Attorney General's Office |
| | Define Government Policy and Operational Roles, and Responsibilities- particularly with respect to the cybersecurity agency, the National CSIRT, the National Emergency Management Authority | |
| Medium-term Action | Elevate Cyber Security to the Highest Levels of Government via key Presidential Advisory. | Cybersecurity Agency SOE MOH MOF MOI Indonesia National Police Indonesia National Army |
| | Develop sector-specific cybersecurity regulations (healthcare, finance, etc.) in collaboration with regulatory bodies. | |
| | Strengthen compliance mechanisms and enforcement through regular audits. | |
| Long-term Action | Ensure regular updates to cybersecurity regulations in response to evolving global cybersecurity frameworks. | House of Representatives State Intelligence Agency Private sector Academia Research Institutions Industry Association IGO OJK Central Bank of Indonesia |
| | Establish a fully centralized governance model under the cybersecurity agency to ensure seamless law enforcement across all sectors. | |

| 3 rd Pillar: Developing a Skilled Cybersecurity Workforce | | |
|--|--|--|
| Immediate Action | Designate Government Agency Lead for Cyber Education and Awareness Raising. | Kadin MOCI MOD Cybersecurity Agency MOE SOE Private Sector Education Institutions Academia Civil society Practitioner Media Industry association Think Tanks Philanthropic Local government |
| | Incentivizing ICT and STEM Courses via scholarships or other initiatives. | |
| Medium-term Action | Design cyber education through informal avenues such as MOOC, workshop, mentorship, etc. | |
| | Build comprehensive cybersecurity education and training programs at schools and universities. | |
| | Develop internships, micro-credentials, and apprenticeships for cybersecurity roles. | |
| Long-term Action | Initiate standardized certification programs for professionals and organizations. | |
| | Establish Indonesia as a regional hub for cybersecurity expertise through international collaborations. | |
| Long-term Action | Launch continuous professional development programs tailored for cybersecurity staff. | |
| | Establish Indonesia as a regional hub for cybersecurity expertise through international collaborations. | |
| 4 th Pillar: Fostering Public-Private Partnerships | | |
| Immediate Action | Develop real-time threat intelligence sharing platforms. Establish a Cyber Incident Review Board that includes key public and private stakeholders. | Kadin MOCI MOD Cybersecurity Agency SOE Attorney General's Office Indonesia National Police Indonesia National Army House of Representatives |
| Medium-term Action | Strengthen law enforcement and private sector collaboration for combating cybercrime. | |
| | Foster cross-sector collaboration through Kadin-led cybersecurity exercises. | |
| Long-term Action | Formalize long-term collaboration agreements with global cybersecurity leaders for threat intelligence sharing. | |

| | | |
|--|--|--|
| | Create a self-regulatory organization for cybersecurity management. | State Intelligence Agency Private sector Industry Association Media |
| 5th Pillar: Adopting Global Cybersecurity Best Practices | | |
| Immediate Action | Require immediate adoption of internationally recognized cybersecurity standards/Risk Management Practices (e.g., SNI/ISO/IEC 27001, NIST CSF, RMF). | Kadin Coord. Ministry of Politics, Law, and Security MOCI MOD |
| | Incentivize Attack Surface Management (ASM) adoption across SOEs and private organizations. | Cybersecurity Agency SOE |
| Medium-term Action | Develop guidance and/or incentivise the adoption of Zero Trust security across sectors. | Attorney General's Office Indonesia National Police |
| | Mandate continuous monitoring and visibility programs for all critical organizations | Indonesia National Army House of Representatives |
| Long-term Action | Achieve national leadership in cybersecurity by aligning Indonesia's standards with global best practices. | State Intelligence Agency Private Sector Academia |
| | Conduct annual reviews to update standards as per evolving global benchmarks. | Research Institutions Industry Association IGO |
| 6th Pillar: Strengthening Local Players in Indonesia Cybersecurity Industry Growth | | |
| Immediate Action | Protecting local players with policy support such as enforcing local content mandates, encouraging local companies with supportive procurement policies, and implementing anti-dumping laws. | Kadin MOCI MOI MOT |
| | Set up cybersecurity innovation hubs to drive local innovation and startup growth. | KPPU LKPP Private Sector |
| | Begin the establishment of a Self-Regulatory Organization (SRO) to develop and implement cybersecurity standards and certification programs. | Industry association BRIN Academia |

| | | |
|---------------------------|--|---|
| Medium-term Action | Expand R&D grants and tax incentives for local cybersecurity firms and innovation hubs. | Venture Capitalists Angel Investors |
| | Allocate a portion of government cybersecurity projects for Indonesian local companies. | |
| | Mandate top global enterprises to transfer technology and knowledge to Indonesian local companies via licensing, partnerships, or joint ventures. | |
| Long-term Action | Using solutions from local companies for advanced threats, to bring technological independence by reducing reliance on foreign technologies. | Kadin MOCI MOI MOT MLHR MOFA Private Sector Industry Association BRIN Academia |
| | Maintaining sustainable innovation by strengthening intellectual property (IP) rights protection and commercialization for local innovation. | |
| | Achieving global cybersecurity leadership by positioning Indonesia as a global leader in cybersecurity standards and practices. | |
| Financing Pathways | | |
| Options | State budget, investment, grants, CSR, PPP, foreign aid, Government Cooperation with Business Entities (KPBU), innovation matching funds, and blended finance. | |

10.2 Measuring Success

Key Performance Indicators for Indonesia's Cybersecurity Strategy

| 1st Pillar: Strengthening Cybersecurity Infrastructure | | 2nd Pillar: Enhancing Regulatory and Legal Framework | | 3rd Pillar: Developing a Skilled Cybersecurity Workforce | |
|--|---|---|---|---|---|
| 1.1 | Frequency of audits and assessments | 2.1 | The quantity of cybersecurity laws that conform to global norms | 3.1 | Total number of trained cybersecurity professionals |
| 1.2 | Time to patch critical vulnerabilities | 2.2 | Regulatory compliance rate | 3.2 | Number of colleges that grant degrees in cybersecurity |
| 1.3 | Incident response time (Mean Time to Respond-MTTR) | 2.3 | Frequency of legal framework updates | 3.3 | The degree of public knowledge on cybersecurity threats |
| 1.4 | Recovery Time Objective (RTO) | 2.4 | Number of organizations with a dedicated CISO | 3.4 | Number of participants in upskilling programs |
| 1.5 | Number of sector-specific SOCs established | | | | |
| 1.6 | Rate of information sharing between the national SOC and sector-specific SOCs | | | | |
| 4th Pillar: Fostering Public Private Partnerships and Collaboration | | 5th Pillar: Adherence to International Cybersecurity Standards | | 6th Pillar: Strengthening Local Players in Indonesia Cybersecurity Industry Growth | |
| 4.1 | Number of public-private partnerships formed | 5.1 | Number of organizations adhering to international standards | 6.1 | Policy and Regulatory Support |
| 4.2 | Frequency of threat intelligence sharing | 5.2 | Frequency of cybersecurity audits | 6.2 | Fostering a Competitive and Resilient Local Industry |
| 4.3 | Number of joint R&D projects initiated | 5.3 | Adoption rate of risk management frameworks | 6.3 | Local Firms' Participation in Government Projects |
| 4.4 | Number of Cyber Incident Review Boards forged | 5.4 | Number of organizations achieving specific CMMC level | 6.4 | Technology Transfer and Fair Competition |

Exhibit 10.2 Key Performance Indicators for Indonesia's Cybersecurity Strategy

Pillar 1: Strengthening Cybersecurity Infrastructure

1.1 Frequency of audits and assessments:

In order to find flaws and vulnerabilities in systems and procedures before attackers can take advantage of them, regular audits and assessments are helpful. Generally speaking, a higher frequency denotes a more proactive security posture. The risk profile of the systems being audited should dictate how frequently these audits occur.

