Deloitte.

Centre for
Regulatory Strategy
Asia Pacific

Safeguarding Cybersecurity in AI:
Building Resilience in a New Risk Landscape

December 2025

Navigating the Report

Click icon to navigate to the relevant section

Introduction

Artificial intelligence (AI) is reshaping the cybersecurity landscape across Asia Pacific (AP).

Even before the rise of advanced AI, the increasing digitisation of business operations had already made cyber-attacks more frequent, scalable and effective. AI is now amplifying this trend by enabling malicious actors to work more quickly and produce more convincing and adaptive attacks. For example, AI can help generate persuasive phishing messages and deepfakes, analyse systems to identify weaknesses, and adjust attack methods in real-time. This lowers the barrier for attackers and increases both the speed and potential impact of a cyber incident.

As organisations adopt AI across core processes, the attack surface is also expanding. AI introduces new systems and data flows into technology architecture, including model training environments, automated decision workflows and large-scale data pipelines. These components can potentially create additional points where vulnerabilities may arise. Further, the AI systems are also subject to attack. Adversaries may try to corrupt the data used to train models, influence or distort model outputs, or exploit weaknesses in how the systems interpret and respond to user inputs.

These threats create clear business risks. AI-related cyber incidents can cause financial losses, compromise intellectual property, distort critical decision outputs, expose sensitive customer data, and erode organisational reputation and stakeholder trust. Therefore, as AI adoption grows, it is critical that risks must be assessed and managed as part of a wider cyber defence strategy.

However, despite the potential risks, AI also provides opportunities to strengthen cybersecurity. AI-enabled tools can help organisations detect issues, improve the security of software and systems, and respond to incidents more quickly and consistently. Firms that combine these capabilities with strong governance and proportionate controls will be better positioned to manage the evolving cyber threat landscape.

Cybersecurity is now firmly a Board level responsibility. The additional risks introduced by AI make strong oversight, clear lines of accountability, and Board fluency in AI technology essential. These capabilities are needed not only to protect critical operations and meet regulatory obligations, but also to maintain customer and stakeholder trust.

This paper examines how AI is impacting cybersecurity risk, how supervisors in AP are responding and what organisations can do to build stronger and more resilient defences. It outlines key attack vectors, emerging regulatory expectations, and practical steps for Boards and senior executives to bolster their firm's cyber resilience.

Whilst this paper focuses on AI security considerations, it is important for firms to take a holistic view and address all AI-related risks when developing their technology strategy and AI systems.

AI Security vs. AI Safety

For the purposes of this report, we define AI security as the protections that keep AI systems resilient against attacks and misuse. This includes defending against adversarial inputs, tampered data, stolen models, and attempts to manipulate or extract model outputs.
We distinguish this from AI safety, which concerns how an AI system behaves such as its accuracy, reliability, fairness, and alignment with intended goals.

In practice, these two domains often overlap. Weak safety, such as a model that is brittle, poorly calibrated, or prone to hallucination can create openings that attackers can exploit. Conversely, a security failure like compromised training data or manipulated content can degrade safety by changing a system's behavior and eroding trust in its outputs.

This paper focuses on the cybersecurity risks associated with AI systems while recognising these risks can affect broader safety outcomes and vice-versa.

AI Cybersecurity

AI Cybersecurity Risks

As organisations begin to adopt and scale AI, malicious actors are evolving to target these systems. Some techniques such as prompt injections, jailbreaks and model extraction are relatively new and arise from the way AI models process data and instructions. Others, including supply chain compromise or the exploitation of vulnerable components, build on long standing cyber-attack methods. Nevertheless, the impacts are amplified by AI's reliance on external models, open source tools and complex data pipelines. The result is a broader and more dynamic attack surface that can impact the integrity, confidentiality and reliability of AI systems and the processes they underpin. Understanding these risks is an important first step in developing the security controls and monitoring mechanisms needed to keep AI systems safe.

The table below summarises some of the key security risks impacting AI systems.

Attacks on Model Behaviour

Attack Vector	What It Is	How Attackers Exploit It	Why It Matters
Prompt injections	Malicious or carefully crafted instructions inserted into prompts or contextual data that an AI model relies on to generate outputs. These instructions are often hidden within user inputs, documents, websites or datasets	Attackers trick the model into following unintended instructions by embedding commands in user text, metadata or external content pulled into the model's context. This can override intended logic and cause the model to behave unpredictably	Prompt injections can cause the model to disclose sensitive information, perform unintended actions, generate harmful or unauthorised outputs or undermine downstream automated processes that rely on model-generated content
Jailbreaks	Techniques that deliberately bypass guardrails and restrictions built into AI systems, allowing them to output content that would normally be blocked	Attackers chain prompts, use role play, disguise requests or create multi-step instructions that gradually weaken the model's guardrails until it produces restricted or inappropriate content	Jailbreaks expose firms to the generation of harmful, misleading or non-compliant outputs, which can create regulatory, ethical and reputational risks. They can also enable attackers to map weaknesses in a model's control framework
Adversarial prompts or examples	Inputs that have been subtly and intentionally altered in a way that misleads the model, even though the changes may be imperceptible to humans	Attackers adjust words, phrasing, images or data patterns so the model interprets them incorrectly. These manipulations exploit how models process and weight different features	This can cause models to misclassify or misinterpret information, resulting in unreliable decisions, manipulation of automated workflows or incorrect outputs in high-stakes environments such as fraud detection or content moderation

Attacks on Data and Training Pipelines

Attack Vector	What It Is	How Attackers Exploit It	Why It Matters
Data poisoning	The deliberate introduction of corrupted, biased or misleading data into training or fine-tuning pipelines. Poisoned data may look legitimate but is engineered to distort model behaviour	Attackers insert manipulated samples into data sources the model relies on, such as open datasets, web-scraped material or internal update pipelines. In some cases, attackers add ' trigger' patterns that cause the model to behave differently only in specific scenarios	Poisoning weakens model performance, embeds backdoors, creates systematic inaccuracies and erodes trust in the system. Poisoning attacks can be difficult to detect, and damage can persist across iterations of the model
Model inversion	A method of reconstructing sensitive information about the training data by analysing patterns in the model's outputs. Over time, attackers can infer details about the original dataset	Attackers issue repeated, carefully structured queries and analyse returned patterns to infer personal attributes, confidential information or proprietary training data	This can expose sensitive or regulated data, violate privacy obligations and allow attackers to build detailed profiles of individuals or datasets. Regulators increasingly view this as a significant compliance and confidentiality risk
Model extraction or theft	A process where an attacker replicates a model's functionality, logic or parameters by querying it repeatedly, effectively cloning the model without direct access to its code or training data	Attackers systematically probe the model's inputs and outputs, often using automated tools, until they can reproduce its decision boundaries or generate an equivalent model	This undermines intellectual property, reduces competitive advantage and enables malicious actors to deploy the stolen model for harmful purposes, including large-scale attacks or disinformation

Attacks on Supply Chain and Infrastructure

Attack Vector	What It Is	How Attackers Exploit It	Why It Matters
Compromised components or external models	Weaknesses or hidden risks in open-source software, shared libraries or pre-built AI models that an organisation downloads or integrates into its systems. These components may contain coding flaws or may have been tampered with before distribution	Attackers compromise popular open-source packages or pre-trained models so that any organisation that installs them unknowingly imports the attacker's code or manipulated model weights. This allows the attacker to spread malware or influence AI behaviour across many organisations at once	A single compromised component can affect every system that uses it, creating widespread and hard-to-trace vulnerabilities. Many organisations rely heavily on shared code and models, therefore an attack on one component can escalate into a broader systemic issue across sectors or regions
Compromised AI development pipeline	Attacks on the tools and systems used to build, test and deploy AI models. This includes code repositories, model storage locations and automated deployment tools	Attackers target the places where models are updated or stored, such as version-control systems or deployment scripts, and insert changes without detection. This can allow them to modify how a model behaves, disable key security checks or add hidden functions	This can result in corrupted models, unauthorised model updates, silent tampering or disruption of production systems. Because pipelines automate deployment, a single compromise can spread widely and rapidly
Third-party exploitation	Weaknesses in other companies' systems or services that the AI relies on for data, processing or functionality. These are often external tools that supply inputs into the AI system	Attackers take advantage of poorly protected interfaces with third-party services or manipulate the data being sent through these connections. In some cases, they intercept information or feed incorrect data into the system to alter outputs	Even if an organisation's own systems are secure, weaknesses in an external partner can create a pathway for attackers. This can result in data exposure, incorrect model outputs or disruption to business processes that depend on those external services

These attack vectors illustrate the AI cyber threat environment, and underscore the importance of robust security controls throughout the AI model lifecycle.

Supply Chain and Third-Party Risks
As highlighted above, third-party relationships and extended supply chains are a major source of cyber and AI-related vulnerability, particularly for firms in complex vendor ecosystems. Many incidents now stem from vendors and the AI capabilities embedded in the software and services they provide. As firms connect more tools and data pipelines, they can also be susceptible to weaknesses across this extended ecosystem. In practice, a company's attack surface therefore expands to include how its vendors design, deploy, and update AI.

