Curbing the cost of cybersecurity fragmentation

An agenda for harmonisation across the Indo-Pacific

BART HOGEVEEN
GATRA PRIYANDITA
JAMES CORERA

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

AUGUST 2025

Policy Brief

About the authors

Bart Hogeveen is a Senior Fellow and Director Europe at ASPI.

Dr Gatra Priyandita is a Senior Analyst at ASPI's Cyber, Technology and Security Program.

James Corera is the Director of ASPI's Cyber, Technology and Security Program.

Acknowledgements

The authors would like to thank colleagues at Microsoft for their insights and support as well as ASPI colleagues who helped work on or reviewed this report, including Chris Taylor and John Coyne. We would also like to thank Jason Van der Schyff and Manoj Harjani for their valuable feedback, and Ravi Nayyar for his foundational research that enabled this report.

This report was produced as part of ASPI's partnership with Microsoft investigating the nature and consequences of regulatory fragmentation with respect to cyber resilience in the Indo-Pacific.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cyber, Technology and Security Program

ASPI's Cyber, Technology and Security Program (CTS) analysts inform policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS is a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public, private and civil-society sectors.

CTS enriches regional debate by collaborating with civil-society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on.

If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Cover image: Byron Illyes, ASPI.

Curbing the cost of cybersecurity fragmentation

An agenda for harmonisation across the Indo-Pacific

BART HOGEVEEN
GATRA PRIYANDITA
JAMES CORERA

AUGUST 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief

First published August 2025

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Contents

Overview

This report documents the width and depth of fragmentation of cybersecurity regulation in the Indo-Pacific—focusing on Australia, Japan, South Korea and Indonesia. It investigates whether the divergent regulatory burdens placed on the private sector are creating a systemic vulnerability and therefore deserve a strategic policy response.

We conclude that there is a strong degree of coherence in the principles and overall approaches to cybersecurity governance, but that fragmentation arises primarily at the level of implementation. That's creating negative effects on corporate cybersecurity culture, operational efficacy and responsiveness; it also creates barriers to innovation and international cooperation. Taken together, we conclude that issue deserves a strategic policy response by Indo-Pacific policymakers.

The shared principles among the four Indo-Pacific nations offer a sound base to pursue a targeted harmonisation agenda. This requires a strategically calibrated, multi-platform and multi-speed approach—leveraging the comparative strengths of the Association of Southeast Asian Nations (ASEAN), the Asia–Pacific Economic Cooperation forum (APEC), the Quad, the Organisation for Economic Co-operation and Development (OECD) and others. It offers the potential to incrementally transform fragmentation into interoperability. But the key implementation challenge lies in reconciling legal definitions, enforcement thresholds and jurisdictional reach. Mutual recognition of certifications, streamlined reporting obligations and coordinated enforcement mechanisms are critical—yet difficult—steps.

While this report concentrates on formal regulation, it's important to recognise the significant role of private-sector actors in shaping cybersecurity norms. Industry consortia, multinational firms and dominant technology providers often define technical baselines well ahead of regulatory processes. Common security frameworks and assurance practices—many originating from US and European institutions—have been informally adopted across much of the region, shaping everything from risk assessments to incident response procedures. Those influences offer a quiet but powerful form of alignment, one that often underpins interoperability even where legislative approaches diverge. This dynamic underscores the virtue of democratic states sustaining engagement in multinational institutions—even when these bodies feel slow or ineffective.

Harmonisation also cannot be understood in isolation from the broader and sharpening strategic environment. While this report excludes China from its core analysis, Beijing's influence is nonetheless salient. Its regulatory model—focused on data sovereignty, state-led controls and increasingly exportable governance frameworks—is offering Indo-Pacific states an alternative path, particularly where strategic alignment with the West is less established. That parallel system is already creating tension in areas such as cross-border data flows, supply-chain transparency and vendor certification. Any Indo-Pacific harmonisation agenda must contend not only with technical diversity, but with competing models of digital governance.

The path forward should not be expected to be linear. It will require diplomacy, transparency and above all, trust. Capacity building must accompany standard-setting. Pilot initiatives must precede mandates. And sovereignty must be respected even as risks are jointly managed. Ultimately, digital sovereignty and strategic cyber resilience are not mutually exclusive—but if countries continue to pursue the former without regard for the latter, the Indo-Pacific will remain vulnerable to exploitation by malign actors and regulatory overstretch. Without targeted alignment, cyber fragmentation will slow down commerce, hinder innovation and become a lasting drag on regional security and prosperity.

What's the problem?

Cyberspace and technology are borderless but their infrastructure and operations are bound by national laws shaped by differing threat perceptions and governance models. That has created a mishmash of regulatory obligations, particularly in regions lacking a common market such as the Indo-Pacific. In April 2025, Chief Information Security Officers (CISOs) of global companies raised the alarm, calling on G7 and OECD states to address regulatory fragmentation.[1]

Why is this a problem? Fragmented cybersecurity regulations are undermining technical efficiency, innovation and international trust. In the Indo-Pacific, where digital trade is surging and demands for more stringent data protection and cybersecurity are increasing, mismatched regulations are hampering crisis response, weakening operational resilience and driving up compliance costs. This should not be seen as merely a technical issue but a strategic vulnerability.

Fragmentation leads to *operational inefficiency and lags in responsiveness*. Companies operating across borders must navigate different compliance obligations for the same product or service, while cybersecurity service providers must adapt centralised solutions—often developed, patched or updated remotely—for each regulatory environment. Those inefficiencies are slowing response times and increasing operational costs.

Furthermore, fragmentation encourages *risk-averse checkbox compliance* rather than fostering the agile, risk-informed security postures necessary to address a rapidly evolving threat landscape.[2] Digital service providers and ICT manufacturers operating across multiple jurisdictions are driven to divert resources from core security operations to meet market-specific compliance obligations. That could undermine the effectiveness of the very regulations designed to enhance cyber resilience as it creates duplicative efforts and incentivises minimal adherence to disparate standards rather than the proactive measures required to counter sophisticated, cross-border, cyber threats.