Aim for at least once a year for critical infrastructure companies and more frequently for businesses that pose a higher risk.

1.2 Time to patch critical vulnerabilities:

This indicator assesses how fast a company can address serious security flaws in its hardware and software. Attackers have a smaller window of opportunity when patches are applied more quickly. This is a crucial sign of how well-equipped a company is to handle threats.

Aim for less than 2 hours, *with continuous improvement towards real-time response.*

1.3 Incident response time (Mean Time to Respond-MTTR):

The duration required to identify, contain, and resolve a cybersecurity incident is measured by MTTR. A lower MTTR means an organization can minimize damage and downtime caused by attacks. This is an important indicator of how prepared a company is for cybersecurity threats.

Less than 2 hours, with continuous improvement towards real-time response

1.4 Recovery Time Objective (RTO):

The maximum allowable time to restore a system or service following an outage is defined by the RTO. A shorter RTO is a sign of a more resilient company that can recover from setbacks fast. Maintaining vital services and reducing downtime depend on this.

Aim for less than 4 hours for critical systems, with well-tested recovery plans.

1.5 Number of sector-specific SOCs established:

Within critical infrastructure sectors, sector-specific Security Operations Centers (SOCs) facilitate specialized threat intelligence exchange and incident response. An increased number of SOCs points to a more effective and well-coordinated defense across several industries. This demonstrates an industry-wide commitment to cybersecurity.

At least one dedicated SOC per critical sector, integrated with the national SOC.

1.6 Rate of information sharing between Indonesia's SOC and sector-specific SOCs:

For rapid threat identification and response, sector-specific SOCs and the national SOC must effectively share information. A high sharing rate promotes effective teamwork and makes it possible to comprehend the danger landscape more thoroughly. A concerted national cybersecurity effort requires this.

Enable real-time, automated sharing of threat intelligence and incident reports between the national SOC and sector-specific SOCs.

Pillar 2: Enhancing Regulatory and Legal Framework

2.1 The quantity of cybersecurity laws that conform to global norms:

A country's alignment with international cybersecurity standards like SNI/ISO/IEC 27001 and GDPR demonstrates its commitment to robust cybersecurity practices. This alignment fosters trust in digital services, facilitates cross-border data flows, and strengthens the overall cybersecurity posture, indicating a dedication to protecting data and systems in the digital age.

100% alignment with key standards like SNI/ISO/IEC 27001 and GDPR within 3 years

2.2 Regulatory compliance rate:

Cybersecurity compliance rates reflect the percentage

of organizations adhering to established regulations within a jurisdiction. High compliance suggests effective enforcement and strong cybersecurity awareness, contributing to a more secure environment, while low compliance may indicate awareness gaps, enforcement challenges, or overly burdensome regulations.

Achieve at least 90% compliance with cybersecurity regulations within 5 years, with stricter targets for critical sectors.

2.3 Frequency of legal framework updates:

The frequency of updates to a country's cybersecurity laws reflects its proactive approach to addressing new threats and technologies. Regular updates ensure a



robust and effective legal framework, while infrequent updates can leave organizations vulnerable due to an outdated legal landscape.

Review of cybersecurity rules and regulations once a year to keep pace with the developments in technology and threats.

2.4 Number of organizations with a dedicated CISO:
The prevalence of Chief Information Security Officers

(CISOs) within organizations signifies a strong commitment to cybersecurity. CISOs provide expertise and leadership to manage risks, foster a security-conscious culture, and align cybersecurity with business goals, ultimately enhancing an organization's cybersecurity maturity.

Ensure 100% of critical infrastructure organizations and large enterprises have a Chief Information Security Officer (CISO) within 4 years.

Pillar 3: Developing a Skilled Cybersecurity Workforce

3.1 Total number of trained cybersecurity professionals:

The number of people who have obtained cybersecurity education or training is tracked by this measure. These could be online courses, workshops, official degrees, or certifications. It sheds light on the pool of talent that is accessible for cybersecurity positions.

Train at least 500,000 new cybersecurity professionals within 3-5 years, with a focus on critical sectors.

3.2 Number of colleges that grant degrees in cybersecurity:

This refers to the number of universities and other educational establishments that provide formal courses (such bachelor's or master's degrees) with a cybersecurity concentration. This shows how much is being invested in training the next generation of cybersecurity experts.

Establish and develop at least 10 universities with dedicated cybersecurity undergraduate and postgraduate programs within 3 years.

3.3 The degree of public knowledge on cybersecurity threats:

This assesses how well-informed the general population is about cybersecurity threats, hazards, and best practices. It demonstrates how knowledgeable people are about internet safety and their capacity for self-defense. Surveys, tests, and the observation of security measure adoption can all be used to gauge this.

Achieve 80% public awareness on basic cybersecurity hygiene within 5 years through national campaigns.

3.4 Number of participants in upskilling programs:

This monitors the quantity of people who are actively participating in courses intended to improve their current cybersecurity expertise. To address new threats and technology, these programs may involve workshops, certifications, or specialized training. This indicates a dedication to lifelong learning and professional growth for cybersecurity professionals.

Upskill at least 10,000 IT professionals in specialized cybersecurity areas within 3 years.

Pillar 4: Fostering Public-Private Partnerships and Collaboration

4.1 Number of public-private partnerships formed:

This measures the degree to which formal collaboration on cybersecurity projects occurs between public and commercial sector entities. These collaborations can be in the form of cooperative research initiatives, information sharing agreements, or joint task force, among other things. A higher figure denotes a stronger dedication to shared cybersecurity responsibility and cooperative defense.

Formalize at least 10 major public-private partnerships in cybersecurity within 2 years, with at least one focused on each critical sector.

4.2 Frequency of threat intelligence sharing:

This gauges the frequency with which various institutions exchange cybersecurity-related information about risks, vulnerabilities, and attack techniques. Numerous metrics, including the quantity of data exchanged, the frequency of meetings and communications, and the number of alerts shared, can be used to monitor this. Higher frequency typically indicates improved cooperation and communication when reacting to cyberthreats.

Real-time sharing of actionable threat intelligence between government and private sector via a dedicated platform.