Companies that utilise third-party infrastructure should be aware that vendor practices vary significantly. Some providers have mature governance and monitoring processes for their AI models; others are still developing basic policies and controls. Visibility into how vendors use data, train and update models, and respond to issues is therefore essential for understanding residual risk.

Contracts and operating terms need to reflect how AI features will evolve, how changes will be announced, and how incidents will be reported. Ongoing dialogue with key vendors especially around new features, model changes, and system updates is crucial to ensure systems remain secure and sensitive data is protected.

AI Security Trade-offs

Implementing cybersecurity measures for AI systems requires a careful balance between the performance and security of AI systems. Organisations must protect AI assets against increasingly sophisticated cyber threats, while recognising that greater security constraints can directly reduce the accuracy, adaptability, and overall utility of AI models. As AI becomes embedded in critical business operations and decision-making, the need for strong cybersecurity control is intensifying. In order to safeguard against key risks such as data poisoning, model theft and unauthorised access, firms typically deploy a range of controls. These security measures include encryption, access management, continuous monitoring and rigorous auditing of models and training data.

However, many of these protections come with performance trade-offs and can be resource intensive. Restrictive access to data, for example, can materially limit an AI system's ability to learn from diverse and representative datasets, reducing the robustness and accuracy of its outputs. Likewise, frequent authentication checks or highly segmented environments can introduce latency, disrupt real-time processing, and frustrate end-users who expect seamless interactions. Overly conservative policies can also stifle innovation by preventing teams from experimenting with new use cases or iterating models at pace.

A key consideration is the distinction between productivity tools (e.g., enterprise chatbots, research tools) and AI models that drive business decisions (e.g., decision-support algorithms, model-based risk engines). Productivity tools typically operate on lower-risk data and can therefore be deployed with lighter security controls without significantly increasing exposure. In contrast, decision-critical and customer facing AI models usually require more stringent protections due to the sensitivity of the underlying data and the potential impact of model compromise.

Applying a uniform, high-security posture across all AI tools can unnecessarily degrade performance and reduce business value, particularly for low-risk, high-volume productivity applications where usability and speed are essential. The challenge, therefore, lies in calibrating security frameworks to the risk profile and unique characteristics of each AI use case. Doing so allows firms to protect critical assets without constraining model performance or impeding business productivity.

AI-enabled Cybersecurity Capabilities

As cyber threats become more frequent and complex, organisations are increasingly turning to AI to strengthen their defences. When used appropriately, AI can automate routine tasks, detect suspicious activity earlier, and support faster more accurate incident response. These capabilities enhance both the efficiency and effectiveness of existing cybersecurity controls while helping firms scale their defences across a complex digital environment.

AI Enabled Solution	How does this Strengthens Cybersecurity
Threat Detection and Response	AI analyses network, endpoint, and user activity to identify anomalies and suspicious patterns that may indicate an emerging threat. It prioritises alerts and proposes likely causes, enabling faster and more targeted responses
Secure Code Development	AI reviews code for unsafe patterns and known vulnerabilities as it is written, reducing the likelihood of security defects entering production and lowering remediation effort
Secure Pipeline and Deployment Automation	AI predicts build issues and identifies configuration weaknesses before deployment. This helps ensure that only securely configured code progresses through the pipeline, reducing the risk of introducing vulnerabilities
Policy, Control, and Compliance Assurance	AI continuously checks systems against internal security policies and regulatory baselines, flagging deviations in real time. This reduces the risk of misconfigurations, weak controls, and audit findings
Incident Response and Monitoring	AI correlates and summarises large volumes of logs and telemetry to identify root causes more quickly. It automates parts of triage and supports more consistent remediation across teams
Software Supply-Chain Security	AI scans third-party components and open-source libraries to detect vulnerabilities, tampering, or unexpected changes. It helps firms manage dependency risks across increasingly complex software ecosystems
Security Testing and Vulnerability Management	AI identifies security-relevant code weaknesses, prioritises vulnerability remediation based on risk, and recommends where additional testing is needed. This enhances the robustness of preventive controls
Developer and Analyst Support	AI acts as an assistant that explains security issues in plain language, recommends remediation steps, and reduces manual effort across secure-coding and security-operations workflows
Architecture and Attack-Surface Management	AI evaluates system design and dependencies to highlight components that increase attack surface or introduce security fragility. It supports long-term planning for hardening and modernisation

AI is becoming an increasingly important enabler of modern cyber-defence. While these tools do not replace established controls or human judgement, they support more scalable and efficient security operations. As firms adopt AI-enabled capabilities, success will depend on embedding them within existing governance, risk, and assurance frameworks to ensure they enhance rather than complicate a firm's cyber defence strategy.

Deepfakes

Deepfakes are synthetic images, videos or audio recordings generated by AI to imitate real people with a high degree of realism. They can make it appear as though an individual has said or done something they never did, creating risks to information security, reputation management, and trust in digital communications.

Although deepfake techniques are improving rapidly, this is one area where effective mitigation is already achievable. Risks associated with deepfakes can be successfully mitigated by organisations which adopt robust cybersecurity controls that both detect and limit the spread of manipulated content. Advanced machine learning-based detection tools can analyse audio-visual cues and metadata to identify forged media, while digital watermarking and provenance-tracking technologies help verify the authenticity of files. These capabilities continue to mature and are increasingly being integrated into mainstream cybersecurity and content-verification tools. However, regularly updating these detection mechanisms is essential, as deepfake techniques continue to evolve.

In addition to technical solutions, implementing strict access controls and multi-factor authentication can reduce the likelihood of attackers obtaining original content to create convincing deepfakes. Security awareness training also plays a vital role; educating employees and stakeholders about the potential signs and dangers of deepfakes fosters a culture of vigilance. By combining sophisticated detection systems, access management, and ongoing awareness initiatives, organisations can significantly mitigate the cybersecurity risks posed by deepfakes.

Overview of the Regulatory Landscape

AI security is increasingly on the regulatory agenda across AP, driven by the growing frequency and severity of cyber incidents and the rising reliance on digital infrastructure across industries.

Authorities are responding by strengthening cyber-specific frameworks and embedding cyber security expectations as part of broader operational resilience or AI governance requirements. Nevertheless, the regulatory landscape across AP remains highly fragmented, with each jurisdiction crafting its own rules, definitions, and enforcement priorities.

Jurisdictions such as Australia, Singapore, Japan, China (Mainland) ("China"), South Korea, and India have enacted comprehensive laws to address cyber risks. However, there are significant differences in the scope, terminology, and enforcement mechanisms. For example, while Singapore's Cybersecurity Act focuses on the protection of "critical information infrastructure" and prescribes sector-specific obligations, China's Cybersecurity Law encompasses a broader range of sectors, and mandates localisation of critical data. Meanwhile, Japan's Cybersecurity Basic Act takes a more strategic, coordination-oriented approach.

This regulatory patchwork creates significant challenges for multinational firms that must ensure their cyber risk management frameworks are adaptable to differing local requirements. In addition, regulatory expectations are rapidly evolving in step with technological change, meaning firms must remain agile and vigilant to maintain compliance and avoid penalties or operational disruptions.

While most jurisdictions still rely on general cybersecurity frameworks to safeguard AI systems, regulators are beginning to introduce AI-specific security expectations. For example, some jurisdictions have introduced rules and guidelines aimed at model robustness, adversarial testing, secure data handling, and protections against model manipulation.

Mandatory Cybersecurity Standards and Incident Reporting

Across the region, there is a clear trend toward the imposition of mandatory cybersecurity standards, often with prescriptive controls and detailed incident reporting requirements. Singapore's Cybersecurity Act, for instance, requires designated critical infrastructure operators to implement approved cybersecurity measures, conduct regular audits, and report significant cyber incidents to the authorities, sometimes within as little as two hours of detection.[1] Australia's Security of Critical Infrastructure Act similarly compels operators to adopt rigorous risk management practices and notify authorities of cyber incidents within 12 hours in some cases. These obligations are not limited to technology firms; they extend to sectors such as energy, finance, healthcare, logistics, and telecommunications. Non-compliance can result in severe financial penalties, regulatory investigations, and public censure. The heightened focus on rapid incident disclosure has forced organisations to enhance their detection, response, and communication capabilities, while also navigating the complexities of reporting to multiple regulators across different jurisdictions.