Company leadership faced with divergent regulatory requirements will prioritise meeting legal minimums instead of comprehensive risk management; and, combined, that inadvertently increases vulnerabilities at the national or regional level.[3]

While regulatory fragmentation affects both large and small enterprises, it places *a disproportionate burden on smaller companies and start-up cybersecurity providers*, which often lack the capacity to absorb complex and diverse compliance demands. That constrains their export potential and hampers cross-regional capacity-building, as divergent regulations and technical standards impede the exchange of best practices, tools and controls—particularly among national cybersecurity and incident response agencies.

Fragmentation also *stifles innovation*, particularly for small and medium-sized enterprises and startups. Those entities often lack the capacity to navigate fragmented frameworks, thereby constraining their ability to scale up and compete in international markets. Innovation in cyber defence depends not only on robust regulation, but on regulatory environments that foster growth and experimentation.

Fragmentation similarly *constrains international cooperation*. Effective cyber partnerships rely on mutual trust, shared threat assessments and regulatory interoperability. Yet diverging national rules on data flows, encryption standards, incident reporting and procurement criteria create barriers to joint action. Partners find themselves duplicating efforts or hesitating to share intelligence for fear of legal incompatibility. For multinational firms and critical infrastructure operators, that divergence weakens trust in regional digital supply chains and creates uncertainty around investment decisions.

Taken together, cyber fragmentation is creating a systemic vulnerability and therefore deserves a strategic policy response.

As India's External Affairs Minister, S Jaishankar, noted at the 2025 Raisina Dialogue, 'The world today makes business decisions factoring in national security in a manner it did not do before, especially in the digital era.'[4] His words reflect mounting frictions: Japanese manufacturers are navigating new hurdles under the EU's 2024 Cyber Resilience Act and US tech companies are pushing back against India's data localisation mandates.[5] Indeed, in much of the Indo-Pacific, cybersecurity has—necessarily so—become inseparable from national security. Governments in the region increasingly view digital infrastructure not just as an enabler of economic growth, but as a potential vulnerability in an age of rising geostrategic contestation.[6]

Therefore, imposed compliance costs placed upon the private sector are not merely one of the costs of national risk management based on technical advice, but inherently political and geo-economic.

What's the solution?

National policies reflect legitimate concerns, but it's their uncoordinated rollout that has widened the regulatory gap across the region. To remedy that, governments should pursue an approach of targeted regulatory alignment: the leveraging of existing regional mechanisms such as ASEAN, APEC and the Quad to endorse shared (market) standards, mutual recognition agreements and frameworks for interoperability—especially for incident reporting, vendor vetting and security-by-design principles.

What's needed is a shift in mindset, from defensive sovereignty to cooperative resilience. Cybersecurity needs to remain a sovereign responsibility, but sovereignty need not come at the cost of unnecessary fragmentation—indeed fragmentation can harm national security. Therefore, states should start working towards shared regulatory outcomes. That means building trust through regulatory design that enables collaborative or collective action and would involve teamed-up endeavours by the legislators, regulators and policymakers of involved countries.

Part 3 of this report presents seven specific courses of action for consideration. This includes picking low hanging fruit by, for example, agreeing to a shared lexicon, address operational inconsistencies by developing standardised thresholds for incident reporting and improve security and transparency by coordinating approaches to supply chain risk management.

This report

This report looks at the cybersecurity regulatory landscape in the Indo-Pacific by reviewing four jurisdictions: Australia, Japan, South Korea and Indonesia. Those countries collectively represent a significant share of the region's digital economy—excluding China—and serve as critical nodes in cross-border data flows, regional supply chains and digital trade. Together, they provide a representative and diverse sample of regulatory models and challenges relevant to Indo-Pacific cybersecurity governance.

This report consists of three parts. The first presents an overview of how Australia, Japan, South Korea and Indonesia are pursuing divergent cybersecurity regulatory paths shaped by national events, priorities and strategic shifts. The second investigates regulatory controls imposed in relation to three key sub-areas: personal information handled by businesses; critical national infrastructure ('CNI') assets; and governance by directors of businesses. The third provides recommendations for targeted harmonisation across the Indo-Pacific.

Part 1: Fragmented frontlines—Case studies of Australia, Japan, South Korea and Indonesia

This section explores the evolving regulatory trajectories of Australia, Japan, South Korea and Indonesia—four nations that, together, anchor the majority of the Indo-Pacific's digital economy outside China and India. Each of the four countries is heavily invested in and increasingly dependent on, the integrity of cross-border digital trade and the stability of global data flows. Yet their respective cyber regulatory frameworks have been shaped not just by economic imperatives, but by distinct national inflection points, critical incidents, strategic realignments or political decisions that have calibrated their approach to cyber governance.

What emerges is a region where state intervention is no longer the exception but the norm, as governments seek to harden digital infrastructure, assert data sovereignty and mitigate transnational risks. In an environment marked by geopolitical uncertainty and technological contestation, these regulatory journeys reflect deeper questions about how the Indo-Pacific balances open digital trade with national security and strategic resilience. The resulting divergence in

regulatory models is creating friction across borders, slowing incident response and weakening collective cyber resilience. Without greater alignment around shared security outcomes, the region risks entrenching a fragmented ecosystem that undermines both innovation and strategic trust.

Key takeaway

- Fragmentation patterns are playing out differently across the Indo-Pacific. In Australia, the challenge lies in the complexity of overlapping frameworks. In Japan, voluntary guidelines dominate, creating inconsistency. In South Korea, a proliferation of laws, agencies and rigid procedures is slowing innovation. And, in Indonesia, legislative gaps and institutional undercapacity remain impediments.

Joint technical advisories: a means to incentivise harmonisation

While legislation and regulation can go in different directions, the cybersecurity community—in particular the incident-response community—is known for a high degree of information-sharing of technical tactics, techniques and procedures (TTPs) and following common practices and *de facto* industry standards.[7] An example is the practice of technical advisories: public documentation that reports observed tradecraft of malicious cyber actors.

Between January 2023 and July 2025, we counted 34 advisories involving either Australia, Japan, South Korea or Indonesia. Of note is that almost all advisories involve a partnership with one or more US cyber agencies; and the majority are co-authored by all Five Eyes partners. Since May 2024, broader coalitions have formed, disclosing the TTPs of Russian threat actors. Since October 2024, Japan and South Korea have joined in five advisories, although those were threat-actor-agnostic and focused on best practices. Advisories related to the behaviour of nation-state actors involve Russia (38%), China (24%) and Iran (1 case).