4.3 Number of joint R&D projects initiated:

This monitors the quantity of collaborative research and development initiatives with a cybersecurity focus. Through these projects, several organizations collaborate to create innovative technology, approaches, and strategies to deal with cybersecurity issues. A greater figure suggests more funding for innovation and a team effort to improve cybersecurity skills.

Initiate at least 5 collaborative research and development projects in cybersecurity within 3 years, involving the public, private, and academic sectors with an emphasis on fields like AI-driven security.

4.4 Number of Cyber Incident Review Boards forged:

This assesses the official entities established to examine and assess noteworthy cybersecurity incidents. Experts from several companies or sectors usually serve on these boards, collaborating to comprehend the origins, effects, and reactions to incidents. An increasing number of boards suggests a stronger focus on enhancing future cybersecurity posture and drawing lessons from previous occurrences.

Within 2 years, create at least one sector-specific board for critical infrastructure and one national Cyber Incident Review Board.

Pillar 5: Adherence to International Cybersecurity Standards

5.1 Number of organizations adhering to international standards (NIST, ISO):

This monitors the number of companies who have embraced and put into practice well-known cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework or SNI/ISO/IEC 27001 (information security management). Adhering to these guidelines indicates a dedication to methodical security procedures and frequently entails external evaluations or accreditations.

100% compliance with SNI/ISO/IEC 27001 or NIST Cybersecurity Framework for critical infrastructure organizations within 5 years, with voluntary adoption for others.

5.2 Frequency of cybersecurity audits:

This gauges how frequently businesses assess their cybersecurity posture through internal or external audits. Frequent audits assist in finding weaknesses, evaluating standard compliance, and guaranteeing the efficacy of security procedures. A more proactive and sophisticated approach to security management is typically indicated by higher frequency.

Annual audits for all organizations, with more frequent audits for high-risk entities and critical infrastructure.

5.3 Adoption rate of risk management frameworks:

This measures the proportion of companies that have explicitly implemented a framework for risk management in order to recognize, evaluate, and reduce cybersecurity threats. Frameworks such as NIST SP 800-30 offer an organized method for managing risk and assisting organizations in setting security priorities according to their unique requirements and the threats they face.

80% adoption of comprehensive risk management frameworks (like NIST CSF or FAIR) across large organizations and critical sectors within 5 years.

5.4 Number of organizations achieving specific CMMC levels:

The Cybersecurity Maturity Model Certification (CMMC) program mandates that defense contractors adhere to particular cybersecurity requirements. There are various maturity levels for the CMMC; higher levels correspond to more sophisticated cybersecurity procedures. This indicator shows the number of organizations that have attained every certification level.

Within 3 years, target certain CMMC levels for defense and sensitive industry firms based on their risk profile and data sensitivity.

Pillar 6: Strengthening Local Players in Indonesia Cybersecurity Industry Growth

6.1 Policy and Regulatory Support:

This measures the impact of policy and regulatory intervention such as local content, preferential treatment, regulatory simplification, and anti-dumping law towards the business growth of local firms in a form of market share that signifies a substantial shift towards prioritizing local providers.

Increase market share for local firms and reduce reliance on foreign products to 30-40%. While complete self-reliance may not be feasible, this shows significant progress in building domestic capacity.

6.2 Fostering a Competitive and Resilient Local Industry:

This tracks how R&D grants, tax incentives, research collaboration between industry and universities as well as IP protection leads to the creation of new local cybersecurity companies and innovation. The bigger number resulted from this metric, it indicates a vibrant and growing ecosystem with new players emerging.

Thriving local cybersecurity industry in Indonesia should see 30-50 new companies and startups, 5-10% annual R&D growth, and new patents filed annually, demonstrating a commitment to innovation and technological advancement.

6.3 Local Firms' Participation in Government Projects:

This gauges the uplift of local companies' participation in procurement and government cybersecurity projects generated from procurement set aside mode, standardization, capacity building, mentorship, pilot project, and

business incubation. This ensures widespread involvement and opportunity for local businesses.

To significantly boost local companies' participation in government cybersecurity projects, the goal is to have 30-40% of local companies becoming capable of independently leading large-scale projects.

6.4 Technology Transfer and Fair Competition:

This monitors the inflow of advanced technologies and knowledge which derived from technology licensing, Value Added Resellers (VARs), and enterprise reseller business model, transfer agreement, joint venture, and knowledge sharing initiatives.

Indonesia aims to facilitate 3-7 major technology transfer agreements or joint ventures each year, involve 500-1,000 local professionals in knowledge sharing, and ensure that local companies maintain majority ownership in critical cybersecurity infrastructure.



Works Cited

Works Cited

- Access Partnership. 2023.** Google's role in helping Indonesia build a safe and productive society through digital tools. Economic Impact Report, Access Partnership.
- Andersen, Grady. 2024.** *Building Cyber Security Partnerships: Collaborative Efforts across Universities*. February 1st. Accessed October 2nd, 2024. <https://moldstud.com/articles/p-building-cyber-security-partnerships-collaborative-efforts-across-universities> .
- Assoudi, Omar. 2024.** *Leveraging the R&D Tax Credit: Cybersecurity Innovation*. February 8th. Accessed October 3rd, 2024. <https://leyton.com/us/insights/articles/leveraging-the-rd-tax-credit-cybersecurity-innovation/>.
- Blomstein. 2020.** *Cybersecurity and the Procurement Procedure*. November 3rd. Accessed October 1st, 2024. <https://www.blomstein.com/en/news/cybersecurity-and-the-procurement-procedure> .
- BSSN, Kadin, Ministry of Manpower, Ministry of Communication and Informatics, Ministry of National Development Planning, BNSP. 2019.** Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber Tahun 2019. Roadmap, Jakarta: BSSN.
- edX Enterprise. 2024.** *Indonesia Cyber Education Institute case study: Supporting students in building in-demand skills*. March 27th. Accessed October 1, 2024. <https://business.edx.org/case-study/indonesia-cyber-education-institute-case-study-supporting-students-in-building-in-demand-skills>.
- ET Bureau. 2017.** *Government to introduce preferential public procurement for cybersecurity products*. September 26th. Accessed October 1st, 2024. <https://economictimes.indiatimes.com/tech/software/government-to-introduce-preferential-public-procurement-for-cybersecurity-products/articleshow/60843739.cms?from=mdr> .
- European Commission.** n.d. *European Digital Innovation Hubs (EDIHs) - Cybersecurity Innovation Hub*. Accessed October 9th, 2024. https://commission.europa.eu/projects/european-digital-innovation-hubs-edihs-cybersecurity-innovation-hub_en .
- Gevelber, Lisa, and Phil Venables. 2023.** New cybersecurity training to help build a safer world. May 4th. Accessed October 3rd, 2024. <https://blog.google/outreach-initiatives/grow-with-google/google-cybersecurity-career-certificate/>.
- Google. 2024.** Secure, Empower, Advance: How AI Can Reverse the Defender's Dilemma. Industry Report, Google.
- Google Indonesia. 2024.** Google Bekerja Sama dengan BSSN dan Ekosistem Digital Indonesia untuk Memperkuat Pertahanan dan Keamanan Siber Nasional Berteknologi AI. March 5. Accessed October 1st, 2024. https://blog.google/intl/id-id/company-news/technology/2024_03_google-bekerja-sama-dengan-bssn-dan/?

