Opportunities at the Nexus of AI and Cybersecurity

August 2025

Southeast Asia
Public Policy Institute

This paper has been researched and produced by the Southeast Asia Public Policy Institute with support from Microsoft. The information and analysis presented are based on interviews with relevant stakeholders, publicly available information, and analysis by the authors. It does not represent the views of Microsoft. It is not intended to be an exhaustive review of policy, legislation, or regulation and should be used with due caution and consideration of its scope and limitations.

About the Southeast Asia Public Policy Institute

The Southeast Asia Public Policy Institute is a research institute based in Bangkok and Singapore, working across the region. Our mission is to support the development of solutions to the most pressing public policy challenges facing Southeast Asia in the 21st century. The Institute works on a range of issues across sustainability, technology, public health, trade, and governance.

We convene dialogues with stakeholders and decision makers to drive discussion on the challenges and opportunities facing markets in the region. The Institute draws on a network of in-market researchers, advisors, and partners to provide insights and recommendations for governments, policymakers, and businesses.

We collaborate with partners on projects to explore and drive discussion on policy challenges through:

- **Research and Policy Development**
  In-depth research providing insights and actionable policy solutions aimed at policymakers looking to move the needle on key issues.

- **Policy Dialogues and Roundtables**
  Present policy ideas and start a dialogue with the most relevant stakeholders holding the pen on policy development in markets across the region.

Contents

Introduction

Southeast Asia has evolved to become the world's fastest-growing digital economy and is due to surpass US$1trillion by 2030. To meet demand and take advantage of the efficiencies and opportunities that technology offers, companies across the region have digitalized rapidly, with billions of dollars invested in technology platforms, networking infrastructure, and digital transformation. Meanwhile, governments are also investing heavily in digitalization with ambitious goals such as Vietnam's aims for 80% of public services to be fully online by 2025, with 40% of adults using them.

Increasing Cyber Threat Volume and Cost

However, the rapid digitalization has come with an 82% increase in cybercrime and a doubling of successful cyberattacks between 2023 and 2024[1]. A string of high-profile cyberattacks have targeted government institutions, resulting in compromised personal data, financial losses, and threats to election integrity. In 2023, Southeast Asian businesses experienced an average of over 36,000 online attacks per day[2]. The average cost of a cyberattack, including data breaches, in the region was approximately US$3million[3].

According to the ITU's Global Cybersecurity Index 2024, many countries in the region—including Indonesia, Malaysia, Thailand, Singapore, and Vietnam—are rated relatively highly, all falling within Tier 1 performance. However, this impressive score may not fully reflect the reality, as many cyberattacks likely remain undetected[4]. The trend of increasing risk has incentivized both public and private organizations to improve cybersecurity measures, as well as motivating governments to reassess their approach to cybersecurity policy and cooperation at the regional and global level.

Changing Landscape – Rising Threat from Nation-State Actors

In addition to increasing volume and costs, the nature of the cyber threat landscape is changing too. Cyberattacks are no longer driven solely by criminals or criminal groups. Nation-state actors are increasingly adopting tactics traditionally associated with cybercriminals, and in some cases, even collaborating with criminal groups to further geopolitical objectives. This has led to a blurring of the lines between nation-state threats and financially motivated cybercrime, as state-affiliated actors may engage in espionage, financial theft, and destructive operations, often disguising their motives behind criminal fronts.

In recent years, there has been a growing number of targeted cyberattacks on critical infrastructure, defence systems, and political institutions across the Indo-Pacific region. Many of these incidents have been reported by affected countries as state-backed operations. These activities are often linked to key nation-state actors such as China and North Korea, and are designed to undermine democratic governance, gain military advantage, or exert economic coercion[5].

Other nation-state actors, including Russia and Iran, are also active in the cyber domain. Recent observations have noted that Russia has outsourced operations against Ukraine to cybercriminal groups, while Iran has conducted financially motivated campaigns targeting Israel. These examples of operation reflect strategic interests and broader geopolitical objectives[6].

Cybercriminals now operate with greater sophistication, leveraging a full spectrum of capabilities, including techniques learned or borrowed from nation-state entities. These challenges are amplified by the widening gap in cyber capabilities across Indo-Pacific countries, creating an uneven regional security environment. As a result, some states remain significantly more vulnerable to sophisticated and coordinated state-sponsored cyber operations.

Key Cyberattacks in SEA

Thailand

2022 TCAS Student Data Leak
Over 23,000 students' personal data from the 2021 admissions process was sold on the dark web

2023 9near Hacker Incident
Data of 55 million Thai citizens, including sensitive identification details were leaked

Vietnam

2024 Widespread brute-force attacks
Vietnam recorded nearly 20 million brute-force cyberattacks in 2024, or 37% of all such incidents in Southeast Asia

Singapore

2018 SingHealth data breach
Personal information of 1.5 million patients and recorded of outpatient dispensed medicines were stolen

Indonesia

2024 National Data Center Ransomware Attack
Disrupted hundreds of public services for several days, including airport immigration processes and online student registration

Malaysia

2025 Kuala Lumpur International Airport (KLIA) Ransomware Attack
An attack on KLIA disrupted flight information systems and check-in counters

Phillippines

2016 COMELEC Data Breach
Personal data of 55 million registered voters was stolen from the website of the Commission on Elections

2023 PhilHealth Ransomware Incident
The online system was shut down and personal data of over 13 million individuals have been compromised

The AI Factor

Like many emerging technologies, AI can be a double-edged sword. In cyberspace, while AI can serve as a powerful tool for defence, it also has the potential to significantly amplify the scale, speed, and sophistication of cyberattacks. In the hands of malicious actors—including nation-state operators—AI can automate complex campaigns, making them harder to detect, defend against, and recover from.

The most effective way to counter AI-enabled cyber threats is by leveraging AI itself; this approach is increasingly recognized by governments, regulators and industry. Many advanced cybersecurity tools now integrate intelligence to enhance their effectiveness in detecting and responding to today's increasingly complex attacks. To illustrate this more clearly, AI is also being used to enhance Security Operations Centre (SOC) performance. On average, it takes 277 days to identify and contain a breach, but by leveraging AI, defenders can significantly reduce this delay. A recent study found that security analysts using AI tools were 26% faster and 44% more accurate across all tasks[7].

However, there are significant practical and policy challenges to the adoption of cutting-edge technology solutions that will allow governments to keep their societies, economies and critical infrastructure safe. While national security policy is often conservative in nature, there is a growing need for an innovative approach to allow greater public-private collaboration.

Cloud as an Enabler of AI and Advanced Threat Defence

While AI holds significant promise in identifying and responding to cyber threats, its full potential can only be recognised when it operates on consolidated data. A unified data estate enables AI to analyse large volumes of security information, continuously refine its capabilities, and develop a more accurate understanding of emerging threats. This, in turn, ultimately enhances the precision and effectiveness of cybersecurity solutions.

It is no surprise that cloud-enabled AI plays a leading role in modern cybersecurity. With unified data stored in the cloud, AI can operate at greater speed and scale. Its threat detection capabilities are strengthened by its ability to identify novel, never-before-seen attacks through learning behavioural baselines and flagging anomalies. It also enables automated incident response, triggering defensive actions within seconds, far faster than any human analyst. Furthermore, cloud platforms support end-to-end orchestration of security across entire networks, ensuring that no component is left exposed when a new threat arises.