Australia: Strong foundations, fragmented outcomes

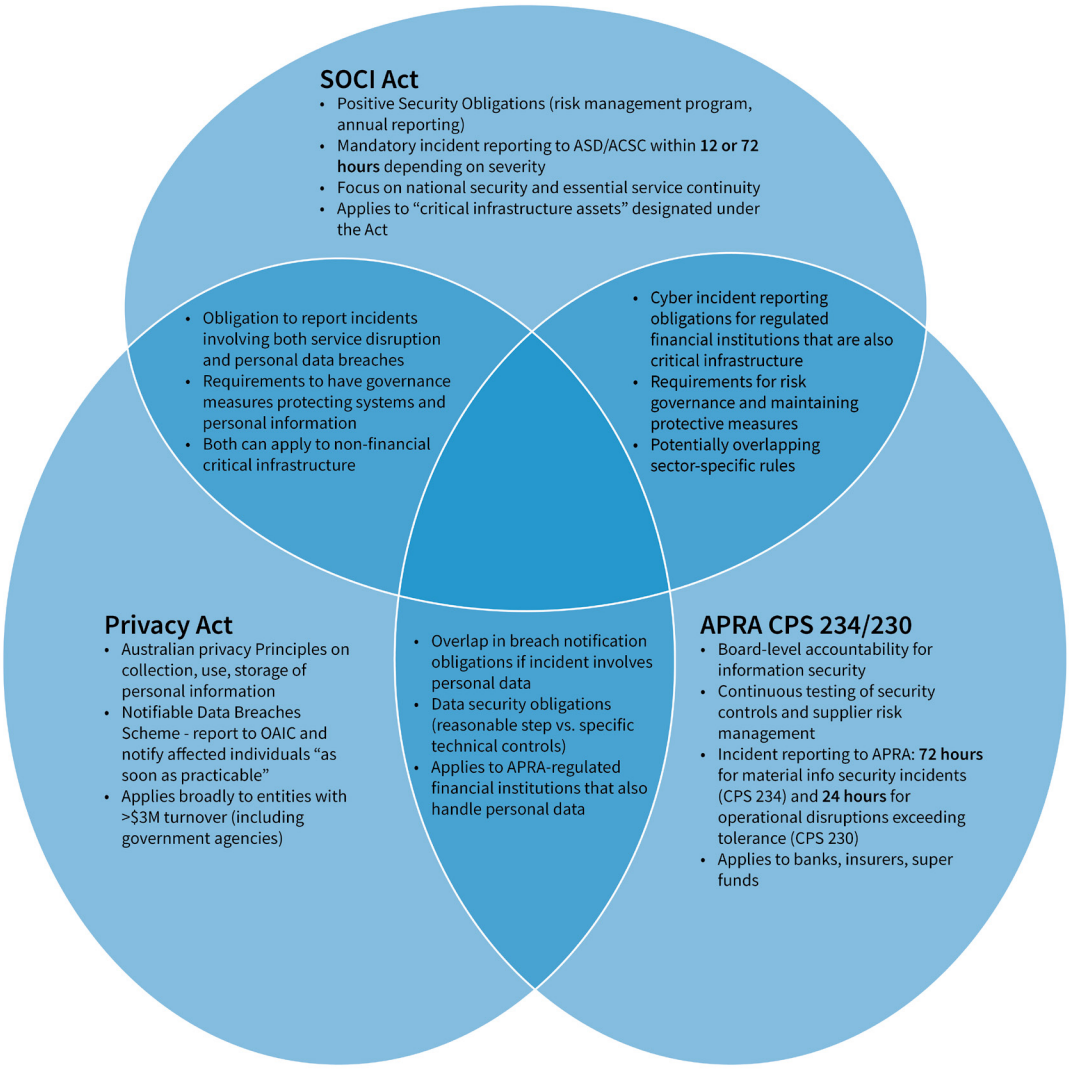
With 97% of its population online and digital activity contributing over 6% of GDP, Australia is one of the Indo-Pacific's most digitally connected—and therefore cyber-exposed—economies, with deep reliance on data-driven services and digital activity.[8] That connectivity has brought enormous economic and societal benefits—but it's also made Australia a prime target for cybercrime and state-linked cyber threats. Public and political awareness of those vulnerabilities surged following the 2022 Optus and Medibank breaches, in which foreign actors exploited basic security lapses—such as the absence of multifactor authentication and delayed incident escalation—to access the personal data of millions of people. Those breaches transformed cybersecurity from a technical issue into a national political and security priority, triggering a coordinated, whole-of-government effort to build resilience.

In response, Australia has made significant progress. The 2023 amendments to the *Security of Critical Infrastructure Act 2018* (the SOCI Act) have positioned the country at the forefront of global cybersecurity regulation, with a legislative and institutional framework that's among the most comprehensive in the world.[9] Eleven critical sectors and 22 asset classes are now subject to a layered set of obligations, from mandatory incident reporting and asset registration to critical infrastructure risk-management programs and enhanced cybersecurity obligations for designated entities.

Crucially, industry has played an active role in shaping this evolving regulatory landscape. Through formal consultation processes, advisory panels and engagement with the Cyber and Infrastructure Security Centre, Australian businesses—particularly those operating critical infrastructure—have helped inform risk definitions, implementation pathways and sector-specific obligations. While government sets the strategic direction, industry has been vital in translating regulatory goals into operational practice, flagging implementation challenges and contributing expertise on threat environments and system vulnerabilities.

Figure 1 outlines relevant pieces of Australian legislation and their overlaps.

Figure 1: Differences in Australian cybersecurity regulations



ACSC= Australian Cyber Security Centre; APRA = Australian Prudential Regulation Authority; ASD = Australian Signals Directorate; OAIC = Office of the Australian Information Commissioner; SOCI Act = *Security of Critical Infrastructure Act 2018*. Source: ASPI.