Regulatory Scrutiny of AI Systems

As AI systems become integral to business operations, governments in AP are stepping up their scrutiny of AI deployment, particularly with respect to security, safety, and resilience. While binding AI-specific legislation is yet to be implemented in most regions, a growing number of soft law instruments and guidelines are shaping expectations. For example, Singapore's Model AI Governance Framework and the Infocomm Media Development Authority (IMDA) AI Verify Programme urge firms to adopt security-by-design principles, conduct regular testing for vulnerabilities, and build robust and resilient AI systems. Japan's AI Governance Guidelines similarly emphasise the importance of ensuring AI systems are resistant to adversarial attacks and manipulation. In South Korea, the Personal Information Protection Commission issued the Policy Direction on the *Safe Use of Personal Information in the AI Era* in 2023 which introduced principles-based regulations regarding privacy and security risks relating to AI systems.[2] Regulators are especially concerned about the use of AI in critical sectors such as financial services, healthcare, and transport, where errors or malicious interference can have severe consequences. The increasing regulatory focus on the security and reliability of AI systems means firms must establish rigorous governance and testing regimes for their AI assets and be prepared for greater oversight as legislation inevitably evolves.

Cross-Border Collaboration and Regional Initiatives

While national regulation remains the dominant force, there is a limited movement toward greater cross-border cooperation and harmonisation of cybersecurity and AI standards in AP. Initiatives such as the Association of Southeast Asian Nations (ASEAN) Cybersecurity Cooperation Strategy[3] are laying the groundwork for shared principles, best practices, and incident response coordination. The ASEAN-Japan Cybersecurity Community Alliance (AJCCA) in partnership with the Japan Network Security Association (JNSA) hosted the 2nd AJCCA Conference in October 2025 where a collaborative approach between ASEAN nations and Japan on cyber resilience was proclaimed to be key to counteracting growing cyber threats.[4] Collaboration such as this signals a recognition that cyber threats and AI risks do not respect borders and require collaborative solutions. For firms, this means staying alert not only to domestic regulatory changes, but also to developments in regional and international standards. Participation in cross-border and regional initiatives can offer firms early insights into emerging cyber threats and regulatory requirements and help shape future frameworks to be more aligned with business realities. Nevertheless, the lack of full harmonisation means that, for the foreseeable future, firms will continue to face the challenge of aligning their cybersecurity and AI governance with a series of overlapping, and potentially conflicting, rules and expectations.

Overlap with Data Privacy Regulations

As highlighted in our recent paper on safeguarding data privacy in AI[5], data privacy laws will have a significant impact on how organisations secure and govern their AI systems. For example, Indonesia does not have a standalone cybersecurity law, but cybersecurity provisions are included within the *Law No. 1 of 2024* on *Electronic Information and Transactions* (EIT Law) which is primarily focussed on data privacy. Other jurisdictions with dedicated data privacy and cybersecurity regulations will also see significant overlap. In Hong Kong, Data Protection Principle (DPP) 4(1) of Schedule 1 to the Personal Data (Privacy) Ordinance mandates that organisations must take "all practicable steps" to ensure that any personal data held is protected. This includes safeguarding against unauthorised or accidental access, processing, erasure, loss or use.[6] In a Guidance Note in 2022, the Privacy Commissioner for Personal Data detailed specific ICT measures to ensure the protection of such personal data in line with the definition of "all practicable steps".[7] These two examples demonstrate how there is an intrinsic link between cyber security and data privacy and regulators across AP have put in place strong obligations with respect to securing personal data.

Further, the introduction and strengthening of requirements focused on data minimisation, purpose limitation and secure disposal also help to ensure robust cyber resilience by limiting the amount of personal data collected and stored. These requirements ensure that firms reduce both the potential impact of a system breach and the volume of data that needs to be protected.

However, growing localisation and cross-border transfer restrictions add operational complexity. Fragmented data architectures and jurisdiction-specific local control requirements can make it harder to maintain consistent cybersecurity standards and streamline incident response.
Executives must therefore approach privacy and security in an integrated manner and fully embed these considerations into AI governance and control frameworks. This is essential to ensure that compliance obligations enhance, rather than hinder, cyber resilience.

*Please see the ACRS report Safeguarding Data Privacy in AI – Balancing Innovation against Risk, and Ethical Challenges, published October 2025

Recommendations

Below are some key considerations for firms:

Enhance third-party and supply chain risk management. Implement a robust framework for assessing and managing the AI cybersecurity risks posed by third parties. Regularly review supplier contracts and ensure AI security and service continuity obligations are included

Invest in Board and executive education. Provide ongoing training on AI security risks to directors and key executives, so they remain informed of evolving threats and regulatory expectations whilst developing effective policies

Monitor regulatory developments and engage externally. Stay abreast of legislative changes and participate in industry or regional initiatives to help shape emerging standards. Consider joining public-private partnerships or working groups focused on AI security

Engage with experts in AI governance practices and associated cybersecurity considerations such as the Deloitte Trustworthy AI Framework. Leverage industry-leading expertise to assist in building a comprehensive cybersecurity framework with AI in mind

Integrate cybersecurity considerations into the broader technology strategy. In the increasingly digital world, cybersecurity and broader technology strategies cannot be developed in isolation, it is vital for firms to unify their strategy to ensure that AI is developed and used in a secure manner

Verify that the adequacy of existing security standards and associated operational flows do not need to be revisited in response to the threat of AI-enabled deepfakes

Adopt a risk-based approach to securing AI systems. Classify AI tools according to their potential impact, and align security expectations with the firm's risk appetite. This ensures that the most rigorous and resource-intensive controls are reserved for AI systems that carry significant business, regulatory or customer impact, while low-risk tools remain flexible, easy to deploy and free from overly burdensome security restrictions

Promote AI explainability and human oversight. Require that AI systems, especially those used in high-impact business processes, are auditable and capable of providing clear explanations for their outputs. Maintain human oversight for critical decisions that is commensurate with the level of risk posed by the AI system

Prioritise AI cyber risk at Board level. Set a clear policy to ensure that cybersecurity considerations and trade-offs are fully reflected in AI governance, paying attention to the risk profile and unique characteristics of each AI use case. AI-related cyber threats should be well understood by senior executives and should be standing agenda items for the Board. Assign responsibility for oversight to a specific committee or Board member with relevant expertise

Integrate security-by-design into AI development. Mandate that all material AI projects consider security threats from the outset. Ensure that all high-risk applications are subject to rigorous adversarial testing and red-teaming before deployment and throughout the model lifecycle. All AI systems should be subject to ongoing monitoring with periodic testing for adversarial vulnerabilities and resilience to attacks commensurate with the model's risk profile

Establish incident response and reporting protocols. Develop and regularly test response plans for AI cyber-related incidents integrating AI-specific scenarios such as data poisoning, model theft etc. Require real-time monitoring and logging of AI system behavior to detect anomalies which may indicate an attack. AI-incidents and near misses should also be regularly reported to the Board. Ensure that AI cyber-related incident reporting follows established cyber incident notification pathways in compliance with relevant local requirements

Maintain a centralised inventory of AI systems and associated risks. Collect information on AI models across the organisation including their risk classification and purpose. This should also capture key data sources, model components, and any integrations so the organisation can see how tools connect to one another. This matters because even 'low-risk' AI systems can create exposure if they rely on, feed into or share data with higher-risk systems. It is also imperative that the central inventory is updated as soon as a new model is commissioned or following a significant change to a pre-existing model

In summary, as AP firms harness the benefits of digital innovation and AI, they must also navigate a complex and dynamic regulatory environment. Proactive governance, investment in secure and responsible AI practices, and a culture of continuous learning are essential for Boards and executives seeking to mitigate risks and maintain a competitive edge.

Jurisdictional Deep Dive

This section focuses on cybersecurity laws and regulations across AP, however, it is important to note that many jurisdictions are also introducing AI-related guidelines and rules that include recommendations to address security risks. These measures include expectations for the secure development, testing, and monitoring of AI systems, as well as obligations aimed at preventing the misuse of AI-generated or synthetic content, including deepfakes.

Examples include:

Australia
Guidance for AI Adoption (GfAA) which prescribes six "essential practices" for the development and deployment of AI[8]

China (Mainland)
Interim Measures for the Management of Generative Artificial Intelligence Services[9] and the Administration of Deep Synthesis of Internet Information Services (Regulations)[10], which require content labelling, risk assessments, and controls to prevent the misuse of synthetic or manipulated media.