- Hansen, Royal, and Christoph Kern. 2024.** *Tackling cybersecurity vulnerabilities through Secure by Design*. March 4th. Accessed October 4th, 2024.
- Hukumonline. 2024.** “Strengthening the National Cybersecurity Ecosystem: Unveiling New BSSN Frameworks on Cyber Incidents and Cyber-Crisis Management.” *Law Digest*, April 10. <https://pro.hukumonline.com/a/lt66165fbd50830/strengthening-the-national-cybersecurity-ecosystem--unveiling-new-bssn-frameworks-on-cyber-incidents-and-cyber-crisis-management>.
- i3P. 2024.** *I3P launches the Cybersecurity Incubation Program, promoted with ACN and in collaboration with Leonardo and C*Spark*. February 5th. Accessed October 6th, 2024. <https://www.i3p.it/en/news/i3p-launches-cybersecurity-incubation-program-acn-leonardo-c-sparks> .
- ID-SIRTII. n.d.** *History Id-SIRTII/CC*. Accessed October 10, 2024. <https://www.idsirtii.or.id/en/page/history-id-sirtii-cc.html>.
- lfdal, Abdurrahman, and Kenzie Ryvantya. 2024.** “Ketangguhan Diplomasi Internasional.” In *Visi dan Peta Jalan Indonesia Emas 2045 Milik Pemuda*, by Reza Edriawan, Raihan Zahirah and Stephanie Gabrielle, 58. Jakarta: Indonesian Youth Diplomacy.
- IISS. 2021.** *Cyber Capabilities and National Power: A Net Assessment*. Assessment Report, IISS.
- Indosec. 2024.** *What should be Indonesia’s national cybersecurity strategy in 2024?* July 25th. Accessed October 1st, 2024. <https://indosecsummit.com/indonesia-national-cybersecurity-strategy-2024/>.
- International Trade Administration. 2024.** *Indonesia Digital Economy*. September 19th. Accessed October 7th, 2024. September 19th, 2024, .
- Kementerian Komunikasi dan Informatika Republik Indonesia. 2022.** *Presiden Instruksikan Jajarannya Tindaklanjuti Kebocoran Data Pemerintah*. September 14. Accessed October 1, 2024. <https://www.kominfo.go.id/berita/berita-pemerintahan/detail/presiden-instruksikan-jajarannya-tindak-lanjuti-dugaan-kebocoran-data-pemerintah>.
- Lagace, Martha. 2007.** *Industry Self-Regulation: What’s Working (and What’s Not)?* April 9th. Accessed September 26, 2024. <https://hbswk.hbs.edu/item/industry-self-regulation-whats-working-and-whats-not> .
- Ministry of Foreign Affairs of the Republic of Indonesia. 2020.** *Indonesia Voices Cyber Stability in the UN*. May 23. Accessed September 26, 2024. <https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un> .
- OECD. 2015.** “Industry self regulation.” *OECD Digital Economy Papers* 40-63.
- OECD (2018),** *SMEs in Public Procurement: Practices and Strategies for Shared Benefits*, OECD Public Governance Reviews, OECD Publishing, Paris, <https://doi.org/10.1787/9789264307476-en>.
- Palo Alto Networks. n.d.** *What Is Attack Surface Management?* Accessed September 26, 2024. <https://www.paloaltonetworks.com/cyberpedia/what-is-attack-surface-management>.



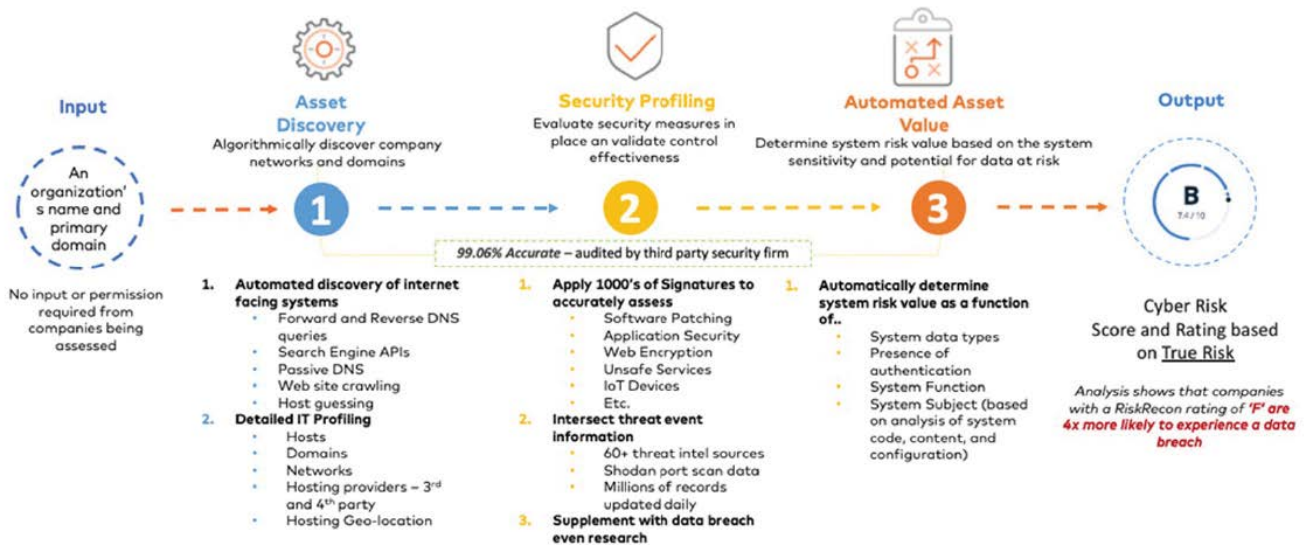
- Parekh, Mitangi. 2024.** *Cybersecurity Ventures Report on Cybercrime*. July 23. Accessed September 11, 2024. <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime>.
- Poireault, Kevin. 2023.** *Manufacturing Top Targeted Industry in Record-Breaking Cyber Extortion Surge*. November 30. Accessed September 4, 2024. <https://www.infosecurity-magazine.com/news/manufacturing-top-targeted-orange/>.
- Priyandita, Gatra. 2024.** *Indonesia's Cybersecurity Woes: Reflections for the Next Government*. Commentaries, Jakarta: CSIS.
- Rahmansyah, Denny. 2019.** *Data Protection and Cybersecurity in Indonesia: Enforcement and Litigation*. December 12. Accessed September 26, 2024. <https://www.ssek.com/blog/data-protection-and-cybersecurity-in-indonesia-enforcement-and-litigation/>.
- Real, Emily. 2023.** *Rethinking Cyber Security Strategies: The Role of VARs*. December 27th. Accessed October 4th, 2024. <https://www.veeam.com/blog/cyber-security-resellers-veeam.html>.
- Ridwan, Raihan, and Theo Gerald. 2024.** "Digitalisasi, Teknologi, dan Inovasi." In *Visi dan Peta Jalan Indonesia Emas 2045 Milik Pemuda*, by Reza Edriawan, Raihan Zahirah and Stephanie Gabrielle, 84. Jakarta: Indonesian Youth Diplomacy.
- Sari, Amelia Rahima. 2024.** Revisi UU Polri Bikin Polisi Bisa Awasi Ruang Siber hingga Blokir Internet, Pengamat: Jadi Dilema. May 30th. Accessed October 1, 2024. <https://nasional.tempo.co/read/1873786/revisi-uu-polri-bikin-polisi-bisa-awasi-ruang-siber-hingga-blokir-internet-pengamat-jadi-dilema>.
- Sekretariat Kabinet. 2021.** *Pengadaan Barang dan Jasa Pemerintah, Wapres: 40 Persen Alokasi untuk UMKM*. June 18th. Accessed October 3rd, 2024. <https://setkab.go.id/pengadaan-barang-dan-jasa-pemerintah-wapres-40-persen-alokasi-untuk-umkm/>.
- SentinelOne. 2023.** *Risks Within The Factory Lines | Examining Top Threats Facing The Manufacturing Industry*. September 19. Accessed September 11, 2024. <https://www.sentinelone.com/blog/risks-within-the-factory-lines-examining-top-threats-facing-the-manufacturing-industry/>.
- Shepherd, Christian, Cate Cadell, Ellen Nakashima, Joseph Menn, and Aaron Schaffer. 2024.** *Leaked files from Chinese firm show vast international hacking effort*. February 22. Accessed September 4, 2024. <https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoan/>.
- Statista. 2023.** *Estimated annual cost of cyber crime in Indonesia from 2018 to 2028*. March. Accessed September 11, 2024. <https://www.statista.com/forecasts/1411153/indonesia-cost-of-cyber-crime#:~:text=In%202022%2C%20the%20cost%20of%20cyber%20crimes%20in,from%202018%20to%202028%20%28in%20billion%20U.S.%20dollars%29>.
- Sury, Dr. Kartina. 2023.** *Indonesia's Cyber Resilience: At the Epicenter of ASEAN Digital Economy Growth*. Accessed September 25, 2024. <https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/>.