As the regulatory model has matured, new—and in some cases unanticipated—risks have emerged. Chief among them is a growing form of regulatory fragmentation, both domestically and internationally, that risks undermining the very resilience that the regime is intended to strengthen. Institutions often face overlapping and occasionally inconsistent requirements across the SOCI Act, the CPS 234 and CPS 230 standards of the Australian Prudential Regulation Authority (APRA), and the *Privacy Act 1988*—each enforced by different agencies, such as the Office of the Australian Information Commissioner (OAIC). The Australian Signals Directorate (ASD) also plays an important role in defining cybersecurity standards, particularly for critical infrastructure. The result is that firms may expend significant resources in navigating complex compliance landscapes, rather than meaningfully improving operational resilience. Combined with the national shortage of cybersecurity professionals, those factors risk leaving major parts of the economy exposed—contrary to the broader national resilience objectives.

A further risk is the emergence of a compliance-first mindset, in which security is viewed as a legal hurdle rather than a continuous, risk-based operational imperative. As ASPI's analysis of the Qantas data breach illustrates, regulatory compliance isn't synonymous with protection.[10] Australia's regulatory foundations are strong. The challenge looking forward is that any regulatory reform needs to be pursued in parallel with a sharper focus on systemic risk, capability uplift and operational agility.

Case study: Medibank's 2022 cyberattack

In October 2022, Medibank, one of Australia's largest health insurers, suffered a major cyberattack that compromised the personal and health data of 9.7 million customers. The breach—attributed to stolen credentials and inadequate security controls—exposed critical gaps in Medibank's cybersecurity governance, including the absence of multifactor authentication and ineffective incident monitoring. Despite prior warnings from consultants, those deficiencies allowed attackers to access and exfiltrate 520 gigabytes of sensitive data undetected for nearly two months.

The incident triggered a complex regulatory response. APRA imposed a $250 million capital charge under CPS 234 for inadequate information security controls and required Medibank to implement a remediation program.[11] The OAIC initiated investigations under the Privacy Act, citing failures to protect personal information and mandating notifications to affected individuals.[12]

The convergence of those regulatory requirements tested Medibank's operational resilience. While addressing internal security failures, the company had to navigate overlapping obligations from multiple agencies, each with distinct timelines and compliance expectations. That dual challenge—remediating internal weaknesses while managing complex external oversight—strained resources and underscored the need for both stronger cybersecurity governance and more cohesive regulatory coordination.

Japan: Voluntary measures limiting resilience and interoperability

Japan's cybersecurity regulatory landscape reflects a decentralised and predominantly voluntary approach, which, while encouraging sectoral flexibility and private-sector engagement, results in regulatory fragmentation that undermines national resilience and limits international collaboration.

At the strategic level, Japan's National Centre of Incident Readiness and Strategy for Cybersecurity (NISC), operating under the cabinet's Cybersecurity Strategic Headquarters, sets the overall direction. However, implementation is devolved to sector-specific ministries—such as the Ministry of Economy, Trade and Industry, the Ministry of Internal Affairs and Communications, and the Financial Services Agency—which issue their own guidelines tailored to distinct industries. That has created overlapping standards, inconsistent security baselines and gaps in coverage across critical infrastructure sectors.

Crucially, Japan's Basic Act on Cybersecurity outlines guiding principles but doesn't impose enforceable obligations on private-sector operators. The policy framework for protecting 15 designated critical infrastructure sectors is largely voluntary. Only limited mandatory obligations exist under the Economic Security Promotion Act, and those focus narrowly on supply-chain risks for a subset of 'specified essential infrastructure service providers'.[13] The result is a patchwork of inconsistent protections and reporting practices, hindering both internal cohesion and external threat intelligence sharing.

Private-sector participation has been central to the design and evolution of Japan's voluntary cybersecurity regime. Industry bodies, including the Japan Business Federation (*Keidanren*), play a significant role in shaping guidelines, risk frameworks and sector-specific norms through formal consultation and public–private collaboration platforms.[14] That approach has helped to ensure business buy-in and foster innovation, particularly in sectors such as manufacturing, telecommunications and financial services. However, it also means that the pace and depth of cybersecurity adoption vary significantly across industries. While Japan's industry-led model reflects a deliberate effort to avoid heavy-handed regulation, it places a premium on voluntary compliance and sectoral leadership—raising questions about baseline protection and the system's ability to respond to rapidly evolving threats.

That regulatory model presents significant challenges for businesses. Companies must reconcile non-binding sectoral guidance with enforceable instruments such as the Act on the Protection of Personal Information (APPI), which includes mandatory breach notifications. Multinational firms operating in Japan face additional difficulties aligning

domestic compliance obligations with more stringent international regimes—raising costs, reducing agility and hampering interoperability.[15]

Well-intentioned initiatives such as Japan's 'internet of things' (IoT) device labelling scheme (JC-STAR) and the push for 'software bills of materials' demonstrate a commitment to resilience, but, without enforceability, those measures risk adding to regulatory complexity without delivering consistent outcomes. The consequences are strategic as well as technical. Fragmentation in Japan's regulatory ecosystem limits its ability to engage deeply with like-minded partners on joint cyber resilience initiatives. Interoperability and intelligence sharing—essential to multilateral frameworks such as AUKUS Pillar 2—are constrained by incompatible systems, divergent legal authorities and limited mandatory reporting channels.

Japan's JC-STAR and software bills of materials

Japan's IoT device labelling scheme, JC-STAR, and its work on 'software bills of materials' (SBOMs) are the latest steps in a longer effort to improve cybersecurity. In 2019, the government launched the NOTICE program, which scans Japan's internet for insecure IoT devices and alerts their owners. That revealed how many devices still used weak passwords or outdated software.

To address this, the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency introduced JC-STAR in 2024—a voluntary label that shows which products meet basic security standards. The aim is to make it easier for consumers and businesses to choose safer products, while encouraging manufacturers to raise their standards.

At the same time, Japan has been promoting SBOMs—lists of all the software components inside a product—to improve transparency and reduce supply-chain risks. METI began this work in 2019, running pilot projects in sectors such as health care, cars and industrial systems, and published practical guidance in 2024.

In both cases, Japan has favoured a cooperative approach, using voluntary standards and market incentives rather than strict regulation—while leaving the door open to stronger measures in the future, such as making those standards part of government procurement rules.

South Korea: Barrier to resilience and innovation

South Korea's cybersecurity regulatory framework, while comprehensive in scope, is marked by fragmentation, complexity and bureaucratic friction. The country's cyber landscape is shaped by multiple overlapping laws and the involvement of numerous agencies with divergent mandates—an arrangement that complicates compliance and impedes effective threat response.