Japan
AI Guidelines for Business, which set out lifecycle obligations relating to robustness, system resilience, secure data handling, monitoring, and incident response[11]

Singapore
Model AI Governance Framework and its accompanying AI Verify testing framework, which outline expectations on robustness testing, secure development practices, transparency, and ongoing monitoring of model behaviour[12]

South Korea
AI Basic Act, which introduces safety and reliability requirements for high-impact AI systems and mandates labelling of generative-AI outputs, including deepfake-type content. This is complemented by amendments to the Act on Special Cases Concerning the Punishment of Sexual Crimes, which criminalise the production, distribution, and even viewing of sexually explicit deepfakes, and amendments to the Public Official Election Act restricting political deepfakes during election periods[13]

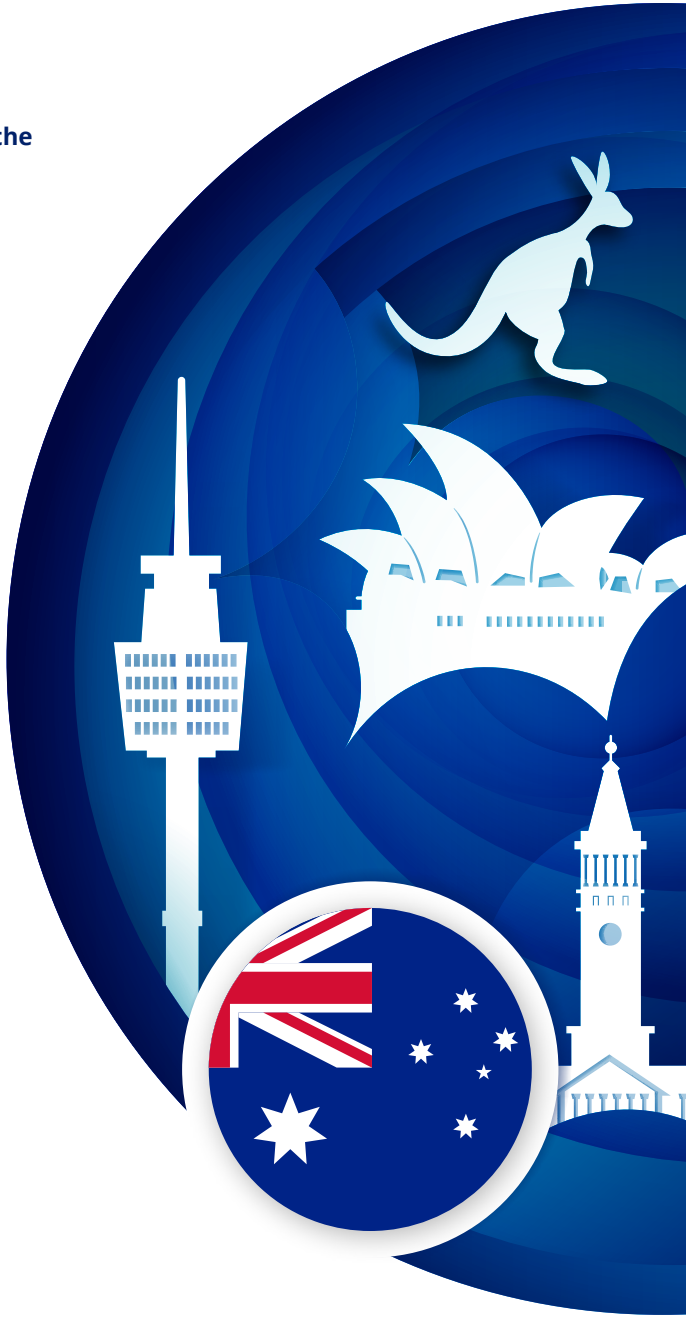
While the core requirements in most jurisdictions remain traditional cybersecurity rules, firms will still need to consider these emerging AI-related guidelines and laws to determine whether they introduce additional obligations for how AI systems are developed, monitored and controlled.

Australia

In November 2024, Australia introduced the Cyber Security Act 2024 ("Cyber Security Act"), the first extensive legislation focused on cybersecurity.[14]

The Cyber Security Act:

- Creates a Cyber Incident Review Board to assess certain cybersecurity incidents
- Requires manufacturers and suppliers to meet minimum security standards for smart devices sold in Australia, with detailed standards to be defined in Ministerial rules
- Obligates businesses that make or facilitate a ransomware payment due to a cybersecurity incident to report this payment to the Commonwealth within 72 hours of its occurrence or discovery
- Establishes a limited use obligation to restrict the dissemination of information provided to the National Cyber Security Coordinator, encouraging businesses to share information following an incident



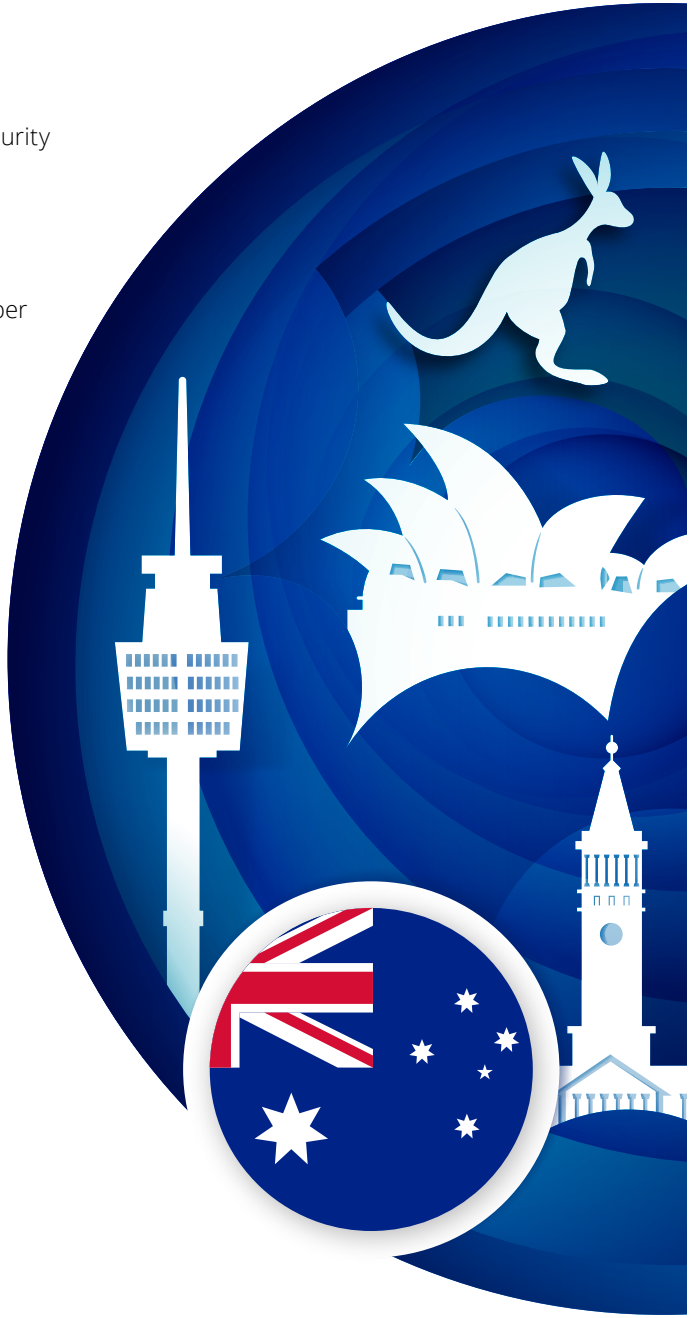
The National Cyber Security Coordinator ("the Coordinator"), alongside the National Office of Cyber Security (NOCS), act as Australia's lead authority for managing significant cyber incidents.

The Coordinator aids the Minister for Cyber Security in coordinating national cyber security policy, responses to major incidents, government preparedness, and enhancing Commonwealth cyber capabilities. This role involves collaboration with key policy and security agencies, providing strategic oversight for cyber security policy across the government, and working with industry to strengthen cyber resilience.

The Minister for Cyber Security appointed members to the Cyber Incident Review Board. This happened after the Cyber Security *(Cyber Incident Review Board)* Rules 2025 came into effect on 30 May 2025.[15] The Cyber Incident Review Board is an independent statutory advisory body conducts no-fault, post-incident reviews of significant cybersecurity incidents in Australia, recommending actions to the government and industry to prevent, detect, respond to, or minimise similar future incidents.[16]

The Australian Signals Directorate's Australian Cyber Security Centre released guidance for firms in January 2024 on how to use AI securely with key AI cyber threats identified.[17] The guidance is not in the form of binding regulation but serves to outline the Australian government's expectations on secure AI usage. Key security challenges when using AI systems are explained with examples of AI-related threats provided such as data poisoning and input manipulation attacks. The guidance also provides some practical mitigation considerations for firms to address when using AI systems.

The main sector-specific cybersecurity legislation is the Security of Critical Infrastructure Act 2018 (Cth) ("SOCI Act"), which applies to 22 categories of critical infrastructure assets across 11 sectors, including communications, financial services, data processing, defence, higher education, energy, food supply, healthcare, space technology, transport, and water management.[18] The Cyber and Infrastructure Security Centre of the Department of Home Affairs released AI-specific guidance on the obligations of operators and owners of critical infrastructure as defined under the SOCI Act.[19] The guidance is designed to aid operators and owners of critical infrastructure identify AI-related risks and how their regulatory obligations under the SOCI Act apply.



China (Mainland)

China (Mainland) ("China") has introduced a comprehensive cybersecurity legislative regime.