- Thales Group.** n.d. *Software Intellectual Property: What It Is & How to Protect It*. Accessed October 4th, 2024. <https://cpl.thalesgroup.com/software-monetization/protecting-software-intellectual-property> .
- The Asia Foundation.** 2023. *APAC Cybersecurity Fund*. October 10th. Accessed October 1st, 2024. <https://asiafoundation.org/apac-cybersecurity-fund/> .
- TJC Group.** 2024. *The strategic imperative: Decommissioning legacy systems for better cybersecurity*. July 2. Accessed September 15, 2024. <https://www.tjc-group.com/blogs/the-strategic-imperative-decommissioning-legacy-systems-for-better-cybersecurity/>.
- Unit 42.** 2022. *GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool*. June 13. Accessed September 2, 2024. <https://unit42.paloaltonetworks.com/pingpull-gallium/>.
- Unit 42.** 2024. *ASEAN Entities in the Spotlight: Chinese APT Group Targeting*. March 26. Accessed September 4, 2024. <https://unit42.paloaltonetworks.com/chinese-apt-target-asean-entities/>.
- Unit 42.** 2024. *Threat Actor Groups Tracked by Palo Alto Networks Unit 42*. June 27. Accessed September 10, 2024. <https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/>.
- Unit 42 by Palo Alto Networks.** 2024. *Incident Response Report*. Industry Report, Unit 42 by Palo Alto Networks.



Appendices

Appendix A: Mastercard RiskRecon Overview



Mastercard's innovative technology, RiskRecon, allows organizations to monitor the security programs of third parties and business associates based on their internet presence alone. Through close collaboration with governments worldwide, RiskRecon offers improved third-party risk management and better cyber hygiene. It does not require any proprietary information, permissions, disclosures, or invasive scans—it observes only what is directly available on the internet.

Unique Technology and Data Ownership

RiskRecon uses proprietary techniques that combine algorithmic and machine learning processes to discover the global IT profile of any internet-facing domain. A discovery process would involve all the systems managed by an entity, systems outsourced by them, including fourth-party domains such as Amazon, GoDaddy, and Azure. Once a system has been identified, RiskRecon captures its network information, geolocation, and all the corresponding host details. It captures in-depth security measurements through direct observation and data collection across nine security domains and 40 unique security criteria.

Unlike competitors that leverage bought databases or licensed feeds, RiskRecon owns its data. Owning the data allows the firm to create highly accurate information—a false positive rate of less than 1.0 percent—and provide a thorough, detailed data set to customers. Owning the data set in this way also enables RiskRecon to innovate rapidly, adding new measurements or scanning for additional exposures as new vulnerabilities emerge.

Automated Asset Value and True Risk Prioritization

In addition, understanding asset importance with the severity of an issue creates the critical capability to understand actual risk. RiskRecon automatically combines both of these—the issue severity and the asset's risk categorization—to determine true risk.

RiskRecon runs all that data against sophisticated models, generating an asset value profile that characterizes each IT system as high, medium, low, or idle value. Where issue severity calculates the likelihood of a system being compromised, asset value calculates the impact should that system be compromised. It may be an online banking system or an electronic commerce portal. This is a high-value asset since it contains very sensitive information like names, credit card numbers, and login credentials. In contrast, the marketing website, if hosted separately, may be considered a low-value asset in that it does not ask for sensitive data from its visitors, and it is not linked to those systems that do.

Together, asset value and issue severity measurements for each system, combined with the specific risk policy of its clients, enable RiskRecon to provide customer-specific, risk-prioritized action plans for monitored companies, along with all the supporting evidence needed to identify precisely which issues make the biggest difference to the risk. Whereas competitors provide mere lists or categorizations of the problems based on criticality, RiskRecon delivers prioritized action plans that identify the small set of issues that most make a difference in risk reduction. This enables clients to understand specific risk quantification and drive dramatic improvement in risk reduction and process efficiencies.



Accurate, Deep, and Broad Security Measurements

RiskRecon measures each control through direct observation and analysis of an entity's internet-facing systems. The company provides the most accurate, deep, and broad security measurements made up of 40 unique criteria by directly observing an organization's internet-facing footprint. Since RiskRecon has full control over data quality and timeliness, it has a false positive rate less than 1.0%.

Traditional solutions rely on threat intelligence feeds, which are inherently noisy and prone to false positives, and supplement these with purchased, dated IT asset data bases. Without full control over the results, they can never ensure accuracy nor provide the evidence required to properly remediate findings.