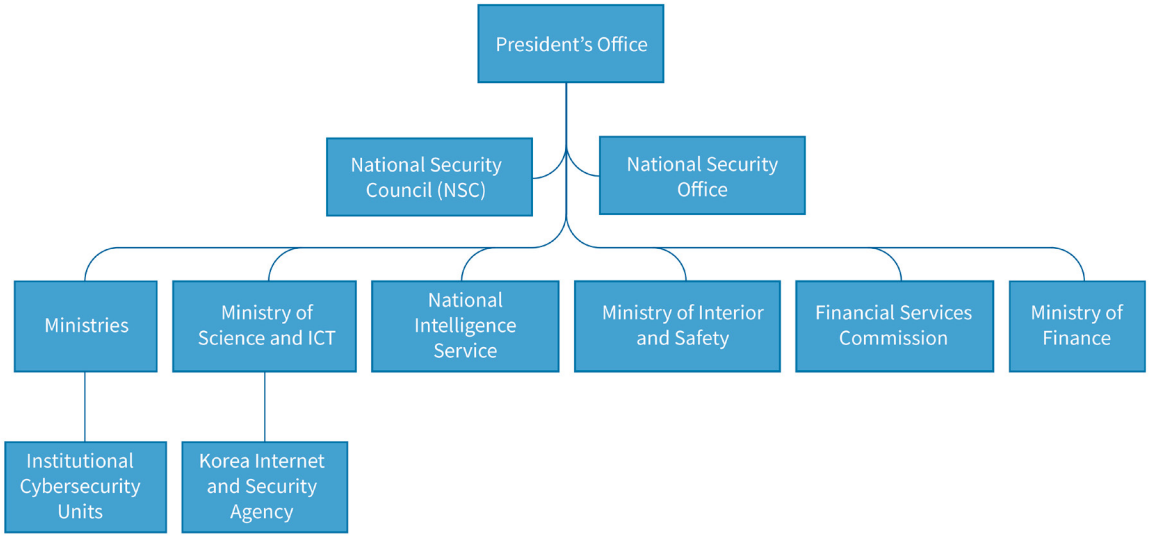
At the core of South Korea's cyber governance is the Ministry of Science and ICT (MSIT), supported by the Korea Internet and Security Agency (KISA), which oversees general cybersecurity under the Network Act. However, that central oversight is diluted by the prominent roles of other powerful institutions. The Personal Information Protection Commission (PIPC) enforces the Personal Information Protection Act (PIPA), the National Intelligence Service (NIS) handles critical infrastructure and national-security-related cyber threats, and sector-specific regulators—such as the Financial Services Commission and the Ministry of Health and Welfare—administer their own cybersecurity mandates.

South Korea's fragmented regime creates real compliance overhead—especially in convergent sectors such as fintech and digital health. In the absence of a single, comprehensive cybersecurity statute, firms must align obligations across PIPA (the enforceable, post-2020 centrepiece for personal-data governance and breach notification), remnants of the Network Act, the Act on the Protection of Information and Communications Infrastructure for critical ICT infrastructure, and sectoral laws (such as electronic finance / credit-information statutes)—each with distinct reporting channels and authorities. That dispersion produces overlapping oversight and higher compliance costs and can delay consistent security implementation.[16]

Despite those challenges, South Korea's private sector plays an important role in shaping and operationalising cybersecurity policy. Industry associations regularly provide input into regulatory revisions, technical standards and certification frameworks.[17] Leading technology firms and telecommunications providers, including KT, SK Telecom and Samsung, are often engaged by the government in pilot projects, threat-sharing platforms, and R&D initiatives under MSIT or KISA. However, that engagement tends to be concentrated among large conglomerates, with small and medium enterprises often lacking the capacity or channels to meaningfully participate in regulatory design. As a result, while industry–government cooperation has helped to advance cyber capabilities and sector-specific expertise, it has yet to fully address inclusivity, consistency or the creation of a level playing field across the economy.

South Korea's reliance on a 'positive regulation' model—in which new activities typically require prior authorisation—further compounds those challenges (Figure 2). The model, combined with regulatory overlap, slows innovation, discourages the agile adoption of new security measures and deters the rapid deployment of cyber capabilities.

Figure 2: South Korea's cyber governance landscape



Source: ASPI.

Coordination between key cyber authorities, notably MSIT/KISA and the NIS, remains a persistent point of friction. During major cyber incidents, overlapping responsibilities blur lines of command, hindering cohesive threat intelligence sharing and slowing unified responses. Efforts to develop a national digital identity framework have also been stymied by interagency misalignment and competing priorities—symptomatic of broader governance fragmentation.

While South Korea is clearly advancing a more proactive cyber posture, its current regulatory architecture poses structural challenges to achieving national cyber resilience and sustaining its role as a global technology innovator.

Indonesia: Risk to national resilience and regional stability

Indonesia's cybersecurity governance remains structurally weak, fragmented and underdeveloped—posing a significant challenge to its national resilience and the broader stability of the Indo-Pacific cyber environment. The absence of a dedicated, comprehensive cybersecurity law has left a critical gap in the country's ability to manage and respond to growing cyber threats.

Current regulation is based on a patchwork of legislative instruments—including the Electronic Information and Transactions (EIT) Law, the Personal Data Protection (PDP) Law, and Government Regulation no. 71 of 2019 (GR 71). While those laws address specific areas such as cybercrime, data protection and electronic system operations, they fall short of delivering a holistic, risk-informed cybersecurity framework. Key areas such as critical infrastructure protection, coordinated incident response and proactive cyber defence remain poorly regulated.

The result is a weakened institutional environment. The National Cyber and Crypto Agency (BSSN), which has been designated to lead Indonesia's national cybersecurity coordination efforts, operates without a strong legal foundation that clearly defines its authority, responsibilities and enforcement powers—undermining its ability to assert leadership across government. BSSN also suffers from chronic underfunding, with limited technical resources, staffing and budgetary support, all of which hinder its capacity to manage complex cyber threats and drive cross-agency coordination in a bureaucratic environment shaped by competing actors such as the Ministry of Communication and Digital Affairs and the National Police.[18] That has created overlapping responsibilities, unclear operational boundaries and interagency tensions that continue to undermine effective response and accountability.