The key piece of cybersecurity legislation is the *Cybersecurity Law* ("CSL") which came into effect in July 2017.[20]

Key features of the CSL include:

Network Operator Responsibilities
Defines obligations for network operators to ensure network security and respond to incidents

Government Oversight
Grants the government significant authority to conduct cybersecurity inspections and audits, promoting compliance with the law

Penalties for Violations
Introduces penalties for non-compliance, including fines and potential criminal charges for serious breaches

International Cooperation
Encourages international collaboration on cybersecurity issues while emphasising national sovereignty over data

Critical Information Infrastructure (CII)
Establishes specific protections for CII, which includes sectors like finance, energy, and transportation, mandating stricter security protocols

In April 2025, the State Administration for Market Regulation and the Standardization Administration of China released three standards issuing specific cybersecurity guidance for AI which became effective in November 2025:

Cybersecurity Technology — *Generative Artificial Intelligence Data Annotation Security Specification*[21]
Prescribes security requirements for data labelling processes used when training GenAI

Cybersecurity Technology — *Security Specification for Generative Artificial Intelligence Pre-training and Fine-tuning Data*[22]
Specifies the necessary requirements and assessment criteria to secure datasets utilised during the pre-training and fine-tuning stages of GenAI development

Cybersecurity Technology — *Basic Security Requirements for Generative Artificial Intelligence Service*[23]
Sets out security requirements for GenAI services, including user data security evaluations, data protection strategies, and the preservation of training models and datasets

Cybersecurity regulations in Mainland China are embedded within other pieces of legislation. For example, the *Data Security Law* ("DSL") which primarily focusses upon data privacy contains cybersecurity provisions.[24] Mainland China also releases specific cybersecurity guidance such as the Regulations on Critical Information Infrastructure Security Protection which creates tailored cybersecurity measures for different industries and sectors.[25] Mainland China engages in a constant progress of developing their cybersecurity regulatory framework.

In a similar way to data privacy enforcement, there is not one specific regulatory body responsible for cybersecurity regulatory enforcement. The Cyberspace Administration of China ("CAC") is the main regulatory body responsible for overseeing internet and cybersecurity policies. Other government agencies also hold significant responsibility in the enforcement of cybersecurity regulations and the prosecution of cyber criminals.

The Chinese government in October 2025 introduced a set of amendments to the CSL which include specific provisions for the development and oversight of AI systems.[26] Among amendments which include alignment of the CSL with the *Personal Information Protection Law*[27] and increasing repercussions for violations of cybersecurity and personal information regulations, there is the inclusion of an expansion of state support for research and development for AI. There are also enhancements to requirements relating to ethics, security, and infrastructure capabilities which have been designed with AI in mind. China is modernising its cybersecurity regulatory framework to reflect the increasing use of AI and its associated cyber-risk profile.

Hong Kong SAR

Hong Kong has not implemented specific cybersecurity legislation until 2025.

In March 2025, the Protection of Critical Infrastructures (Computer Systems) Bill ("CI Bill") was passed by the Hong Kong Legislative Council.[28] This legislation aims to bolster cybersecurity for critical infrastructure and maintain the reliability of essential services. Effective from 1 January 2026, it mandates Critical Infrastructure Organizations (CIOs) to comply with specific cybersecurity protocols and gives regulatory bodies the power to address cyber risks.

Key obligations for Critical Infrastructure (CI) operators include:

- Maintain an office in Hong Kong and notify authorities of any operator changes
- Establish a computer-system security management unit
- Notify authorities of major system changes and submit security management plans
- Conduct security risk assessments and arrange security audits
- Participate in security drills and submit emergency response plans
- Report incidents to the Commissioner of Critical Infrastructure (Computer-system Security) (the "Commissioner") within specified timeframes - 12 hours for serious incidents and 48 hours for others, along with a written report within 14 days

Non-compliance can result in fines of up to HKD 5 million. Enforcement of the CI Bill will be the responsibility of the Commissioner, the Commissioner's office is set to be created in early 2026. The Commissioner's Office will have the authority to investigate computer security threats and incidents and can obtain a warrant from a magistrate to compel cooperation from CIOs or service providers, as well as access premises or collect evidence pertinent to the investigation.

India

The key pieces of Cybersecurity regulation in India are the *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* ("CERT-In Rules") and the *Notification of the Ministry of Electronics and Information Technology, Government of India No. 20(3)/2022-CERT-In dated 28 April 2022* ("Cyber Security Directions").[29,30]

The CERT-In rules were framed under *The Information Technology Act, 2000*[31] to formally establish and empower the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency for cybersecurity.

Key Provisions:

Advisories and Directions
CERT-In can issue advisories and directions to enhance cybersecurity and respond to incidents

Confidentiality and Cooperation
Entities are required to maintain confidentiality of information related to incidents and cooperate with CERT-In during investigations or incident response

Reporting and Incident Response
Individuals, organisations, and service providers must report certain types of cyber incidents to CERT-In. The rules enumerate categories of reportable incidents (like unauthorised access, malware attacks, DDoS attacks, etc.)

Roles and Responsibilities
CERT-In is mandated to collect, analyse, and disseminate information on cyber incidents; forecast and issue alerts on cybersecurity incidents; coordinate responses to such incidents; and issue guidelines, advisories, and directions on cybersecurity

The Cybersecurity Directions, issued under powers granted to CERT-In, significantly expand and clarify obligations for organisations regarding cybersecurity practices and incident reporting.

Key Provisions:

Designated Point of Contact
Entities must designate a Point of Contact to interface with CERT-In

Response to Requests
Entities must respond to CERT-In's requests for information or assistance within specified timeframes

Logs Retention
All entities must maintain logs of ICT (Information and Communication Technology) systems for a rolling period of 180 days within India and make them available to CERT-In when required.

Synchronisation of Clocks
All ICT system clocks must be synchronised with NTP (Network Time Protocol) servers of the National Informatics Centre (NIC) or NPL (National Physical Laboratory) or with other government-authorised NTP servers

Mandatory Reporting
Organisations (including service providers, intermediaries, data centres, government bodies) must mandatorily report certain cyber incidents (specified in the Directions) to CERT-In within six hours of noticing the incident or being notified about it

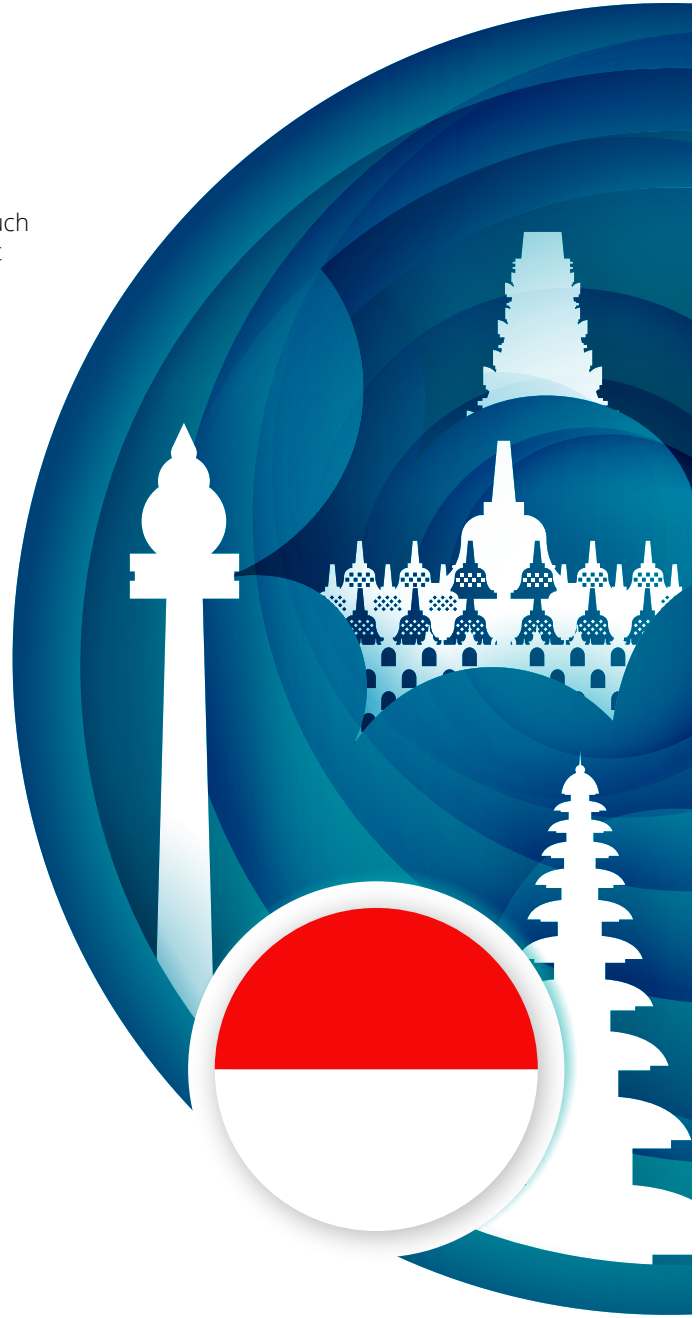
CERT-In is the primary cybersecurity regulatory body in India.