All in all, available data estate at single place like cloud is critical for AI-powered cybersecurity enhancement. In an environment where higher levels of security are increasingly essential, migrating organisational systems and critical infrastructure to the cloud allows institutions to better harness the full potential of AI and other emerging technologies.

Artificial Intelligence is Reshaping Cybersecurity Landscape

Threat Detection: AI leverages machine learning algorithms to analyze vast amounts of data and identify patterns that signal potential threats.

Automated Responses: AI can automate responses to cyber incidents, reducing the time it takes to react and minimizing potential damage.

Predictive Analysis: Predictive analysis involves using machine learning to forecast potential attacks, allowing organizations to bolster their defenses proactively.

AI gets smarter, faster, and stronger in the cloud

Benefits of Cloud in Enhancing AI for Cybersecurity Purpose

Scalability and Flexibility: Cloud computing provides the infrastructure to handle large volumes of data for AI-driven cybersecurity solutions.

Accessibility: Cloud enables AI to access comprehensive and up-to-date practices, reducing the risk of blind spots caused by fast-changing attack techniques.

Collaboration: AI can streamline the management of cloud resources and support end-to-end orchestration of security across entire networks.

Challenges to Enabling AI-enhanced Cybersecurity

There are a range of obstacles to the adoption of cloud-based AI-enhanced cybersecurity defence in the Southeast Asia region. The challenges fall broadly into five categories: fragmented domestic policy, limited international coordination, outdated technology, insufficient investment, and human capital.

FRAGMENTATION: Fragmented approach to digital policy

A fragmented approach to digital policymaking remains a significant barrier to the adoption of new technologies in Southeast Asia. In many countries, such as Indonesia and Thailand, multiple laws and regulatory bodies govern the same technology domains. This results in overlapping mandates, inconsistent rules, and limited coordination.

These fragmented structures create a complex policy landscape and lead to misalignment among regulators, which hinder the development of a supportive ecosystem. This fragmentation can also erode confidence among organisations, making them hesitant in deployment of cloud and emerging technologies due to uncertainty and confusion over existing regulations.

MOTIVATION: Barriers and a lack of incentives to the adoption of cloud technologies that would enable AI-driven cybersecurity defence

As previously discussed, cloud infrastructure is a critical foundation for harnessing the full potential of AI to enhance cybersecurity at both speed and scale. However, despite the introduction of supportive initiatives such as “Cloud First” across several Southeast Asian countries, actual adoption remains limited.

Regulatory uncertainty continues to discourage the use of cloud infrastructure and AI-driven cybersecurity solutions. In addition, a lack of awareness and a shortage of skilled professionals further hinder progress. Without strong incentives—such as tax relief, government subsidies, or clear digital transformation targets—many organisations still view cloud adoption as costly, risky, or unnecessary.

MODERNISATION: Bridging legacy systems and AI-driven cybersecurity

Even when laws and regulations are in place to support cloud adoption, implementation remains a major challenge, especially when integrating new technologies into existing systems. Across Southeast Asia, many government agencies and critical infrastructure operators, particularly in sectors such as finance and transportation, still rely on outdated and custom-built systems. These legacy systems often lack robust cybersecurity features and are inadequate to handle today’s sophisticated cyber threats.

Modernizing such systems is complex. Not only are they difficult to upgrade, but they are also frequently incompatible with new technologies. Integrating advanced AI tools or cloud-based security solutions can be costly and may still leave vulnerabilities in place.

CHALLENGE 4

FOUNDATION: Insufficient national investment in technology and human capital

Investment in AI-enabled cybersecurity remains insufficient across most of Southeast Asia. In 2025, only around 0.1% of the region's total GDP is expected to be spent on cybersecurity[8]. Moreover, most cybersecurity spending is concentrated in urban centres and the finance sector, leaving critical infrastructure and rural areas exposed.

The region also faces a significant shortage of skilled professionals in both AI and cybersecurity. High training costs, limited time, and the constant need to keep up with evolving technologies make it difficult to develop a workforce with advanced, hands-on experience. As a result, there is a widening gap between the region's cybersecurity needs and the available talent to support its digital transformation.

CHALLENGE 5

COORDINATION: Need for international coordination

Cyberattacks are inherently transnational, yet Southeast Asia's responses remain largely fragmented at the national level. Restrictive data policies and siloed data environments hamper cross-border threat intelligence sharing, weakening the region's ability to coordinate effectively against shared threats.

Meanwhile, international capacity-building efforts, such as the ASEAN-Japan Cybersecurity Capacity Building Centre, have seen uneven participation and impact. While some countries are advancing with comprehensive cybersecurity frameworks, others continue to lag behind, creating vulnerabilities that can be exploited by malicious actors.

International and Regional Coordination

Addressing cybersecurity challenges effectively requires cooperation beyond the national level. Cyberattacks are increasingly transnational, and attributing them to specific actors is often difficult, as attackers routinely mask their identities or disguise operations as hacktivist movements. This complexity calls for enhanced coordination among domestic agencies, regional institutions, and international partners to share resources, intelligence, and best practices.

To that end, while national-level progress is essential, Southeast Asian countries can also pursue regional collaboration when designing their national cybersecurity strategies. Aligning domestic frameworks with regional mechanisms will help facilitate seamless cross-border cooperation and response capabilities.

At the ASEAN level, member states can play a more collaborative role in building regional cyber resilience. Implementing the ASEAN Framework on Digital Data Governance is a vital step toward modernising cross-border data governance. It enables secure and trusted data flows, supports cloud adoption, and allows for exemptions on threat intelligence from restrictive localisation mandates—thereby enhancing regional cybersecurity readiness.

Strengthening and operationalising the ASEAN Regional Computer Emergency Response Team (CERT) is also critical. Real-time threat intelligence sharing, coordinated incident response, and joint cyber drills under the ASEAN Cybersecurity Cooperation Strategy will help bolster collective capacity and foster trust among member states.

Beyond intra-regional cooperation, partnerships with global stakeholders offer additional value. Institutions such as the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) provide technical training, knowledge exchange, and alignment with international standards. ASEAN could further institutionalise coordination by establishing dedicated subcommittees under the ASEAN Digital Ministers' Meeting (ADGMIN) or the ASEAN Working Group on Digital Data Governance to ensure policy alignment and sustained progress across all member countries.

Alternatively, rather than creating new bodies, there is potential to leverage existing ASEAN sectoral groups—such as those in finance, energy, and healthcare, which are particularly vulnerable to cyberattacks—to collaborate with the ASEAN Working Group on Digital Data Governance. Such cross-sector coordination could help develop shared best practices and strengthen regional cybersecurity resilience. Leveraging the ASEAN AI Safety Network to develop appropriate practices for applying AI in cybersecurity is also a valuable step toward establishing shared principles that ASEAN countries can adopt in their own policies and guidelines.

By integrating cybersecurity cooperation within countries' agenda, the region will be better positioned to counter cross-border cyber threats, support innovation, and build a secure digital economy.

Recommendations for Meeting the Challenge

This section outlines a set of high-level recommendations for all policymakers in the region to consider as a baseline for enabling AI-driven cybersecurity response to an evolved threat landscape.