Supply Chain Explorer for Vulnerability Triage and Situational Awareness

RiskRecon delivers ad-hoc search to provide instant IT and security visibility across an organization's portfolio, and deep into individual third parties. Examples of this include instantly determining which third-party systems can be vulnerable to a new security vulnerability, which suppliers store data in an unapproved hosting provider or new country, and fourth-parties and concentration risks are easily identified. Indirect data sources were also added to its Data Search feature to expand knowledge of fourth-party relationships, such as vendors' vendors, further down the supply chain and expand the capability for vulnerability impact.

Measurement Criteria and Scoring

RiskRecon assesses nine security domains through direct observation and analysis of an entity's internet-facing systems:

- 1. Software Patching**
- 2. Web Application Security**
- 3. Network Filtering**
- 4. Web Encryption**
- 5. System Reputation (e.g., Command and Control, Botnet, Phishing)**
- 6. Breach Events**
- 7. System Hosting**
- 8. Email Security**
- 9. DNS Security**

With its true risk-responsive rating model, RiskRecon is the only provider. From its data, the company provides risk-adjusted weighting to each and every one of the security criteria and domains. The overall risk performance of each company with a rating falls within the range from 0. These risk-based scores are further classified, based on performance, into performance tiers of A, B, C, D, or F. This combination of performance tier and risk score provides an intuitive, risk-informed understanding of the cybersecurity maturity and risk posture of any entity.

Data Gathering and Accuracy

RiskRecon has a very accurate system in place for finding an organization's internet-facing systems and finding problems in security, thus helping identify an organization's vulnerable points on the internet. Being concerned with the accuracy of its data, it periodically audits data with third-party security firms to verify this. At the time of the last review, RiskRecon's data was certified to have an accuracy rating of 99.1%. The company does further work in refining their methodology to keep accuracy rates at or above this level.

Risk-Prioritized Findings

RiskRecon offers risk-prioritized findings for exact identification and efficient eradication of an organization's most critical third-party security risks. The SaaS service delivers the data-driven evidence necessary to rapidly identify and remediate security weaknesses on the externally facing systems associated with the companies being monitored.

Instead of overwhelming an organization with long lists of issues, RiskRecon provides risk-prioritized findings, action plans, and risk-adjusted ratings. Its customized analytics assess the IT systems of each third party to identify all security issues and calculate the asset value of each system—that is, the magnitude of resulting business impact if that system is compromised.

Measurement Criteria and Scoring

Appendix B: Identify Step in NIST Cybersecurity Framework



The Identify function lays the groundwork for an effective cybersecurity program. This pillar focuses on developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. By identifying critical functions and the related cybersecurity risks, organizations can prioritize their efforts in line with their risk management strategy and business needs.

Appendix D: Detect Function based on NIST Cybersecurity Framework



The Detect function focuses on identifying the occurrence of cybersecurity events in a timely manner. This pillar is crucial for the early detection of anomalies and incidents, enabling organizations to respond promptly and mitigate potential damage.

Appendix C: Protect in NIST Cybersecurity Framework



The Protect function outlines the safeguards necessary to ensure the delivery of critical infrastructure services. This pillar emphasizes the implementation of appropriate safeguards to protect organizational systems, assets, and data from cybersecurity threats. By developing and implementing these protection mechanisms, organizations can limit or contain the impact of potential cybersecurity events.

Appendix E: Respond based on NIST Cybersecurity Framework



The Respond function details the steps necessary to take action regarding a detected cybersecurity event. This pillar involves developing and implementing appropriate activities to respond to detected incidents and mitigate their impact. Controls in this section focus on response planning, communication, analysis, mitigation, and improvements. By establishing a robust response framework, organizations can manage and contain incidents effectively, reducing their potential harm.

Appendix F: Recover from Incident based on NIST Cybersecurity Framework



The Recover function emphasizes the importance of restoring services and capabilities following a cybersecurity incident. This pillar focuses on planning for resilience and the timely recovery of normal operations to reduce the impact of cyber incidents.



Appendix G: Basic Control Families

1. Management Responsibility

Understand existing cyber threats, and devise a work plan to close defense cyber gaps

2. Avoid Malicious Code:

Use technologies to cope with malware, and update the organization system defenses.

3. Encryption:

Encrypt remote access of employees and suppliers, using commercial encryption means. Encrypt access to sensitive data, use an encrypted communication medium (both from domestic surfing through wireless networks to the organization and vice versa to customers and suppliers).

4. Cloud Computing and Software Purchase:

Require (contractually) the supplier to comply with common software and data protection standards.

5. Data Protection:

Define protection mechanisms to protect data existing in the organization.

6. Computer Protection:

Define a required computer defense level. Including changing equipment default passwords, removal of unnecessary software programs, redundant connection blocking, removing unnecessary admin accounts.

7. Human Resources:

Instruct new employees and remove former employees' authorizations.

8. Documentation and Monitoring:

Document and monitor exceptional activities, which may attest to cyber threats.

9. Network Security:

Ensure that network access is under the organization's control (suppliers and employees cannot connect remotely at will) and that the network is prepared to withstand denial of service attacks.

10. Business Continuity:

Recover capabilities from site failures, deletion of data, file blocking.

Appendix H: Guide for Regulators on Mapping and Rating Organizations in Critical Infrastructure

Introduction:

This guide is intended for regulators and provides tools for risk assessment and classification of organizations within critical infrastructure sectors. This process is essential to ensure that regulatory measures are appropriately tailored to the risk level and operational significance of each organization.

Importance of Mapping and Rating:

Understanding the risk profile and operational importance of organizations within critical infrastructure sectors is vital. It allows regulators to prioritize resources, enforce targeted regulations, and ensure that the most critical components of the nation's infrastructure are adequately protected against cyber threats.

Incorporating Supply Chain Considerations:

1. Supply Chain Dependency:

Assess how much an organization relies on its supply chain. Those heavily dependent are at higher risk of disruption and cyber threats.

2. Supply Chain Resilience:

Evaluate the resilience of the supply chain to disruptions such as natural disasters, geopolitical tensions, or cyberattacks.

3. Third-Party Risk:

Identify and assess risks from third-party service providers and suppliers, especially those involving critical services or components from regions with lax cybersecurity measures.

4. Supply Chain as a Cyber Threat Vector:

Consider the potential for the supply chain to serve as a conduit for cyber threats.

Updated Risk Assessment Table with Supply Chain Considerations

Include columns for assessing supply chain risk alongside traditional risk factors such as market dependency, economic impact, and data sensitivity.

Guidance for Regulators with a Focus on Supply Chain:

- Regulators should use the enhanced risk assessment framework to understand how supply chain factors influence an organization's overall risk profile.
- Organizations identified with significant supply chain risks may require additional oversight, such as audits of suppliers and third-party risk management practices.

Appendix I: Regulatory Risk Assessment Checklist

Organizational Impact

1.1 Essential Services

Question:

Does the organization provide essential services that, if disrupted, would have a significant impact on public safety or national security?

1.2 Economic Impact

Question:

How significant is the organization's role in the national or regional economy?

1.3 Monopoly Status

Question:

Is the organization a sole provider of critical services or products in its market?