Indonesia

Indonesia does not have a specific standalone law or regulatory framework relating to cybersecurity.

The Electronic Information and Transactions (EIT) Law regulates elements of electronic transactions such as ensuring data integrity and authentication, and provisions for preventing cybercrime.[31] Government Regulation No. 71 of 2019 ("GR 71") was introduced to regulate electronic systems and transactions, it contains provisions relating to the preventing data breaches and cybersecurity incident reporting.[33]

The National Cyber and Crypto Agency (BSSN) (Badan Siber dan Sandi Negara) is Indonesia's primary agency for signal intelligence, cyber intelligence, cyber threat intelligence, cyber defense, and cybersecurity.



Japan

The foundational cybersecurity legislation in Japan is the *Basic Act on Cybersecurity* ("the Act"), enacted in 2014, establishes a comprehensive framework for cybersecurity policy and governance.[34]

Key features of the Act include:

International Cooperation
It emphasises the importance of international collaboration in addressing cybersecurity threats

Research and Development
The Act promotes research and development in cybersecurity technologies and practices

Private Sector Engagement
It encourages private companies to implement cybersecurity measures and share information about threats and vulnerabilities

Cybersecurity Strategy
The Act mandates the creation of a national cybersecurity strategy, which includes risk assessment, incident response, and public awareness initiatives

Government Responsibilities
It designates the Prime Minister as the head of cybersecurity policy, coordinating efforts among various government agencies and promoting collaboration with the private sector

Responsibility of national-level cybersecurity under the Act is given to the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).

Malaysia

The core cybersecurity regulation in Malaysia is the *Cyber Security Act 2024* ("the Act") which came into effect on 26 August 2024, it aims to bolster Malaysia's cyber defences and resilience against emerging threats.[35]

Key components of the Act include:

National Critical Information Infrastructure (NCII)
Identifies systems critical to national functions, public safety, and order

Sector-Specific Governance
Designated NCII Sector Leads are responsible for regulating critical sector entities

Licensing for Cybersecurity Providers
Service providers must obtain licences, with penalties for non-compliance

Extraterritorial Application
The Act applies to offences impacting Malaysia's NCII, even by foreign entities

National Cyber Security Committee
Established to oversee cybersecurity policies, chaired by the Prime Minister

Penalties for Non-Compliance
Violations can lead to fines, imprisonment, or both, with harsher penalties for NCII obligations

Obligations for NCII Entities
Must implement specific cybersecurity measures, conduct risk assessments, audits, and report incidents

NACSA's Role
The National Cyber Security Agency is designated as the lead agency with regulatory and enforcement powers

The Act is accompanied by four sets of guidelines for specific provisions within the Act:

- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024[36]
- Cyber Security (Notification of Cyber Security Incident) Regulations 2024[37]
- Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024[38]
- Cyber Security (Compounding of Offences) Regulations 2024[39]

The Act and accompanying guidelines are enforced by the National Cybersecurity Agency (NACSA) and the newly established National Cyber Security Committee.

New Zealand

New Zealand does not have a specific cybersecurity law or dedicated regulations.

One of the 13 Information Privacy Principles (IPPs) of the *Privacy Act 2020* ("the Act") states that firms must ensure personal information is stored securely and protected against loss, misuse, or unauthorised access.[40] This is the extent of the formalised cybersecurity regulatory framework.

The Act is enforced by the Office of the Privacy Commissioner (OPC).

Philippines

The current primary piece of cybersecurity regulation in the Philippines is the *Cybercrime Prevention Act of 2012* ("the Act").

Key features of the Act include:

- Covers offences such as illegal access, data interference, system interference, misuse of devices, cybersex, child pornography, and identity theft
- Establishes protocols for law enforcement agencies to investigate and prosecute cybercrime
- Creates the Cybercrime Investigation and Coordination Centre (CICC) to oversee investigations
- Defines penalties for various offences, including imprisonment and fines
- Promotes awareness and education regarding cyber threats and safe online practices

The Act is focussed on the prosecution of cybercrimes specifically and has limited oversight on issues such as cyber governance. Enforcement of the Act is the responsibility of the CICC.

The Philippines has released its National Cybersecurity Plan 2023-2028 which is a roadmap to enhance the country's cybersecurity capabilities.[41]

Key features of the plan are:

Strengthening Cybersecurity Infrastructure
Improving the technical infrastructure for better protection against cyber threats

Legislative Support
Advocating for policies and laws that strengthen cybersecurity frameworks

Public-Private Partnerships
Encouraging collaboration between government and private entities to share information and resources

Incident Response and Recovery
Establishing mechanisms for effective response to cyber incidents, including a national incident response team

Capacity Building
Training personnel across government agencies and the private sector to increase cybersecurity awareness and skills

Awareness Campaigns
Promoting public awareness about cybersecurity threats and best practices for individuals and organisations

International Cooperation
Collaborating with other nations and international organisations to combat global cyber threats

Singapore

The key piece of cybersecurity legislation is the *Cybersecurity Act 2018* ("the Act").[42]

Amendments were made to the Act in 2024 through the *Cybersecurity (Amendment) Bill*[43] reflecting the evolving cyber threat landscape and the shift towards cloud computing and third-party infrastructure.

Key features of the Act include:

Empowering the Cyber Security Agency (CSA)
Granting authority to investigate and respond to cybersecurity threats effectively

Facilitating Cybersecurity Information Sharing
Promoting timely sharing of information between CSA, CII owners, and other stakeholders to identify vulnerabilities and prevent incidents

Strengthening Protection of Critical Information Infrastructure (CII)
Safeguarding essential systems that impact the economy and society. CII sectors include Energy, Water, Banking & Finance, Healthcare, Transport, Infocomm, Media, Security & Emergency Services, and Government

Establishing a Licensing Framework for Cybersecurity Service Providers
Licensing for penetration testing and managed security operations centre (SOC) monitoring, ensuring providers meet competency and integrity standards given providers of such services have access to sensitive information from their clients

Key Amendments:

- Updated CII provisions to ensure owners remain responsible for cybersecurity amidst new technologies
- Expanded CSA oversight to include Systems of Temporary Cybersecurity Concern (STCCs) and Entities of Special Cybersecurity Interest (ESCI)
- Regulation of companies providing foundational digital infrastructure, requiring adherence to cybersecurity codes and incident reporting

The enforcement of the Act is the responsibility of the Cyber Security Agency of Singapore ("CSA") formed in 2015. The CSA is managed by the Ministry of Digital Development and Information.

Other general regulations in the Cyber space

The Monetary Authority of Singapore (MAS) Notice on Cyber Hygiene sets out legally binding requirements for financial institutions (FIs) to strengthen their cybersecurity posture. It complements the Technology Risk Management (TRM) Guidelines by mandating baseline security measures that all FIs must implement.

Key Requirements:

Secure Administrative Accounts
Implement preventive controls to restrict unauthorized use of privileged accounts

Multi-Factor Authentication (MFA)
Enforce MFA for administrative accounts and systems accessing customer data

Security Standards
Establish and enforce written security standards for all systems

Network Perimeter Defense
Deploy controls to block unauthorized network traffic

Malware Protection
Install anti-malware solutions on all critical systems

Timely Patch Management
Apply security patches promptly; implement mitigating controls if patches are unavailable

These measures are mandatory and non-compliance can result in regulatory penalties.

The Infocomm Media Development Authority (IMDA) IoT Cyber Security Guide offers baseline security recommendations for IoT systems across their lifecycle—design, deployment, and operation. It targets IoT developers, solution providers, and enterprise users.

Key Principles:

Secure by Default
Use strong cryptography, secure transport protocols, and protect sensitive data

Rigour in Defence
Conduct threat modeling, establish root-of-trust, and implement layered security

Accountability
Enforce access controls, maintain audit trails, and ensure vendor disclosure

Resilience
Design for fault tolerance and recovery to maintain service continuity

The guide includes checklists for threat modeling and vendor self-assessment, promoting security-by-design and risk-based procurement for IoT solutions.

South Korea

Korea's cybersecurity framework is primarily based on the *Act on Promotion of Information and Communications Network Utilization and Information Protection* ("the Act").[44]

The Act is enforced by the *Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection*.[45]

Key features of the Act and associated Enforcement Decree include:

Data Protection
Mandates the protection of personal information and requires service providers to implement safeguards against data breaches

User Consent
Requires explicit user consent for the collection and processing of personal data, ensuring transparency in data handling

Security Measures
Obligates service providers to establish security measures, including encryption and access controls, to protect user data

Incident Response
Stipulates procedures for responding to data breaches, including notification requirements to affected users and authorities

Regular Audits
Encourages regular security audits and assessments to identify vulnerabilities and ensure compliance with cybersecurity standards

Penalties for Non-Compliance
Imposes penalties for failure to comply with data protection and security requirements, ensuring accountability

Collaboration with Authorities
Promotes cooperation between service providers and regulatory bodies to enhance overall cybersecurity resilience

The Ministry of Science and ICT ("MSIT") is the main Cybersecurity regulatory body. It is responsible for the enforcement of the Act.