Strengthening Cloud-First Policies for Scalable AI Cybersecurity

Adopting AI-enhanced cybersecurity tools begins with enabling the underlying infrastructure and technologies such as cloud computing. Recognising the importance of cloud across, many countries in Southeast Asia have already begun promoting its use, with initiatives such as Cloud First policies introduced as foundational steps.

Singapore stands out as a regional leader in cloud adoption. It launched its Cloud First Policy in 2018 and under this initiative, the country has successfully migrated over 80% of eligible systems to the Government on Commercial Cloud (GCC)[9], laying the groundwork for scalable AI deployment across the public sector. However, not all countries have reached this level of advancement.

For example, Thailand has introduced a Cloud First Policy aimed at encouraging cloud adoption within public agencies. Yet, the initiative has remained more of a symbolic declaration than a driver of tangible change. Implementation has been hampered by outdated regulations, rigid procurement processes, and low confidence among users, resulting in slow or limited progress.

To make meaningful strides, governments must prioritise the reform of legacy regulations that hinder cloud adoption, particularly data localisation laws that restrict the use of cloud infrastructure. These should be aligned with international standards and global best practices. In addition, public procurement processes must be modernised to provide easier access to cloud and AI-powered cybersecurity solutions. Building user confidence is equally important and can be supported through education and awareness-raising efforts about the security and reliability of cloud platforms.

By leading through these actions, countries can set a strong example that encourages private-sector adoption and supports the development of a broader, more resilient ecosystem for AI-enhanced cybersecurity.

Modernise Cyber Threat Assessment and Security Standards

In parallel with promoting cloud and AI adoption for cybersecurity, it is essential for countries to develop or update their national cybersecurity frameworks. These frameworks should align with international standards and adopt a risk-based approach to address evolving threats effectively.

Global standards such as ISO/IEC 42001 (AI management systems), ISO/IEC 27090 (AI cybersecurity controls), and the NIST AI Risk Management Framework (RMF) provide a strong foundation for this effort. By mapping national standards to these internationally recognised frameworks, countries can enhance cross-border interoperability, promote trust, and ensure focus on managing the most critical risks.

A risk-based approach is particularly important in identifying varying levels of

vulnerability across sectors. Critical infrastructure providers—such as those in finance, energy, and telecommunications—may require more robust security measures and advanced technologies. Risk assessments can support the prioritisation of security controls and the allocation of resources based on the severity of threats, moving beyond mere compliance with minimal legal requirements toward proactive risk mitigation.

Balance Security and Openness in Cross-border data Flow

In today's cloud-centric and AI-driven environment, rigid requirements for local data storage can hinder access to advanced cybersecurity tools and global threat intelligence. To maximise the benefits of digital innovation, data governance frameworks should be aligned with international best practices, allowing the storage and processing of most data—including non-sensitive government data—across borders.

Balancing between national security and digital sovereignty is indeed challenging. However, enabling cross-border data flows brings long-term advantages. Data localisation rules can be structured in a tiered manner. Highly sensitive or security-critical data, such as 'top-secret' information, may remain within national borders or be stored in dedicated systems. Meanwhile, most government data, which is typically less sensitive, can be securely managed through public cloud infrastructure or hosted abroad. The adoption of international data transfer frameworks can further support this approach by ensuring confidentiality, integrity, and compliance in cross-border data exchanges.

Singapore serves as a leading example. Its openness to data flows has facilitated higher levels of cloud and AI adoption, compared to other Southeast Asian countries with more restrictive policies. Without calibrated digital protection policies, the deployment of advanced technologies may become unnecessarily complex and costly—slowing progress in enhancing national cybersecurity.

Incentivise Investment in New Technologies

Government support should include targeted incentives to promote the adoption of advanced cybersecurity technologies, particularly cloud computing and AI-driven defences, across both the public and private sectors. This is especially important for state-owned enterprises (SOEs), financial institutions, and other critical infrastructure providers where the cost of adopting new technologies can be a major barrier.

Along with the cloud-first policy which mainly focuses on transformation in public sector, governments should also consider offering tax incentives, subsidies or low-interest loans to private-sector organisations investing in cybersecurity upgrades or cloud migration. In addition, government-backed funds or co-investment programmes can be established to support the development and deployment of innovative cybersecurity solutions. For example, grants could be allocated to projects implementing AI-based

threat detection or to startups developing advanced security tools.

Beyond financial support, technical assistance should be made available to critical infrastructure operators and SOEs to help them meet higher cybersecurity standards. By coupling mandates with incentives and capacity-building support, governments can ensure that key sectors are not left behind due to budgetary or capability constraints.

Greater adoption of cloud and AI technologies will not only strengthen cybersecurity resilience but also generate broader economic benefits through increased digital competitiveness and innovation.

Close the Talent Gap in Cybersecurity and AI

One of the most critical barriers to deploying advanced cyber defences is the shortage of skilled professionals. To build long-term resilience, countries across Southeast Asia must invest in human capital to support the development and deployment of AI-enabled cybersecurity. Comprehensive initiatives are needed to train the next generation of experts while also upskilling the current workforce in both AI and cybersecurity.

A range of approaches should be considered to meet the diverse needs and contexts of each country, including:

- Strengthening education systems by integrating cybersecurity and AI modules into school and university curricula.
- Providing vocational training and certification programmes to equip cybersecurity personnel with practical, job-ready skills.
- Establishing centres of excellence, laboratories, or academies in collaboration with universities and industry, through public-private partnerships. Singapore's CyberSG Talent, Innovation and Growth (TIG) Collaboration Centre serves as a leading example.
- Supporting hackathons, cybersecurity competitions, and innovation incubators to give students and professionals hands-on experience in tackling real-world AI and cybersecurity challenges.

In Southeast Asia, where MSMEs are key drivers of the economy, government support for skills development and professional training is essential. Given their limited resources, many MSMEs struggle to upgrade their cybersecurity capabilities. By taking a leading role, governments can help ensure these businesses are not left behind and that the country's cybersecurity development aligns with global standards.

By anchoring reforms in these areas, Southeast Asia can transform its fragmented landscape into a cohesive defence front against AI-driven cyber threats.

Country focus: Indonesia

Indonesia's digital economy is a lucrative, fast-growing market, driven by a young, digitally-savvy, increasingly online population. Cloud infrastructure now underpins essential services in Indonesia. The adoption of cloud technology in immigration systems, digital education platforms, and the administration of the national universal healthcare programme is helping to drive the country's digital transformation agenda. While Indonesia does not formally designate its approach as a "Cloud First Policy," as seen in countries like the Philippines or the UK, the government has introduced a range of policies and regulations that actively support cloud adoption. This is particularly evident in the public sector, where digital transformation efforts align closely with the principles of a cloud-first strategy.

However, high-profile cyberattacks targeting government institutions and citizen data have raised concerns over the security of cloud infrastructure. Longstanding gaps in data protection and weaknesses in cybersecurity have increased anxiety at the same time as AI has made the cyber threat more sophisticated.

In response, the government has attempted to strengthen its cybersecurity posture with a new cybersecurity law in the pipeline that will strengthen the position of National Cyber and Crypto Agency (BSSN) and active sector regulation particularly in the fintech space. The government has maintained an open approach to coordination with the private sector, including international service providers, acknowledging expertise in areas such as AI and cybersecurity.