Despite those institutional weaknesses, Indonesia's private sector has increasingly played a role in shaping the national cybersecurity conversation. Industry associations such as the Indonesian Telematics Society (MASTEL), as well as large telecommunications and financial firms, have participated in multistakeholder dialogues and public consultations, particularly in response to major cyber incidents and the drafting of new legislation such as the PDP Law and the proposed Cybersecurity Resilience Bill (RUU KKS). Private-sector actors have also provided input on standards development and voiced concerns over the operational feasibility and compliance costs of proposed regulations. However, industry involvement remains *ad hoc* and uneven, with limited institutionalised mechanisms for sustained public–private collaboration. As a result, while industry can serve as a critical partner in capacity-building and early threat detection, its role in long-term policy design and enforcement remains underutilised.

Efforts to introduce coherence through the long-delayed RUU KKS, reportedly set for passage in 2025, are promising—but fraught with risk. While the draft legislation seeks to define institutional roles, establish requirements for critical infrastructure protection and introduce standards for digital product certification, concerns persist over its potential to impose burdensome compliance costs, particularly on small and medium-sized enterprises. Additionally, questions remain about the Bill's alignment with international norms and its ability to overcome entrenched bureaucratic resistance.

The real-world consequences of that fragmented and reactive posture are stark. Indonesia is among the most targeted nations in Southeast Asia, regularly suffering from sophisticated and large-scale cyberattacks. The June 2024 ransomware attack on the National Data Centre, which crippled more than 200 public institutions, laid bare deep deficiencies in coordination, incident preparedness and infrastructure resilience. Other major breaches have compromised citizen data and eroded public trust in the state's ability to safeguard digital systems.

Part 2: Divergent shields: Regulating data, infrastructure and director responsibilities across the Indo-Pacific

In the previous section, this report presented an overview of how Australia, Japan, South Korea and Indonesia are pursuing divergent cybersecurity regulatory paths shaped by national events, priorities and strategic shifts.

In Part 2, the report examines the actualities of fragmentation in cybersecurity regulations in Australia, Japan, South Korea and Indonesia. This is done by considering regulatory controls imposed in relation to three key sub-areas: personal information handled by businesses; critical national infrastructure (CNI) assets; and governance by directors of businesses.

Those sub-areas face the highest regulatory scrutiny and divergence across jurisdictions, making them especially relevant for comparative analysis. They also reflect the growing trend of holding businesses—not just governments—responsible for cybersecurity outcomes. Other areas, such as cybercrime, are important but less directly tied to business operations and cross-border regulatory impacts.

Even where states adopt similar cybersecurity legislation, differences in political will have led to uneven implementation. Those gaps are often shaped by domestic political priorities, resource limitations and divergent threat perceptions,

resulting in inconsistent enforcement and oversight. Consequently, formal alignment doesn't always translate into practical interoperability or mutually reinforcing cybersecurity outcomes.

Key takeaways

- On the surface, Australia, Japan, South Korea and Indonesia regulate cyber risk management, privacy and critical infrastructure protection.
- Each mandates board-level oversight of cyber risks, breach-reporting obligations, and broadly similar corporate duties under their respective company laws. Those shared features reflect a common recognition of the role of regulation in driving national cyber resilience, particularly through industry standards and governance requirements, offering opportunities to pursue a harmonisation agenda.
- However, variations in national perspectives and capacities to enforce those regulations make regulatory alignment more difficult. The divergent internal models create a patchwork of national approaches that obstruct the development of shared standards, mutual recognition and coordinated cyber responses across the Indo-Pacific.

Regulating the protection of personal information

Privacy regulations in the four countries share substantial commonality in the wording or larger intent of the controls listed. For instance, businesses must implement risk-based, 'reasonable' and/or 'necessary' cyber risk management controls; demonstrate internal procedures for the handling of personal information; and are required to report data breaches to relevant authorities and individuals affected. Regulators in the four countries have the powers to audit compliance, mandate corrective action and impose penalties.

Unsurprisingly, the influence of the EU's General Data Protection Regulation (GDPR) is clear. Japan and South Korea have achieved 'adequacy status' with the EU,[19] Indonesia has adopted the GDPR as a model for its PDP Law,[20] and Australia is currently reviewing its Privacy Act to align more closely with it.[21] Despite that convergence, key differences remain in *how* and *when* businesses must comply—particularly in the level of detail required.

For example, while Japan's APPI Guidelines and Indonesia's Ministry of Communication and Digital Affairs Regulation no. 20/2016 explicitly mandate cybersecurity training, Australia's Privacy Act does not.[22] Still, Australian businesses would be likely to meet expectations by instituting such training, as the law implicitly requires responsible personnel to be 'security-literate'.[23] Such logic could be applied to any of the controls listed in Table 1.

The main area of regulatory fragmentation in this area—besides the definition of regulated entities—concerns reporting obligations. South Korea and Indonesia require breach reporting within 72 hours of discovery. In contrast, Australia and Japan allow up to 30 to 60 days for businesses to assess whether notification is necessary. However, industry standards[24] increasingly favour rapid identification and response, including timely assessments of harm to affected individuals and organisations.

Those divergences may have limited impact on firms operating solely within one jurisdiction. But for companies delivering similar digital products or services across multiple Indo-Pacific markets, fragmented privacy obligations complicate compliance, raise legal risk and increase operational overhead.

In summary:

- Australia has a risk-based approach focused on 'serious harm' with strict procedural expectations.
- Japan emphasises detailed reporting timelines and requires both preliminary and final reports.
- South Korea has volume-based triggers (for example, 1,000+ affected) with public notification obligations.
- The implementation of Indonesia's PDP Law is evolving, with a strong impetus on government oversight and early notification.