Taiwan (China)

The core cybersecurity legislation in Taiwan (China) ("Taiwan") is the *Cyber Security Management Act* ("CSMA").[46]

Key features of the CSMA include:

Cybersecurity Governance
Establishes a framework for cybersecurity governance, requiring organisations to appoint a dedicated cybersecurity officer

Risk Assessment
Mandates regular cybersecurity risk assessments to identify vulnerabilities and implement necessary security measures

Incident Management
Requires the development of incident response plans, including protocols for reporting and managing cybersecurity incidents

Information Sharing
Encourages collaboration and information sharing between public and private sectors to enhance overall cybersecurity posture

Training and Awareness
Stipulates the need for cybersecurity training and awareness programmes for employees to mitigate human-related risks

Penalties for Non-Compliance
Imposes penalties for organisations that fail to comply with the Act's requirements, ensuring accountability

Regulatory Oversight
Grants authorities the power to monitor compliance and enforce regulations, including conducting audits and inspections

The Ministry of the Digital Affairs of the Executive Yuan ("MODA") is the main regulatory body responsible for cybersecurity enforcement. Within the MODA, there is a specific Administration for Cyber Security which oversees compliance with the CSMA.

Thailand

Thailand enacted the *Cybersecurity Act, B.E. 2562* ("the Act") in 2019.[47]

The Act is the core cybersecurity regulatory framework for Thailand.

Key features of the Act include:

Definitions and Scope
It defines key terms related to cybersecurity and outlines the responsibilities of various stakeholders, including government agencies, private sector organizations, and individuals

Cybersecurity Committee
The Act establishes the National Cyber security Committee (NCSC) responsible for coordinating national cybersecurity policies and strategies

Critical Information Infrastructure (CII)
Identifies and designates CII sectors and mandates measures to protect them from cyber threats

Incident Reporting
Organizations must report cybersecurity incidents to authorities, facilitating timely responses and mitigation efforts

Penalties
The Act includes penalties for non-compliance with cybersecurity obligations, enhancing accountability

International Cooperation
Encourages collaboration with international partners to address transnational cyber threats

The Act is enforced by the NCSC. The NCSC have also released *the Policy and Plan on Maintaining Cybersecurity for the period of 2022-2027 (B.E. 2565-2570)* ("the Policy") which establishes a policy framework to enhance Thailand's cybersecurity infrastructure.[48]

Key features of the Policy include:

Framework
It establishes a framework for risk assessment, incident response, and recovery to ensure resilience against cyber threats

Capacity Building
Emphasis is placed on training, education, and awareness programs to develop a skilled cybersecurity workforce

Legal and Regulatory Measures
The plan includes updating legal frameworks to address emerging cyber threats and ensure compliance with international standards

Public-Private Partnerships
Encourages cooperation between government and private sectors to enhance information sharing and collective defense

Research and Development
Supports innovation in cybersecurity technologies and practices through funding and collaboration with academic institutions

Implementation and Evaluation
Outlines mechanisms for monitoring progress and adapting strategies based on evolving threats

Thailand in October 2025 released specific guidance for firms promoting the secure and responsible use of AI, including some specific cybersecurity considerations. The National Cyber Security Agency released the *AI Security Guidelines* which include a section outlining key principles for AI security systems throughout the AI lifecycle.[49] It emphasises the need for security assessments in line with international standards and frameworks (such as those set by the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO)) to identify and address potential vulnerabilities. The appendix of the guidelines also contains an AI security checklist along with example case studies and policies for secure AI use. The *AI Security Guidelines* lay the foundations for the creation of the "Thailand AI Security Framework" which will establish cybersecurity controls for AI use in both the public and private sectors in Thailand.[50]

Vietnam

Vietnam in December 2025 passed the Cybersecurity Law which aims to create a robust legal framework that strengthens the ability to safeguard national sovereignty in cyberspace and supports the sustainable growth of the digital economy.[51]

The Cybersecurity Law comes into effect in July 2026 and will consolidate the 2018 *Law on Cybersecurity* ("LOCS")[52] and 2015 *Law on Cyberinformation Security*[53] which will continue to act as the active cybersecurity legislation until then.

Key features of the Cybersecurity Law include:

Personal Information
Forbids unauthorised eavesdropping and selling cryptographic tools of unclear origin

Prohibition on Harmful Content
Prohibits psychological warfare and incitement of hatred between ethnicities and religions

Misinformation
Forbids historical distortion, undermining national unity, and insults to national symbols. Strictly prohibits spreading false information that harms individuals or organisations

National Security Requirements
Prohibits dissemination of content opposing the State and distorting government information. Bars unauthorised collection or exposure of personal and state secrets. Bars unauthorised collection or exposure of personal and state secrets

This builds upon the foundation of the LOCS and Law on Cyberinformation Security which established the following requirements:

Cybersecurity Requirements
Organisations must implement measures to protect information systems, including risk assessments and incident response protocols

Data Localisation
Certain entities are required to store data related to Vietnamese users within the country, facilitating government access for security purposes

Incident Reporting
Organisations must report cybersecurity incidents to authorities, enabling coordinated responses and mitigation efforts

Penalties
The law outlines penalties for violations, enhancing accountability for non-compliance with cybersecurity regulations

Collaboration
It promotes cooperation between government agencies, businesses, and international partners to strengthen cybersecurity defences

In Vietnam, the Ministry of Public Security leads cybersecurity regulation and enforcement, while the Ministry of National Defense manages military information systems and the Government Cipher Committee oversees cryptographic systems.

Contacts

Authors

Nicola Sergeant
Managing Director
ACRS Operations Lead
Japan
nicola.sergeant@tohmatsu.co.jp

Rhys Belcher
Senior Consultant
ACRS
Hong Kong SAR
jobelcher@deloitte.com.hk

Asia Pacific Centre for Regulatory Strategy (ACRS)

Seiji Kamiya
Executive Sponsor
Asia Pacific Regulatory & Financial Risk Lead
seiji.kamiya@tohmatsu.co.jp

Yuki Shuto
ACRS Steering Committee
Partner
AP Consulting Growth Leader
yshuto@tohmatsu.co.jp

Tony Wood
ACRS Steering Committee
Partner
AP Banking & Capital Markets Leader
tonywood@deloitte.com.hk

Ye Fang
ACRS Steering Committee
Partner
China SR&T FS Industry Lead
yefang@deloitte.com.cn

Sean Moore
Australia Co-lead
Partner
AU SR&T FS Industry Lead
semoore@deloitte.com.au

Nai Seng Wong
SEA Co-lead
Partner
SEA Regulatory Strategy Lead
nawong@deloitte.com

Shinya Kobayashi
Japan Co-lead
Managing Director
JP SR&T Insurance Sector Lead
shinya.kobayashi@tohmatsu.co.jp

Asia Pacific Trustworthy AI Leaders

Dr Elea Wurth
Partner
Asia Pacific & Australia
ewurth@deloitte.com.au

Amy Dove
Partner
New Zealand
amydove@deloitte.co.nz

Toyohiro Sometani
Partner
Japan
toyohiro.sometani@tohmatsu.co.jp

Chris A. Chen
Partner
Taiwan
chrisachen@deloitte.com.tw

Jessica Kim
Partner
South Korea
jessikim@deloitte.com

Silas Hao Zhu
Partner
China
silzhu@deloitte.com.cn

Dishell Gokaldas
Partner
Singapore
dgokaldas@deloitte.com

Jayant Saran
Partner
India
jsaran@deloitte.com

Pence Cong Peng
Partner
China
pepeng@deloitte.com.cn

Contributors

Yuichiro Kirihara
Asia Pacific Cyber Offering Leader
Partner
Japan
ykirihara@tohmatsu.co.jp

Luke Forsyth
Emerging Technology Security Leader in Australia
Partner
Australia
lforsyth@deloitte.com.au

Richard Bush
Cyber Strategy & Transformation
Partner
Australia
rbush@deloitte.com.au

Toshiyuki Oba
Privacy, Security & IT Governance Specialist
Managing Director
Japan
toshiyuki.oba@tohmatsu.co.jp