Cloud adoption among companies has accelerated for a variety of reasons, one of which is the enhanced security of digital credentials—as cybersecurity becomes increasingly critical in the face of expanding digital footprints, especially in the financial sector. Reflecting this trend, the country's cloud computing market has grown at a compound annual growth rate (CAGR) of 48% over the past five years.

However, Indonesia's ability to fully leverage cloud technologies is constrained by data localization requirements in certain sectors, complex cybersecurity standards, and overlapping policies and regulations issued by various ministries and agencies. Furthermore, government budget efficiency policies have discouraged agencies from investing in new technologies.

Key Organizations

Indonesia's cybersecurity policy is driven by a host of government ministries and agencies:

National Cyber and Crypto Agency (BSSN)
Oversees national cybersecurity policy and action, though limited enforcement authority

Ministry of Communication and Digital Affairs (KOMDIGI)
Oversees digital services, technology, and data management policies

Ministry of State Apparatus and Bureaucratic Reform (PANRB)
Coordinates GovTech; limited supervision authority over implementation

Financial Services Authority (OJK)
Financial regulator

Bank of Indonesia (BI)
Regulates and supervises banking and payment systems

Ministry of Industry
Oversees policies and regulations related to local content requirement (TKDN) and industrialization

National Research and Innovation Agency (BRIN)
Government science and tech agency for research and development

Coordinating Ministry for Politics, Security, and Legal Affairs
Coordinating role for Komdigi, BSSN, and Ministry of Defense, as well as supervising government control over cyber resilience, security, and data protection

Current Policy Landscape

Indonesia does not have a single dedicated cybersecurity law, but several laws and regulations contain provisions on cybersecurity and support cybersecurity governance and preparedness. Indonesia also has yet to issue any dedicated laws or regulation on AI, though it does have an AI National Strategy 2022-2045 outlining a vision for AI development and priority sectors.

Several other pieces of legislation cover issues such as data protection, electronic transactions, and risk management in the context of cybersecurity and AI implementation. In particular, the Personal Data Protection Law (27/2022) and KOMINFO Regulation (20/2016) regulate the collection, use, disclosure, and other processing of personal data by international organizations and governmental and private entities. The EIT Law and its implementing regulations require electronic operators that use AI to register as electronic system operators, subjecting them to the government's Circular 9/2023 on the Ethics of AI Use.

KOMDIGI Regulation 5/2025 on Public Electronic Systems Providers (ESPs) permits all government data classification (open, limited, and closed data) to be stored through third-party providers, although closed data

is only allowed if the system is hosted in a government-owned data centre. Sector-specific regulations also govern cybersecurity and AI adoption on issues such as payment systems, fintech, and banking, maintaining issues including AI audits and that systems much be supported by reliable technology and data security must be routinely monitored.

The financial regulator (OJK) and the central bank (BI) have been active in regulating for cybersecurity for financial service institutions. In 2022, OJK issued new regulations for better cyber resilience in the financial industry, requiring commercial banks to identify cyber risk by undergoing a series of assessments and processes on an annual basis, in addition to reporting any cyber incident to OJK and setting up a new cybersecurity structure. In 2024, BI introduced a regulation addressing cybersecurity and resilience in the national payments system. In April 2025, OJK published a new guideline on AI governance for the banking industry [10], ensuring the responsible development and implementation of AI technologies, including cybersecurity resilience.

Policy in the Pipeline

Cybersecurity regulation continues to be an active area, with the government drafting a Cybersecurity and Resilience Law (RUU KKS) to address gaps in the regulatory framework. The RUU KKS seeks to establish a comprehensive legal framework for national cybersecurity and resilience. It is expected to serve as the cornerstone of Indonesia's cybersecurity policy by defining the government's responsibilities, outlining a national strategy, safeguarding Critical Information Infrastructure (IIK), and strengthening inter-agency coordination. Notably, the draft law also marks a promising step in preparing the country to address cybersecurity-relevant AI applications.

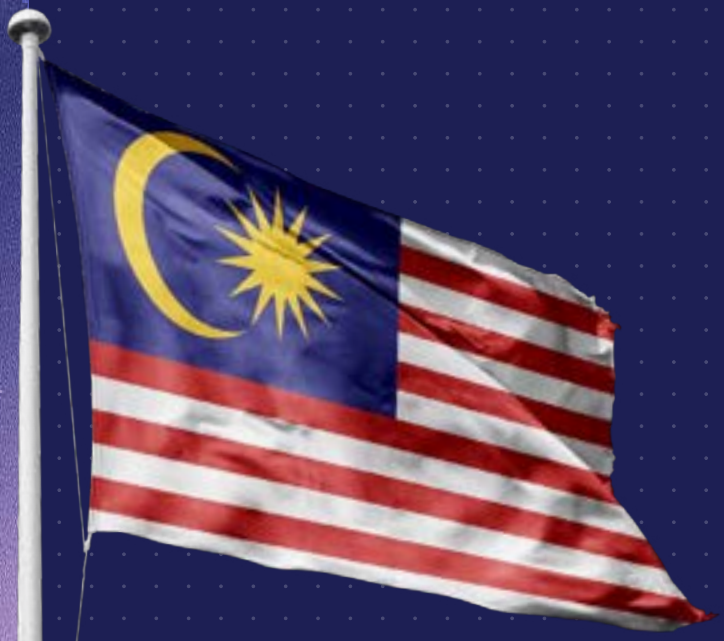
There are other significant developments in the pipeline including:

- The finalisation of Indonesia's AI roadmap for AI development and governance, and the upcoming Presidential Regulation on AI
- Implementing regulations on the Personal Data Protection Law
- Consolidated regulations on e-government, digital transformation, and tech procurement

Policy Recommendations

Regulations in Indonesia, particularly those related to data localisation, continue to constrain cloud adoption and limit the broader application of AI in addressing cybersecurity challenges. There is a clear need to ease overly restrictive rules, especially in sectors that are prime targets for cyberattacks. Beyond simply clarifying and streamlining regulations, greater alignment is also essential, as multiple agencies and overlapping frameworks currently shape the cybersecurity landscape. A centralised and coherent policy framework is needed to reduce complexity and ensure a smoother pathway for technology and cloud adoption.

Country focus: Malaysia



Malaysia has set an ambitious goal to become a leading regional cloud and digital hub by 2030. Amid the rapid development of Malaysia's digital sector and growing foreign investment in the tech and digital sectors, the government recognizes the importance of data protection and digital infrastructure security in enhancing Malaysia's global competitiveness. While Malaysia is more 'online' than many of its neighbours, legislation around cybersecurity and data protection is still undergoing further refinement via guidelines to clarify implementation and enforcement.

As with other countries in the region, several ministries and government stakeholders oversee different aspects of digital governance, leading to fragmentation. There is still room for improved regulatory clarity by building on existing data classification frameworks in the public sector, offering more detailed guidance on managing digital data and workloads, particularly for agencies that are less familiar with these processes.

However, the situation may improve following the Cyber Security Act 2024, and the existence of both technical and policy-focused cybersecurity agencies is an asset. Furthermore, new AI guidelines address the ethical and responsible use of AI across sectors while integrating AI into cybersecurity strategies to secure critical infrastructure. The National AI Office will likely play a key role in advancing AI adoption and promoting its integration into cybersecurity policy.