Table 1: Overview of personal data protection requirements and controls in Australia, Japan, South Korea and Indonesia

Australia	Japan	South Korea	Indonesia
Which entities are subject and at what threshold?			
Data breaches must be reported by government agencies, businesses earning over A$3 million per year, health providers, credit bodies and data traders if they involve unauthorised access or disclosure likely to cause serious harm that can't be prevented.	Data breaches must be reported if they involve sensitive personal information, are likely to cause financial loss, result from unauthorised targeting, or affect more than 1,000 individuals.	All entities at no specific threshold.	Any breach that affects personal data confidentiality or has significant public impact.
Who needs to be informed?			
The OAIC and data subjects.	The Personal information Protection Commission and data subjects.	The data subjects. PIPC/KISA where the number of affected data subjects is 1,000 or more.	The data protection authority and data subjects.
What's the reporting/notification timeline?			
'As soon as practical' after an 'eligible breach' has been determined within 30 days of becoming aware.	'Promptly' followed by a report within 30 or 60 days when breach involves 'an improper purpose'.	Within 72 hours of becoming aware of the breach.	Within 72 hours of becoming aware of the breach. Followed by written notification within 14 days after becoming aware of the breach.
What are required security controls?			
Organisations required to: • have strong internal governance, including strong supervision of personal information • appoint privacy officers • conduct regular reporting to the business's governing body • have a clear privacy policy and culture, and staff security training • conduct privacy impact assessments • conduct risk management for outsourcing arrangements.	Organisations required to: • establish privacy policies and internal rules • assign clear responsibilities for privacy management • implement breach-response procedures • conduct employee security training • apply technological controls such as access restrictions and data-loss prevention measures.	Organisations required to: • implement an internal management plan • appoint a privacy officer • establish a clear privacy policy • conduct privacy impact assessments.	Organisations required to: • implement risk-based operational and technical measures • maintain data confidentiality, using secure and reliable electronic systems • appoint privacy officers in certain cases under the PDP Act.

Regulating critical national infrastructure

The four countries pursue a similar principles-based approach to the management of cyber risks for regulated entities and CNI under their purview. They also rely on similar controls to discharge cyber risk management obligations, such as the need for internal cyber risk management; incident response and business continuity planning; penetration testing; patch management; and security training of personnel. Each jurisdiction has also assigned responsibility for compliance to company boards and/or designated (security) executives. In reviewing regulatory instruments for CNI, we've looked at:

- capstone regulatory frameworks
- coercive powers
- company directors' conduct.

Focusing on the above instruments provides a clear lens into how states define, enforce and operationalise cybersecurity obligations for CNI. Those three dimensions are representative because they collectively capture the full spectrum of how states define, enforce and internalise cybersecurity obligations across public and private actors. Capstone frameworks reveal the scope and architecture of national CNI policy; coercive powers show how governments intervene during threats or noncompliance; and directors' conduct reflects how responsibility is internalised at the corporate level.

Together, those areas expose the balance between state control and private-sector accountability in protecting national systems. Other elements, such as technical standards or industry guidelines, are important but often derivative of these core regulatory levers.

Capstone regulatory frameworks

In each of the four jurisdictions, both generalist and specific regulatory frameworks have been put in place, such as for:

- 'normal' private- and public-sector operators, which are entities that own or operate infrastructure or assets of the highest national-security sensitivity
- federal/central government entities and operators of critical infrastructure and critical information infrastructure
- 'owners of systems of national significance', which are assets or infrastructure deemed vital to national security, economic stability or public safety.

The last of those is a specific Australian arrangement. By the end of 2024, more than 200 systems had been declared to be systems of national significance by the Minister of Home Affairs, obliging them to comply with 'enhanced cyber security obligations'. When operators of critical infrastructure or critical information infrastructure are grouped as sectors, there's typically a sectoral regulator involved additionally, such as for communications, digital services and financial services.

For example, prudentially regulated entities covered by the South Korean regulatory instruments listed in Table 2 are required to report cybersecurity breaches to KISA and to the Financial Services Commission; and when they involve the breach of personal data *also* to the PIPC (see previous section).[25]

Table 2: Overview of authorised information security controls by authorities in Australia, Japan, South Korea and Indonesia

	Australia	Japan	South Korea	Indonesia
Reference	*Information security manual:* updated monthly	Cybersecurity Guidelines for Critical Infrastructure	Information Security Management System: updated annually	Guidelines for Information Security Management of Electronic Government Systems and Technical Standards and Security Procedures for Electronic Government Systems
Scope	Federal government Critical infrastructure operators	Operators of 14 designated critical infrastructure sectors	Regulated sectors	Government and 8 other sectors
Legal status	Mandatory for government	Non-binding but influential	Mandatory for key sectors	Mandatory for key sectors
Technical authority	ASD	NISC	KISA/MSIT	BSSN
Certifiability	No	No	Yes	No
Risk model	Support risk-based implementation of security controls	Risk-based principles	Enforce and certify a minimum baseline of security management (checklist)	Enforce and certify a minimum baseline of security management (checklist)
	22 control groups	3 principles; 10 safety objectives; 43 practices	5 domains; 102 controls	Based on the NIST Cybersecurity Framework
Breach reporting	Mandatory to ACSC	Encouraged, to NISC and sectoral CSIRTs	Mandatory to NIS/KISA	Mandatory to BSSN
Reporting timelines	12 hours for incidents with a 'significant impact' and 72 hours for incidents with a 'relevant impact'	Sectoral coordination	Immediate	Within 72 hours
International standards	Compatible with ISO 27001 Highly aligned with NIST CSF	Consistent with ISO 27001 Strongly aligned with NIST CSF	Derived from ISO 27001 Moderately aligned with NIST Inspired by EU NIS2	Aligned via national interpretation Moderately aligned with NIST

ACSC = Australian Cyber Security Centre; ASD = Australian Signals Directorate; BSSN = National Cyber and Crypto Agency (Indonesia); CSF = cybersecurity framework; CSIRTs = computer security incident response teams; KISA = Korea Internet and Security Agency; MSIT = Ministry of Science and ICT (South Korea); NISC = National Centre of Incident Readiness and Strategy for Cybersecurity (Japan); NIST = National Institute of Standards and Technology

Coercive powers

Each of the four jurisdictions diverges in the coercive powers available for state authorities to direct the conduct of any regulated entity in any context, whether in a crisis or otherwise. In Australia and Indonesia, the respective governments can issue such directions at any point in time. The Australian Home Affairs Minister is empowered by SOCI Act Part 3 to do so in the interests of national security, and the Indonesian Government can do so for any purpose, by EIT Law article 40A.