Acknowledgements

Tommy Hartanto
Director
Indonesia
thartanto@deloitte.com

Anh Quoc Luu
Senior Manager
Vietnam
anhqluu@deloitte.com

Kerrie Hie
Director
Australia
khie@deloitte.com.au

Shoya Kusoda
Senior Consultant
Japan
shoya.kusuda@tohmatsu.co.jp

Eric Kanikevich
Consultant
Australia
ekanikevich@deloitte.com.au

Vijay Shankar
Director
India
vijshankar@deloitte.com

Prakash Arikrishnan
Director
Malaysia
parikrishnan@deloitte.com

Monai Supanit
Senior Manager
Thailand
msupanit@deloitte.com

Tony Zhi-Wei Tang
Associate Director
Australia
totang@deloitte.com.au

Samuel Yue Xuan Ang
Consultant
Singapore
saang@deloitte.com

Endnotes

1. For "Critical Infrastructure" as defined in the 'Government of Singapore, *Cybersecurity (Provider-Owned Critical Information Infrastructure) Regulations*, August 2018, Cybersecurity (Provider-Owned Critical Information Infrastructure) Regulations 2018 - Singapore Statutes Online' the timeline for reporting is 2 hours
2. Personal Information Protection Commission, *Policy Direction on the Safe Use of Personal Information in the AI Era*, August 2023, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9083
3. ASEAN, ASEAN *Cybersecurity Cooperation Strategy (2021-2015)*, January 2022, ASEAN CYBERSECURITY COOPERATION STRATEGY
4. ASEAN–Japan Cybersecurity Community Alliance, *Three Interlocking Pillars of Cyber Resilience*, October 2025, - ASEAN Japan Cybersecurity Community Alliance (AJCCA)
5. Please see the ACRS report Safeguarding Data Privacy in AI – Balancing Innovation against Risk, and Ethical Challenges, published October 2025
6. Privacy Commissioner for Personal Data, *Personal Data (Privacy) Ordinance*, October 2022, 《個人資料(私隱)條例》Personal Data (Privacy) Ordinance
7. Privacy Commissioner for Personal Data, *Guidance Note on Data Security Measures for Information and Communications Technology*, August 2022, guidance_datasecurity_e.pdf
8. Australia Government, *Voluntary AI Safety Standard*, August 2024 Voluntary AI Safety Standard
9. Cyberspace Administration of China, *Interim Measures for the Management of Generative Artificial Intelligence Services*, July 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
10. Cyberspace Administration of China, *Administration of Deep Synthesis of Internet Information Services (Regulations)*, November 2022, 互联网信息服务深度合成管理规定_中央网络安全和信息化委员会办公室
11. Ministry of Internal Affairs and Communications Ministry of Economy, Trade and Industry, *AI Guidelines for Business*, April 2024, 20240419_9.pdf
12. Infocomm Media Development Authority, *Model AI Governance Framework for Generative AI*, January 2024, Model AI Governance Framework 2024 - Press Release | IMDA
13. Ministry of Science and ICT (MSIT), *AI Basic Act*, December 2024 Press Releases - 과학기술정보통신부 〉
14. Australian Government, *Cyber Security Act 2024*, November 2024, Cyber Security Act 2024 - Federal Register of Legislation
15. Australian Government, *Cyber Security (Cyber Incident Review Board) Rules 2025*, February 2025, Cyber Security (Cyber Incident Review Board) Rules 2025 - Federal Register of Legislation
16. Australian Department of Home Affairs, *Factsheet - Cyber Incident Review Board*, Factsheet - Cyber Incident Review Board
17. Australian Signals Directorate, *Engaging with artificial intelligence*, January 2024, Engaging with artificial intelligence | Cyber.gov.au
18. Cyber and Infrastructure Security Centre, *Security of Critical Infrastructure Act 2018*, April 2018, Security of Critical Infrastructure Act 2018 - Federal Register of Legislation
19. Cyber and Infrastructure Security Centre, *Factsheet for Critical Infrastructure – Artificial Intelligence in Critical Infrastructure*, June 2025, Artificial Intelligence in Critical Infrastructure Factsheet
20. Standing Committee of the National People's Congress of the People's Republic of China, *The Cybersecurity Law of the People's Republic of China*, November 2016, Cybersecurity Law of the People's Republic of China
21. State Administration for Market Regulation and the Standardization Administration of China, 网络安全技术生成式人工智能数据标注安全规范, April 2025, 标题
22. State Administration for Market Regulation and the Standardization Administration of China, 网络安全技术 生成式人工智能预训练 和优化训练数据安全规范, April 2025, 标题
23. State Administration for Market Regulation and the Standardization Administration of China, 网络安全技术 生成式人工智能服务 安全基本要求, April 2025, 标题
24. National People's Congress, *Data Security Law of the People's Republic of China*, June 2021, Data Security Law of the People's Republic of China
25. The State Council of the People's Republic of China, *Regulation to strengthen protection over critical information infrastructure*, August 2021, Regulation to strengthen protection over critical information infrastructure
26. Standing Committee of the National People's Congress, 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定, October 2025, 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定 _ 中国政府网
27. Standing Committee of the National People's Congress, *Personal Information Protection Law*, November 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
28. Hong Kong Legislative Council, Protection of Critical Infrastructures (Computer Systems) Bill, March 2025, The Government of the Hong Kong Special Administrative Region Gazette
29. Government of India, *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013*, January 2024, G.S.R_20(E).pdf

Endnotes

30. Government of India, *Notification of the Ministry of Electronics and Information Technology, Government of India No. 20(3)/2022-CERT-In dated 28 April 2022*, April 2022, CERT-In_Directions_70B_28.04.2022.pdf
31. Government of India, *The Information Technology Act, 2000*, June 2000, it_act_2000_updated.pdf
32. Government of Indonesia, *Law of the Republic of Indonesia No.11 of 2008 – Concerning Electronic Information and Transactions*, April 2008, Law No. 11 of 2008 on Electronic information and transactions
33. Government of Indonesia, *Regulation of the Government of the Republic of Indonesia Number 71 of 2019 on the Organization of Electronic Systems and Transactions*, October 2019, PP_NO_71_2019_EN
34. Government of Japan, *The Basic Act on Cybersecurity*, November 2014, The Basic Act on Cybersecurity - English - Japanese Law Translation
35. Government of Malaysia, *Cyber Security Act 2024 – Act 854*, June 2024, NACSA | Act 854
36. Government of Malaysia, *Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024*, August 2024, PUA219_2024.pdf
37. Government of Malaysia, *Cyber Security (Notification of Cyber Security Incident) Regulations 2024*, August 2024, PUA220_2024.pdf
38. Government of Malaysia, Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024, August 2024, PUA 221.pdf
39. Government of Malaysia, *Cyber Security (Compounding of Offences) Regulations 2024*, August 2024, PUA222_2024.pdf
40. New Zealand Government, *Privacy Act 2020*, June 2020, Privacy Act 2020 No 31 (as at 30 March 2025), Public Act Contents – New Zealand Legislation
41. Republic of the Philippines Department of Information and Communications Technology, *National Cybersecurity Plan 2023 – 2028*, February 2024, NCSP 2023-2028 - FINAL-DICT
42. Government of Singapore, *Cybersecurity Act 2018*, March 2018, Cybersecurity Act 2018 - Singapore Statutes Online
43. Government of Singapore, *Cybersecurity (Amendment) Bill*, April 2024, 0ec86552-e671-4f87-928f-7b9d3e8b1276 1..93
44. Republic of Korea Government, *Act on Promotion of Information and Communications Network Utilization and Information Protection*, January 2001, 영문법령 > 본문 - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 | 국가법령정보센터
45. Republic of Korea Government, Enforcement Decree of the *Act on Promotion of Information and Communications Network Utilization and Information Protection*, January 2001, English Statutes > Text - Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. | National Laws and Regulations Information Center
46. Republic of China (Taiwan) Ministry of Digital Affairs, *Cyber Security Management Act*, June 2018, Cyber Security Management Act - Article Content - Laws & Regulations Database of The Republic of China (Taiwan)
47. Government of Thailand, *Cybersecurity Act, B.E. 2562 (2019)*, May 2019, 3572-Cybersecurity-Act-B-E-2562--2019-
48. National Cyber Security Committee, *Policy and Plan on Maintaining Cybersecurity for the period of 2022-2027 (B.E. 2565-2570)*, December 2022, 17236495.pdf
49. National Cyber Security Agency, *AI Security Guidelines*, October 2025, Office of the National Cyber Security Commission
50. National Cyber Security Agency, *AI Security Guidelines: Stepping into a New Standard for Artificial Intelligence Security*, October 2025, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
51. National Assembly of Vietnam, *National Assembly adopts 35 bills and resolutions*, December 2025, National Assembly adopts 35 bills and resolutions
52. National Assembly of Vietnam, *Law No. 24/2018/QH14 on Cybersecurity*, June 2018, Trung ương
53. National Assembly of Vietnam, *Law No. 86/2015/QH13 on Cyberinformation Security*, November 2015, Law No. 86/2015/QH13 on Cyberinformation Security 2015 in Vietnam

Deloitte.

The Deloitte Centre for Regulatory Strategy is a source of critical insights and advice, designed to assist the world's largest financial institutions manage the strategic and aggregate impact of regional and international regulatory policy. With regional hubs in Asia Pacific, the Americas and EMEA, the Centre combines the strength of Deloitte's network of experienced risk, regulatory, and industry professionals — including a deep roster of former regulators, industry specialists, and business advisers — with a rich understanding of the impact of regulations on business models and strategy.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organisation"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organisation") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 415,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, or the Deloitte organisation is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2025 Deloitte Touche Tohmatsu
Designed by CoRe Creative Services. RITM2324024