Despite rapid advancements in the AI landscape, leveraging AI-enabled cybersecurity remains challenging. Awareness of cloud-based solutions is still limited, particularly in the public sector and certain regulated industries, where there is a stronger preference for on-premise systems. This is often due to a lack of familiarity with the security advantages of cloud infrastructure and its potential to significantly enhance cybersecurity capabilities.

Key Organizations

Ministry of Digital
Spearheads the national digitalisation agenda, regulation and infrastructure

CyberSecurity Malaysia (CSM)
Technical agency under the digital ministry

Department of Personal Data Protection (JPDP)
Primary data protection regulator

National Digital Department (JDN)
Responsible for public sector digital transformation

National Artificial Intelligence Office (NAIO)
Agency responsible for AI policy

MyDIGITAL Corporation
Strategic change management office' for digital economy

National Cyber Security Agency (NACSA)
Serves as the authority under the Cyber Security Law and develops national cyber policies and strategies

Malaysian Communications and Multimedia Commission (MCMC)
Sector regulator

Chief Government Security Office (CGSO)
Protects national assets against security threats

Current Policy Landscape

Malaysia has history of digital strategies to implement a modernising vision covering both private sector development and the digitalisation of public service delivery dating back to the late 90s. A 'cloud first' policy was adopted under the Public Sector ICT Strategic Plan 2016-2020. Building on a cybersecurity strategy from 2020-2024, Malaysia issued a **Cyber Security Act in 2024 to strengthen the country's cybersecurity framework through a comprehensive legal foundation for addressing cyber threats.** The Act establishes the National Cyber Security Committee (NCSC) to coordinate cybersecurity strategies, expands the powers of the National Cyber Security Agency (NACSA), and requires specific cybersecurity protocols for National Critical Information Infrastructure (NCII). Together, these bodies oversee the implementation of cybersecurity policies and ensure compliance. Eleven sectors are considered NCIIs, each with a designated Sector Lead that oversees its respective cybersecurity component[11]. The Act also introduces obligations, such as mandatory risk assessments, incident reporting, and licensing requirements, for cybersecurity service providers.

In addition to the new cybersecurity law, there are various laws and regulations on data protection, risk management, and cybersecurity controls. The Personal Data Protection Act (PDPA) 2010 is the principal legislation governing all matters related to personal data, including data storage, data processing and personal data use – though it only applies to the private sector. Following the amendments made to the PDPA in 2024, the Personal Data Protection Department (JPDP) released seven additional guidelines to clarify further details about the amendments' implementation.

Relevant to cloud adoption are the Cross Border Data Transfers (CBDT) Guidelines. The CBDT Guidelines are meant to clarify the replacement for the PDPA's country whitelist system, which was removed to ease bureaucratic burden off JPDP. It is now contingent upon private players (or data controllers) to produce evidence that CBDT is necessary for operational continuity and that copies of Personally Identifiable Information (PII) of Malaysian citizens are stored in countries with data protection laws that are "substantially similar" or "ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the Act 709 (PDPA)".

Malaysia is recognised as a key regional destination for cloud services and data centres, with adoption growing in response to evolving policy requirements and increasing market demand. However, there is no clearly defined preference for a specific cloud architecture. At present, hybrid cloud appears to be the more commonly adopted approach. This trend aligns with Bank Negara Malaysia's Risk Management in Technology (RMiT) policy document[12], which encourages the use of hybrid cloud models to support broader adoption among regulated entities. This also reflects a perception gap within parts of the government, where hybrid cloud is considered more secure than public cloud, despite advancements in the security capabilities of public cloud platforms.

Policy in the Pipeline

2024 and 2025 was a significant period for digital policy development in Malaysia with the setting up of several major policy bodies. The cybersecurity law established a National Cyber Security Committee, chaired by the Prime Minister, to monitor progress on the Act's implementation.

In late 2024, the government launched the National AI Office (NAIO) which will play a major role in shaping national AI policy. The office has numerous deliverables for its first year of operation, including the development of a code of ethics, an AI regulatory framework, and a five-year AI technology action plan.

In February 2025, the Public Sector Artificial Intelligence (AI) Adaptation Guidelines were launched by the National Digital Department (JDN) in collaboration with the Malaysia Digital Economy Corporation (MDEC). The guideline aims to promote responsible and ethical AI adoption across the public sector.

In the following month, National Cyber Security Agency (NACSA) unveiled the National Cyber Crisis Management Plan (NCCMP), which outlines strategies and recommendations for National Critical Information Infrastructure (NCII) in the event of a cyberattack. The NCCMP has not been disclosed to the public as of May 2025, and is disseminated to Sector Leads and NCII entities. The plan will serve as the main guide for relevant entities to develop their own Standard Operating Procedures (SOPs) to address cyber crises, and includes detailed procedures for detection, response, communication, and coordination under a cyber crisis.

NACSA is also in the process of drafting the Cyber Security Strategy 2025-2030, which will serve as a framework to guide national cybersecurity strategies and initiatives. Quantum cryptography and computing will likely be a component of the strategy, especially as NACSA and the Digital Ministry have indicated that it will be a focus on both the national and regional level. Over the past two quarters this year, NACSA established the Malaysian Cryptology Technology and Management Center (PTPKM) and held meetings to draft the National Cryptography Policy and Strategic Implementation Plan 2025–2030.

Policy Recommendations

Malaysia has made strong progress in developing regulations to support cloud adoption, particularly as the country positions itself as a regional data centre hub. While the regulatory framework and broader ecosystem are generally conducive to cloud adoption, user perspectives remain varied. Some public agencies and regulatory bodies continue to favour on-premises or hybrid cloud solutions, often based on the belief that these models offer greater security than public cloud platforms. This reflects a gap in understanding. Addressing this perception gap through targeted education and awareness efforts could help build confidence and encourage wider adoption of cloud technologies, ultimately unlocking greater potential for AI-driven cybersecurity.

Additionally, as Malaysia continues to make progress in AI development, there is also an urgent need to expand the talent pool to support this transformation. The government should prioritise the development of skilled professionals through education, training programmes, and upskilling or reskilling initiatives.

With increased cloud adoption among organisations and a growing pool of skilled professionals to support its use, Malaysia has the potential to become a leading example of best practice in the region.

Country focus: Philippines

Cybersecurity remains a top-of-mind issue for the Philippines due to the country's limited cyber capabilities, which have recently come to light following high-profile cyberattacks on government institutions.

The government generally remains supportive of maintaining an open and enabling data policy environment to allow free flow of cross-border data. There was a feint towards an inward-looking protectionist data regime in 2023 during a failed proposal to introduce a data localization mandate. This policy direction continues to evolve. For instance, the Konektadong Pinoy programme includes provisions related to data localisation, and future legislation may incorporate broader data sovereignty measures. These developments warrant close monitoring, as they could significantly influence the country's digital and cybersecurity landscape.

The Philippines does not currently impose broad data localisation requirements, applying restrictions only to specific types of government data. This relatively open regulatory environment supports promising growth in cloud adoption. While there is no specific policy framework for enhancing cybersecurity, there is a growing recognition amongst government stakeholders and regulators on the need to strengthen the Philippines' cybersecurity posture, particularly following high-profile cyberattacks and threats as well as disinformation affecting election integrity. Meanwhile, local businesses have spoken about the necessity of involving AI in cybersecurity measures in the country, in recognition that threats are getting more sophisticated.