Question:

Does the organization handle sensitive or regulated data such as PHI (Protected Health Information), PCI (Payment Card Industry data), or government data?

2.2 Volume of Data

Question:

What is the volume of sensitive data processed or stored by the organization?

Dependency and Interconnectivity

3.1 Supply Chain Dependency

Question:

How dependent is the organization on its supply chain?

Consideration:

Are there critical components or services sourced from high-risk vendors or regions?

Data Sensitivity

2.1 Type of Data Handled



3.2 Interdependency

Question:

Is the organization part of a critical infrastructure network whose disruption could cascade to other sectors?

Cybersecurity Posture

4.1 Current Security Measures

Question:

What cybersecurity measures does the organization currently have in place?

Consideration:

Are they compliant with national and international standards?

4.2 History of Breaches

Question:

Has the organization experienced any significant cyber incidents in the past?

Consideration:

What was the impact?

Third-Party and Vendor Risks

5.1 Third-Party Management

Question:

Does the organization have a robust third-party risk management program?

5.2 Vendor Security Assessment

Question:

Are vendors and third parties assessed regularly for compliance with security requirements?

Resilience and Recovery

6.1 Business Continuity Planning

Question:

Does the organization have an established and tested business continuity plan?

6.2 Disaster Recovery Capabilities

Question:

What are the organization's capabilities for recovering from a significant cyber incident or physical disaster?

Compliance and Regulatory

7.1 Regulatory Compliance

Question:

Is the organization compliant with relevant sector-specific regulations?

7.2 Reporting and Transparency

Question:

Does the organization adhere to required reporting and transparency standards concerning cyber threats and incidents?

Risk Level Determination

High Risk:

Organizations that are critical to national security or public safety, handle large volumes of sensitive data, or have significant dependencies on potentially risky supply chains.

Medium Risk:

Organizations that have a moderate impact on the economy or public services and have implemented adequate but not comprehensive cybersecurity measures.

Low Risk:

Organizations that have minimal impact on critical services or infrastructure, face lower cybersecurity threats, and maintain good security practices.

Guidance for Regulators

9.1 Use of Checklist

Guidance:

Regulators should use this checklist during audits and assessments to determine the organization's risk level systematically.

9.2 Frequency of Assessments

Guidance:

High-risk organizations may require more frequent and detailed assessments compared to medium or low-risk organizations.

9.3 Tailored Regulations

Guidance:

Based on the assessment, regulators may need to apply tailored regulatory measures to ensure that higher-risk organizations meet stricter security standards.

Additional Questions for Specific Sectors

Note: Tailor additional questions to address unique sector-specific risks, such as energy source diversity for the energy sector or transaction security for the financial sector.

Energy Sector

10.1 Infrastructure Criticality

Question:

How critical is the organization's infrastructure to the national power grid or energy supply chain?

10.2 Regulatory Compliance

Question:

Is the organization compliant with national and international energy sector regulations (e.g., NERC CIP in the U.S.)?

10.3 Environmental Risks

Question:

Are there any environmental risks that could impact the organization's operational capabilities?

10.4 Energy Source Diversity

Question:

Does the organization rely on a single energy source, or does it have diversified energy sources that could mitigate supply disruptions?

10.5 Physical Security Measures

Question:

What level of physical security is in place to protect critical energy infrastructure from sabotage or terrorist attacks?

10.6 Cyber-Physical Systems Security

Question:

How are cyber-physical systems protected against potential cyber attacks that could cause physical disruptions?

10.7 Redundancy and Failover Capabilities

Question:

Are there adequate redundancy and failover mechanisms in place to ensure continuous operation during an incident?

Financial Sector

10.1 Compliance with Financial Regulations

Question:

Is the organization compliant with major financial regulations such as Basel III, Dodd-Frank, or local banking regulations?

10.2 Exposure to Financial Crime

Question:

What measures are in place to prevent exposure to financial crimes such as fraud, money laundering, and terrorism financing?

10.3 Data Breach Impact

Question:

What would be the impact of a data breach, especially regarding customer financial information?

10.4 Systemic Importance

Question:

Is the organization considered systemically important to the financial stability of the country or region?

10.5 Investment in Cybersecurity

Question:

How much does the organization invest in cybersecurity relative to its size and the sensitivity of its operations?

10.6 Transaction Security Measures

Question:

What security measures are in place to protect transactions from cyber threats?

10.7 Audit and Control Procedures

Question:

How robust are the audit and internal control procedures concerning financial reporting and cybersecurity?

Guidance for Regulators

11.1 Sector-Specific Focus

Guidance:

Regulators should use these questions to focus their assessments on the unique aspects of each sector.

11.2 Risk Mitigation

Guidance:

Responses to these questions can help identify areas where risk mitigation measures are needed most urgently.

11.3 Regulatory Adjustments

Guidance:

Based on responses, regulators may need to adjust oversight intensity or focus, ensuring that organizations with higher risk exposures are more tightly regulated.

Adjustments and Highlights for Unique Sectors and Critical Infrastructures

12.1 General Provisions for Critical Infrastructure

Note:

This document serves as the baseline for cybersecurity across all critical infrastructures in Indonesia. While it provides comprehensive guidelines suitable for general application, specific adaptations and enhancements will be directed by sector-specific regulators.

Purpose:

These adaptations are necessary to address unique vulnerabilities and threats faced by critical infrastructures, ensuring both national security and public safety.

Additional Guidance:

Regulators will provide additional guidelines on aspects such as incident reporting, board involvement, and life safety protections tailored to the needs and risks of each sector.

Appendix J: Specific Cybersecurity Framework for Financial Institutions in Indonesia

1. Overview:

This annex outlines heightened cybersecurity expectations specifically for financial institutions in Indonesia, including banks, insurance companies, and fintech firms. It focuses on high-risk financial operations such as credit issuance, loan processing, and payment clearing systems.

2. Introduction to Cybersecurity Challenges in the Financial Sector:

The financial sector, pivotal to national and global economies, faces sophisticated cyber-attacks that threaten individual and institutional stability. This annex addresses these risks with sector-specific security measures.

3. Unique Cyber Threats to the Financial Sector:

- **Credit Card Fraud:**
High incidence of attacks targeting financial data to commit large-scale fraud.
- **Banking Fraud:**
Common use of phishing and malware to infiltrate systems and manipulate financial operations.
- **Targeted Attacks:**
High-risk of operations disruption and market manipulation, impacting trust and causing reputational damage.

4. Regulatory Perspective and Systemic Risk:

Emphasis on stringent cybersecurity protocols to prevent breaches and ensure financial stability, including compliance with international standards like PCI-DSS.

5. Corporate Governance:

- **Board of Directors and Senior Management:** Ensure comprehensive oversight and alignment with cybersecurity initiatives and financial regulations.
- **Chief Information Security Officer (CISO):** Develop and enforce cybersecurity policies, enhancing sector-specific threat awareness and preparedness.

6. IT Risk Management Framework:

Focus on identifying and mitigating risks associated with financial transactions, ensuring data encryption and secure processing.