However, integrating AI into cloud-based cybersecurity solutions remains challenging due to the slow pace of AI adoption and related policy. Although several AI-related bills have been proposed, the Philippines still lacks

a concrete legal framework to guide AI deployment, and it remains uncertain whether these legislative efforts will progress under the 20th Congress. If regulators continue to view AI primarily as a threat, the application of AI across technologies, including cloud, will remain limited. Strengthening the broader digital ecosystem, beyond just cybersecurity and cloud infrastructure, is critical for enabling the country's long-term resilience and innovation.

Key Organizations

Department of ICT (DICT)
Primary digital policy, planning, coordinating entity and cybersecurity

Department of Science and Technology (DOST)
Leads the development of the national AI strategy and ensures that AI systems are ethically guided and deliver positive social impact

Department of Trade and Industry (DTI)
Establishes the Center for AI Research (CAIR) to promote AI innovation and support its application in addressing societal and industrial challenges transformation

National Cybersecurity Inter-Agency Committee (NCIAC)
Coordinator of cyber policies

Office of Cybercrime (OOC), Department of Justice
Handles cybercrime incidents

National Privacy Commission
Conducts compliance checks and investigates cybercrime

Current Policy Landscape

The National Cybersecurity Plan (NCSP) (2024-2028), developed by the ICT Department, addresses growing cybersecurity challenges and aims to build cybersecurity resilience through government, private sector, and international partnerships. It aligns with the Philippine Development Plan (PDP) (2023-2028) and focuses on three main outcomes: proactive protection and security in cyberspace; increased cybersecurity workforce capabilities; and strengthened cybersecurity policy framework.

Complementary to the NSCP, the Financial Services Cyber Resilience Plan (2023-2028) was released by the central bank to outline how the financial sector will deepen its cyber resilience and maturity. Some provisions include establishing baseline industry incident response plans; developing scenario-based incident response playbooks; and conducting industry-wide cyber testing exercises.

However, the Philippines does not yet have a dedicated cybersecurity law, relying on various rules and regulations governing cybersecurity— including but not limited to laws relevant to data protection, financial transactions,

and cybercrime. The Cybercrime Prevention Act 2012, for instance, aims to address legal issues concerning online interactions and the internet in the Philippines. It also ensures data security by codifying cybercrime and standardizing penalties. Meanwhile, the Data Privacy Act of 2012 regulates the rights of data subjects and privacy.

In 2017, the DICT adopted a Cloud First policy through Circular 2017-022, which encourages government agencies to embrace cloud computing and move away from siloed systems. However, data classification continued to play a critical role in this policy, often limiting the ability of government agencies and organisations to fully maximise the benefits of cloud adoption. In 2023, the Department affirmed that it would actively address the risks and vulnerabilities related to the adoption of cloud for data storage and processing, introducing modifications to the original cloud-first policy.

Policy in the Pipeline

A multi-sectoral coalition, supported by key government agencies and stakeholders, is developing a framework that would promote an open access regime for data transmission in the country. The proposed legislation, called the Konektadong Pinoy Act, would look into removing barriers to competition in the data transmission services.

The DICT has also advocated for the passage of a comprehensive law on cybersecurity that would also include language on critical information infrastructure protection, though this has yet to make strong progress in Congress. If enacted, the bill would empower a national regulatory body to oversee all matters related to cybersecurity, classify CIIs, and enforce baseline security requirements for their operators.

Policy Recommendations

The Philippines benefits from less restrictive regulations on data localisation than many of its ASEAN neighbours, making cloud adoption for AI-enabled cybersecurity more feasible than in many neighbouring countries. Policy efforts should now focus on accelerating adoption by encouraging both public and private organisations to embrace cloud technologies. A variety of incentives, both financial and non-financial, could be introduced to support this effort.

The Philippines must take a holistic approach by focusing on the entire ecosystem including cybersecurity, cloud, and AI. Greater emphasis should be placed on the development and promotion of AI to ensure readiness for AI-enabled cybersecurity. Building human capital is equally critical, particularly professionals capable of leveraging AI and cloud technologies for cybersecurity purposes. By training and upskilling citizens to become AI or cloud professionals, the country can accelerate its digital transformation and strengthen its resilience against emerging threats.

Country focus: Vietnam

Vietnam is actively promoting international engagement in its digital economy. The government has lifted the foreign ownership cap for data centres and invited global tech players to establish AI centres in the country. Under Resolution No. 57-NQ/TW, Vietnam has set a strategic goal to become a science- and technology-led nation by advancing secure digital infrastructure and modernising legal frameworks to support innovation, research, and technological development. With ambitions to develop its networks and cloud infrastructure to meet international standards, Vietnam is accelerating its digital growth.

However, this expansion also brings increased cyber vulnerabilities, including more sophisticated threats driven by AI—as demonstrated by the 2024 cyberattack on VNDirect. While the government has begun to prioritise cybersecurity, the country still lacks sufficient skills and capabilities, especially in harnessing AI for cybersecurity defence.

In particular, Vietnam recognises the cybersecurity challenges posed by AI. In 2024, it launched ACID 2024, an international cybersecurity exercise focused on responding to AI-driven cyberattacks. The government is also strengthening its cybersecurity framework by establishing new entities, including the National Cyber Security Association (NCA) and the Vietnam Computer Emergency Response Team (VNCERT), which coordinates national responses to cyber emergencies.

Like in other Southeast Asian countries, data localisation requirements in Vietnam are embedded across multiple regulations—including Decree 53, PDPD, and the new Law on Data. As a result, despite the country's welcoming stance on data centre and cloud investments, strict data localisation and personal data protection rules continue to hinder private sector participation in Vietnam's digital infrastructure, as well as the adoption

of cloud for cyber defence. Outbound data transfers face tight controls, leading to complex administrative procedures and disrupted data flows. In addition, ongoing government reforms may temporarily slow down policymaking, though they are expected to improve efficiency in the long term. The country still faces uneven digital infrastructure distribution and a shortage of skilled professionals in tech and cybersecurity.

Key Organizations

Ministry of Public Security (MPS)
The main authority behind cybersecurity and data regulations. It typically follows a conservative, security-first approach to policymaking

Ministry of Science and Technology (MST)
Leads the development of the Digital Technology Industry Law, Vietnam's first legislation outlining a regulatory framework for AI

Current Policy Landscape

Vietnam's digital policies are economically ambitious. The National Digital Transformation Program sets development goals for 2025, covering digital adoption across households and the private sector. The Central Steering Committee for the Development of Science, Technology, Innovation and Digital Transformation is also a key driver in the country's vision to become a hub for digital technology industries.

Vietnam is stepping up its efforts in the cybersecurity space. Significant legislation—such as the Law on Cybersecurity (2018) and the Personal Data Protection Decree (PDPD, 2023)—has been enacted. To operationalise the Cybersecurity Law, Decree No. 53/2022/ND-CP was issued, outlining provisions that apply to both local and foreign entities, including a dedicated chapter on data localisation requirements. Additionally, the Law on Personal Data Protection passed on June 26 introduces data privacy requirements for several sectors deemed susceptible to personal data infringement risks, including cloud and AI. While governance used to remain fragmented across multiple laws and agencies, MPS has acquired cybersecurity portfolio from the Ministry of Information and Communications (now merged with MST) since early 2025.

Taken together, these regulations shape Vietnam's approach to cloud computing, which is heavily influenced by strict data localisation obligations. The Law on Cybersecurity and Decree No. 53 impose stringent requirements on where and how data must be stored, creating substantial barriers for international cloud providers and AI companies seeking to operate in Vietnam. This centralised control over data flows may hinder the country's broader digital innovation goals.

Policy in the Pipeline

In November 2024, the National Assembly of Vietnam passed the Law on Data (Law No. 60/2024/QH15)—the country's first comprehensive legislation on data governance. Scheduled to take effect on July 1, 2025, the law covers a wide range of issues, including data processing, data classification, and the establishment of a National Data Center and National Database. Complementary regulations under the Law on Data are also being developed, particularly concerning cross-border transfer of data (i.e. core and important data).

The recently adopted Law on Digital Technology Industry (DTI Law) is expected to establish a broad regulatory framework for digital activities and define categories of AI systems—high-risk, high-impact, and standard. Further risk-based requirements for AI systems will be specified under forthcoming subsidiary regulations guiding the DTI Law.

Policy Recommendations

Vietnam faces significant barriers to effective cloud adoption – which would enable AI-enhanced cybersecurity – due to stringent data-related regulations and these challenges are likely to persist. The country would benefit from clearer guidance on permissible cross-border data transfer mechanisms. Adopting widely recognised international standards or implementing a risk-based approach that distinguishes between sensitive and non-sensitive data could help reduce unnecessary compliance costs while still safeguarding national security.

Country focus: Singapore

Singapore has positioned itself as a regional leader in adopting cloud services and AI to drive economic growth and boost the resilience of its digital infrastructure. At the national level, the country is committed to advancing its AI capabilities and deepening collaboration with cloud service providers to create a conducive environment for digital innovation.

Additional approach further enables the rapid adoption of new technologies. In the AI space, the government promotes voluntary standards and provides clear guidance tailored to the needs of small and medium-sized businesses (SMBs). For cybersecurity and infrastructure resilience, the emphasis is on aligning with internationally recognised baselines, such as ISO 27001, rather than introducing overly complex or novel regulatory requirements for regulated entities.

This light-touch, standards-based regulatory approach has played a key role in fostering innovation and enabling the safe deployment of emerging technologies. In addition, the government has introduced a range of measures to incentivise secure cloud and AI practices, helping organisations better manage cybersecurity risks.

- **Leading by example**
  Recognising cloud computing's potential for boosting productivity and fortifying data against cyberattacks, the government has successfully migrated over 80% of eligible, less sensitive government systems and data to commercial cloud platforms by 2024 and introduced the Government on Commercial Cloud Plus (GCC+) in 2023 to allow more sensitive data to be hosted on commercial cloud.

- **Introducing Standards, Certifications and Governance Frameworks**
  In May 2024, the amended Cybersecurity Bill was passed, expanding the scope of the previous Act to include overseas systems and third-party vendors. The following year, Cyber Security Agency significantly expanded its Cyber Trust mark to explicitly cover cloud security and AI security. This certification provides a clear framework

for organisations to adopt secure cloud practices and responsibly implement AI in their cybersecurity defences. There are also talks to make these marks mandatory for vendors handling sensitive data or bidding for government contracts. In addition, Singapore has also developed a Model AI Governance Framework, Model AI Governance Framework for Generative AI, and an AI Verify toolkit to guide the responsible and ethical development of AI crucial in building trust in AI systems. At the sectoral level, the Monetary Authority of Singapore has introduced AI governance frameworks for the financial sector and committed funding to encourage the use of AI for fraud detection and cyber defence. Similarly, the Ministry of Health has promoted the AI in Healthcare Guidelines (AIHGle), focusing on the adoption of AI in the local healthcare sector. These initiatives reflect cross-sectoral collaboration and regulatory harmonisation within the country.

- **Financial incentives**
  The government has introduced a $150 million Enterprise Compute initiative to help businesses access AI tools, computing power and consultancy services by partnering with major cloud service providers. This lowers the cost barriers for companies like SMEs to adopt cloud-based AI solutions for applications including cybersecurity.

Key Organizations

Ministry of Digital Development and Information (MDDI)
Drives Singapore's digital economy agenda and sets the strategic direction to foster a trusted digital environment, which encompasses cybersecurity and AI.

GovTech
Agency under MDDI overseeing the Smart Nation initiative and public sector digital transformation. It is central to adopting cloud and AI within the government, developing the public sector's cybersecurity capabilities and managing digital infrastructure underpinning public sector cloud adoption.

Infocomm Media Development Authority (IMDA)
Agency under MDDI responsible for regulating AI governance, promoting AI adoption, overseeing digital infrastructure, and supporting the development of the tech industry

Cyber Security Agency of Singapore (CSA)
Lead agency under MDDI to safeguard Singapore's cyberspace. It formulates the nation's cybersecurity strategy, develops standards and protects critical information infrastructure

Monetary Authority of Singapore (MAS)
The first regulatory body in the region to introduce sectoral AI governance frameworks for financial institutions

Current Policy Landscape

Singapore has one of the most advanced legal and regulatory frameworks for cybersecurity and data protection in the region. The Cybersecurity Act establishes the core legal structure for national cybersecurity. Its 2024 amendments

significantly expanded the Act's scope to include foundational digital infrastructure services like major cloud service providers and data centres to enhance the government's ability to protect essential digital eservices, even those operated by the private sector in the cloud. The amendments also allow CSA to conduct audits, assess risks and enforce compliance for a broader range of entities deemed crucial to national cybersecurity.

The Personal Data Protection Act (PDPA) 2012 serves as the foundation of Singapore's data protection regime. The Personal Data Protection Commission continues to update its advisory guidelines to keep pace with new technological challenges including greater cloud adoption. Key updates in recent years have strengthened data breach notification requirements and increased financial penalties for breaches to deter inadequate data protection in cloud environments.

To respond to the growing reliance on cloud services, the Infocomm Media Development Authority (IMDA) published its Advisory Guidelines on Resilience and Security for Cloud Services and Data Centres in February 2025. While voluntary, the guidelines outline recommended measures for all cloud service providers and data centre operators in Singapore to strengthen the resilience and security of their services, with the aim of minimising disruptions and ensuring service continuity for cloud users.

Policy in the Pipeline

The Digital Infrastructure Act (DIA) is currently under review and will likely make legally binding elements of IMDA's Advisory Guidelines on Resilience and Security for Cloud Services and Data Centres. The Act aims to enhance the security and resilience of key digital infrastructure across sectors such as banking, transport, and digital identity. It will also establish baseline cybersecurity requirements and incident reporting standards. The Act is expected to be tabled by the end of 2025.

Policy Recommendations

Singapore is well-positioned to be a regional leader in Southeast Asia in enhancing cybersecurity through cloud adoption and AI. The nation's proactive approach, demonstrated by its National AI Strategy 2.0 (NAIS 2.0), the Cybersecurity Act's 2024 amendments, the expansion of the Cyber Trust mark to include Cloud and AI Security, and its aggressive government cloud migration to GCC+, provides a robust model.