7. Operational and Technological Controls:

Implement advanced cryptographic solutions to secure transactions and protect against breaches in critical financial systems.

8. Incident Management and Response:

Establish advanced monitoring and real-time response capabilities to protect financial assets and sensitive customer information.

9. Conclusion:

Adherence to these tailored guidelines is crucial for protecting the financial sector against unique cyber threats, maintaining consumer trust and financial stability.

Appendix K: Cybersecurity Framework for the Energy Sector in Indonesia

1. Introduction to Cybersecurity Challenges in the Energy Sector:

Recognizing the energy sector as a backbone of national economy and security, this annex addresses its unique cybersecurity challenges.

2. Unique Cyber Threats to the Energy Sector:

- Targeted Attacks on ICS: High risk to operational technology controlling energy generation and distribution.
- Ransomware and Insider Threats: Significant risks from both external attacks and internal vulnerabilities.
- Nation-State Attacks: Increasing concerns about external threats aiming to disrupt national infrastructure.

3. Governance and Regulatory Compliance:

Ensure alignment with national and sector specific cybersecurity regulations, emphasizing compliance and strategic security initiatives.

4. Risk Management Framework:

Detailed focus on asset management and risk assessment specific to OT and ICS environments, highlighting the critical nature of these systems.

5. Technical Controls and Security Measures:

Enhanced protections for network segmentation, ICS security, and physical and environmental controls to safeguard critical infrastructure components.

6. Incident Response and Business Continuity:

Develop comprehensive incident response strategies and business continuity plans to maintain operational integrity and energy production.

7. Training and Awareness:

Sector-specific programs to educate and prepare personnel for unique security challenges faced by the energy sector.

8. Conclusion:

This framework ensures the resilience of Indonesia's energy sector against evolving cyber threats, promoting security and reliability of critical energy infrastructure.

These annexes provide a detailed regulatory approach tailored to the specific needs of the financial and energy sectors in Indonesia, enhancing the overall cybersecurity posture and readiness of these critical areas.

Appendix L: Incident Response Policy Template

1. Introduction

This policy outlines the approach that institutions in Indonesia should take to effectively manage cybersecurity incidents.

2. Purpose

The purpose of this policy is to establish a structured framework for responding to cybersecurity incidents within critical sectors. It aims to define roles, responsibilities, and procedures to ensure a coordinated and effective response to incidents.

3. Scope

This policy applies to all institutions under the jurisdiction of Kadin in Indonesia. It covers all types of cybersecurity incidents, including data breaches, ransomware attacks, and system outages.

4. Definitions

- Incident: An event that violates an organization's security policies and could compromise the confidentiality, integrity, or availability of information systems.
- Incident Response Team (IRT): A designated group of individuals responsible for managing the response to cybersecurity incidents.
- Critical Systems: Systems that are essential to patient care and hospital operations, such as EHR systems, medical devices, and patient management systems.



5. Roles and Responsibilities

- Incident Response Team (IRT): Responsible for coordinating the response to incidents, including communication with stakeholders, containment, and recovery.
- Chief Information Security Officer (CISO): Oversees the incident response process and ensures compliance with regulatory requirements.
- IT Staff: Implement technical measures to contain and eradicate threats, and assist in the recovery process.
- Other Staff: Provide input on the impact of incidents on daily institutions activities and assist in prioritizing recovery efforts.

6. Incident Response Process

1. Detection and Reporting: All staff must report any suspected cybersecurity incidents immediately to the IRT.
2. Triage and Classification: The IRT will assess the incident's severity and classify it according to its impact on operations.
3. Containment: The IRT will implement measures to contain the incident, such as isolating affected systems and disconnecting infected devices from the network.
4. Eradication: The IRT will work to remove the threat from the affected systems using advanced forensic tools.
5. Recovery: The IRT will restore affected systems from secure backups, prioritizing critical systems essential to institutions activities.
6. Post-Incident Review: The IRT will conduct a review of the incident to identify lessons learned and update the incident response plan as needed.

7. Incident Reporting

- Internal Reporting: The IRT must document all incidents and report them to institutions leadership and the CISO.
- External Reporting: Significant incidents, such as data breaches, must be reported to regulatory bodies like Kadin and cybersecurity agency within the required timeframes.

8. Training and Awareness

All staff must undergo regular training on cybersecurity best practices and the incident response process. This training should include phishing simulations, tabletop exercises, and role-specific scenarios.

Appendix M: Incident Response Management based on the BSSN Regulation No.1 of 2024

According to the BSSN Regulation No. 1 of 2024, the incident response management consist of:

1. Cyber Incident Response Team

- a. National Cyber Incident Response Team
- b. Sectoral Cyber Incident Response Team
- c. Organization's Cyber Incident Response Team

This team is responsible to issue cybersecurity warnings, formulating technical guidelines for incident handling, issuing cybersecurity warnings; formulating technical guidelines for incident handling; recording all reported incidents/complaints and providing initial handling recommendations to affected parties; triaging incidents based on established criteria to prioritize response; coordinating incident handling with relevant stakeholders; and performing other necessary functions. These other functions may include: addressing vulnerabilities in electronic systems; handling digital artifacts; notifying about potential threat observations; detecting attacks; conducting cybersecurity risk analyses; providing consultations on incident handling preparedness; and/or raising awareness and concern for cybersecurity.

2. Cyber Incident reporting

- a. Complainant's contact information
- b. Cyber Incident description
- c. Chronology of Cyber Incidents
- d. Impact of attack

3. Cyber Incidents handling

a. Cyber incident response and recovery

A cyclical cybersecurity process that involves: preparing mitigation plans and recovery strategies for cyber incidents; analyzing and reporting on incidents when they occur; carrying out response and recovery actions to address the impact; and finally, improving security measures based on lessons learned to prevent future incidents.

b. Delivery of cyber incident information to related stakeholders

A cyber incident information should contain at least:

- i. Type of cyber incident indication
 - ii. Information distribution code
 - iii. Affected systems and/or assets
 - iv. Mitigation recommendations
- c. Dissemination of information

4. Cyber Incidents preparedness implementation

This regulates and mandates the electronic system operators including IIV providers, ministries, and agencies to have adequate preparedness in responding to the cyber incident. This involves:

a. Development of Cyber Incident Response Plans:

Aims to detail how to handle various types of incidents, outlining procedures, roles and responsibilities, necessary resources, recovery processes, and contact lists which must be regularly evaluated and updated.

b. Business Continuity Planning:

Aims to ensure that the operational side will not be disrupted through proper recovery strategies, timelines, resource allocation, and staffing needs.

c. Regular Drills and Simulations:

Aims to regularly test the response plan and business continuity planning which must be conducted at least once every two years.⁶³

⁶³ Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber, BSSN. (2024)

Kadin INDONESIA

Indonesian Chamber of Commerce and Industry

Jl. H. R. Rasuna Said Blok X-5 No.Kav. 2-3,
Kuningan, Jakarta 12950
www.Kadin.id