Building on this, Singapore can champion regional alignment by sharing its expertise on cloud and AI security frameworks, strengthen cross-border cooperation and capacity building through initiatives like the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN Regional CERT, and actively promote cybersecurity and AI principles within regional initiatives like the Digital Economy Framework Agreement (DEFA) to ensure a more resilient digital future in the ASEAN bloc.

Country focus: Thailand

Thailand's Cloud First Policy has become a major catalyst for digital transformation, establishing cloud infrastructure as the foundation for enhancing public services and operational efficiency. As the public sector increasingly adopts cloud services, critical concerns around data localisation, sovereignty, regulatory compliance, and especially cybersecurity have come to the forefront. Cybersecurity is vital to ensure system trust and safety—both of which are essential for a secure, thriving digital economy. As Thailand continues its transition toward a more advanced digital landscape, robust cybersecurity measures are key to protecting sensitive data, maintaining public confidence, and supporting long-term economic growth.

Currently, there is no national-level strategy or official plan from Thai government agencies specifically focused on integrating AI into cybersecurity. The existing National AI Action Plan provides limited recognition of the importance of AI-enhanced cybersecurity and lacks concrete measures to support its advancement.

However, the National Cyber Security Agency (NCSA) has taken initial steps in this direction. It has developed security standards for cloud systems and is in the process of drafting AI Security Guidelines, which are being designed in alignment with international standards. These efforts can be seen as early steps toward integrating AI into cloud systems to strengthen Thailand's cybersecurity capabilities.

Despite Thailand's ambition to become a smart nation leveraging AI and cloud technologies, policy development in these areas remains fragmented. A wide range of government agencies and overlapping working groups are involved in shaping policy across cloud, cybersecurity, and AI. This fragmentation risks creating disconnects between the rapid advancement of technologies and the strategic direction needed to apply them effectively for national cybersecurity. To ensure smooth implementation and long-term resilience, regulatory alignment and cross-agency collaboration are needed.

Key Organizations

National Cyber Security Agency (NCSA)
Oversees cybersecurity policy development

Office of the National Digital Economy and Society Commission (ONDE)
Supports digital economy policymaking, including AI development and application

Electronic Transactions Development Agency (ETDA)
Promotes electronic transactions and supports AI adoption and governance in the public and private sector

Digital Government Development Agency (DGA)
Leads public sector digital transformation, including the Cloud First Policy and integration of AI into government services

Big Data Institute (BDi)
Executes open data and data analytics in the public sector

Current Policy Landscape

Thailand's 'Cloud First' policy is backed by Cybersecurity Standards for Cloud Systems which aims to reduce cybersecurity risks associated with cloud services used by government agencies, regulatory bodies, and critical information infrastructure (CII) organizations.

However, there appears to be a growing regulatory divergence in Thailand regarding data residency requirements. On one hand, the Personal Data Protection Act and the Cybersecurity Act and its implementation regulations, as interpreted by NCSA, allows for cross-border data transfers, provided that such transfers do not pose a threat to national security or public order. This suggests a relatively flexible stance on data residency for all CII sectors.

On the other hand, DGA's Cloud-First Policy is accompanied by a proposed data classification framework that appears to favour local data residency for a broad range of government data. This includes not only classified or sensitive data, but potentially also operational and administrative datasets.

These differing approaches may create uncertainty for government agencies and CII organizations, particularly in determining compliance obligations and infrastructure planning for AI adoption. Greater regulatory clarity and alignment will be essential to ensure that Thailand's digital transformation goals are met without compromising data security or operational efficiency.

Other sets of regulations and policies also govern cybersecurity in the country. The Personal Data Protection Master Plan (2024–2027) builds on the Personal Data Protection Act (PDPA) and seeks to use many methods to elevate Thailand's data protection standards to global levels. The recent Notification on Cloud System Cybersecurity Standards, issued by the NCSA in 2024, establishes a strong link between cybersecurity and cloud adoption. It sets out robust security measures for cloud systems used by government agencies and critical information infrastructure. In addition, Thailand's National Cloud Security Framework is announced by the NCSA in March

2028 to support the regulation by guiding strategic direction and promoting collaboration among stakeholders to create a more conducive and secure cloud ecosystem, ensuring that all organisations are adequately prepared before the regulation takes effect in 2027.

In the AI space, the National AI Committee has been established to steer Thailand's transformation through artificial intelligence. It has set ambitious goals: AI literacy for 10 million people, the training of 90,000 AI professionals, and the development of 50,000 AI developers within two years. AI development is also supported by the National AI Action Plan (2022–2027), which focuses on promoting AI ethics, strengthening AI infrastructure, fostering talent, supporting research and innovation, and increasing public awareness.

Policy in the Pipeline

Thailand is in the process of drafting its first law on artificial intelligence, aiming to support the adoption and regulation of AI technologies to enhance business competitiveness and economic development. The draft AI Principles Law was developed by ETDA with an aim to provide oversight while promoting responsible AI adoption. The direction of this law remains undecided, as it is still in its early stages and currently undergoing public hearing.

Meanwhile, the NCSA is strengthening Thailand's cloud security posture with a Cloud Center of Excellence (Cloud CoE) to promote best practices in cloud security and support capacity building across sectors. Meanwhile, the government is scheduled to officially implement its 'cloud first' policy through the Government Data Centre and Cloud (GDCC) system starting October 2025.

Policy Recommendations

Thailand is following a broadly positive trajectory in terms of cloud adoption, supported by its Cloud First Policy and openness to certain cross-border data transfers. However, a key challenge lies in the complex regulatory enforcement landscape, with multiple organisations involved—often leading to overlaps and inconsistencies. To optimise the country's capacity in cloud, cybersecurity, and AI, a more aligned and harmonised regulatory framework is needed.

Specifically, it is essential that data governance frameworks facilitate the cross-border flow and interoperability of both public and private sector data. National data policies should avoid imposing data localization requirements that hinder efficiency or technological progress. Instead, governments should prioritize enabling trusted, secure, and privacy-conscious access and application of data.

In addition, Thailand faces a shortage of skilled labour and professionals, which hinders organisations from effectively adopting or utilising emerging technologies. Concrete and consistent long-term measures are required to strengthen the talent pipeline and support sustainable digital transformation.

Notes

[1] https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-southeast-asia W

[2] https://www.asiapacific.ca/publication/southeast-asia-cyber-threats-and-opportunities-canadian-co

[3] https://www.atlas-mag.net/en/category/tags/focus/cost-cyberattacks

[4] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[5] https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Indo-Pacific-Cyber_JUNE-2025-final_2025-06-23-224311_elho.pdf

[6] https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[7] https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[8] https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-in-asean/files/assets/common/downloads/publication.pdf

[9] https://govinsider.asia/intl-en/article/the-road-to-cloud-how-singapore-government-achieved-its-ambitious-goals

[10] https://ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Pages/Tata-Kelola-Kecerdasan-Artifisial-Perbankan-Indonesia.aspx

[11] These sectors are government; banking and finance; transportation; defence; national security; information, communication and digital; healthcare services; water, sewerage, and waste management; energy, agriculture and plantation; trade, industry, and economy; and science, technology, and innovation.

[12] https://www.bnm.gov.my/documents/20124/938039/PD-RMiT-June2023.pdf