Only Australia has introduced powers for the government to intervene with coercive crisis-response powers. Under SOCI Act Part 3A, the Australian Home Affairs Minister can authorise the Secretary of the Department of Home Affairs to direct regulated entities to, in specified extenuating circumstances, provide certain information; and take or refrain from taking certain actions. As a last resort, under the SOCI Act Part 3A Division 5, ASD can be requested to intervene in the operation of a CNI asset, and the regulated entity for that asset is obliged to help ASD execute that request if ASD personnel ask for

such assistance.[26] If the entity fails to comply, law-enforcement personnel can assist ASD personnel to get access to its premises with the use of reasonable force against property.[27]

Those coercive powers are in contrast to the crisis support powers under, for example, the South Korean Network Act articles 10 and 11 and Article 7 of the Act on the Protection of Information and Communications Infrastructure (CICI Act) that govern when state agencies are required to provide technical support to regulated entities.

In summary:

- Australia focuses on high-assurance, intelligence-informed controls. It's risk-driven but not certifiable.
- Japan emphasises coordination, public–private partnership and flexibility—ideal for cross-sector operators.
- South Korea enforces strict certification and monitoring, which is valuable for companies requiring third-party assurance.
- Indonesia is in a regulatory buildup phase; it mandates BSSN compliance for all digital infrastructure deemed strategic.

Regulating the conduct of company directors

Cybersecurity is a core pillar of corporate governance, overseen by company boards as part of their duty to manage risk. In Australia, Japan and Indonesia, boards are legally responsible for managing the company, while in South Korea (and, in practice, Japan), boards supervise executive directors. Across all four countries, directors share similar statutory duties: loyalty, care, good faith, and acting in the company's best interests. Those reflect internationally accepted governance standards promoted by the G20 and OECD.

The strong alignment in legal duties underscores a shared recognition of the critical role that boards play in ensuring sound corporate governance—including in maintaining adequate cybersecurity compliance standards. That alignment would help to reduce fragmentation in cyber governance. In all four countries, directors are legally responsible for instituting and overseeing cyber risk management systems and taking a strategic approach to cyber resilience. Regulations for privacy and CNI require board oversight and internal policy. Regulators in both Japan and Australia have explicitly warned that insufficient board attention to cyber risk may constitute a breach of statutory duties, exposing directors to personal liability.

However, differences emerge in how that liability is defined and enforced. While directors in all four countries can face monetary penalties for loss caused to the company by breaching their duties, the legal thresholds and definitions vary (Table 3). South Korea goes furthest, allowing third parties to sue directors for harm caused by misconduct. Only Australia and Indonesia provide 'safe harbour' protections, shielding directors from liability under certain conditions. Additionally, only Australia empowers regulators to disqualify directors who violate their statutory duties (Corporations Act ss. 180(1), 181).

Table 3: Different perspectives on 'misconduct'

	Definition of misconduct	Threshold for liability	Safe harbour provision
Australia	Breach of statutory duties under Corporations Act (ss 180–184); includes negligence, bad faith, improper use of position/information	Negligence for duty of care; dishonesty for duty of good faith; objective reasonable director test	Yes – Business Judgment Rule (s. 180(2)) and Insolvency Safe Harbour (s. 588GA)
Japan	Breach of duty of loyalty (Article 355) and duty of care of a good manager; liability to third parties for bad faith / gross negligence	Negligence to company; gross negligence / bad faith to third parties	No statutory safe harbour; articles may limit liability for certain directors; judicial deference to business judgement
South Korea	Breach of duties of care/loyalty under Commercial Act; includes wilful or gross negligence; criminal 'breach of trust' for serious acts	Negligence to company; gross negligence / wilful misconduct to third parties; bad faith for criminal breach of trust	No statutory safe harbour; some judicial deference to reasonable decisions
Indonesia	Failure to act in good faith, with prudence, and without conflict of interest under Company Law no. 40/2007	Presumption of fault if company suffers loss; director must prove good faith, prudence, no conflict, and preventive action	Yes – statutory defence in Article 97(5) if conditions met (good faith, prudence, no conflict, preventive action)

Those divergences reflect regulatory fragmentation in enforcement rather than in substantive obligations. The core duties of directors—and their role in cyber governance—remain consistent and align with G20 and OECD principles. Directors who follow best practice corporate governance and demonstrate strong oversight of cyber risk are likely to meet their legal obligations across all four jurisdictions and avoid liability in practice.

In summary:

- Australia takes a strict enforcement approach—directors face personal liability and disqualification for failing to oversee cyber risks.
- Japan emphasises compliance through guidance—poor cyber oversight is framed as a breach of directors' legal duties.
- South Korea adopts an expansive liability model—directors may be held accountable by both companies and third parties.
- Indonesia balances responsibility with flexibility—directors must manage cyber risks but can access safe harbour protections.

Part 3: Towards coherence: Building a fit-for-purpose cyber harmonisation framework

So far, this report has argued that, while there are common regulations across the four countries, differences in cybersecurity governance have led to fragmented enforcement. As emerging technologies become more embedded in critical infrastructure and digital trade accelerates, those inconsistencies are no longer just technical frictions—they're becoming strategic liabilities that risk growing costlier over time. In short, those liabilities are weakening collective cyber resilience, delaying coordinated responses to transnational incidents and increasing compliance burdens for firms operating across jurisdictions.

To address this, Part 3 explores how existing international and regional platforms can serve as anchor points for regulatory convergence. Rather than relying on a single body, a lattice of mechanisms—including ASEAN, APEC and the OECD—offers a more adaptive and politically viable approach. Each forum brings distinct strengths: ASEAN offers regional legitimacy

and experience in confidence-building; APEC focuses on economic integration and technical interoperability; and the OECD provides normative leadership and links to global frameworks on privacy and digital security.

This multitrack model allows for progress across different levels and domains. Shared principles can be piloted in one venue, technical standards refined in another, and broader adoption promoted through a third. It also builds resilience: if one forum faces political deadlock, others can continue advancing harmonisation. Engaging across this lattice enables more inclusive, flexible and incremental pathways to cybersecurity regulatory alignment—which is crucial for managing complexity in the Indo-Pacific's dynamic and contested digital landscape.

Key takeaways

- Harmonisation doesn't imply rigid uniformity. In fact, there's no single authoritative mechanism for cybersecurity governance or international cooperation on cyber and digital issues in the Indo-Pacific. That fragmentation makes it necessary to adopt a layered approach—one that leverages different international platforms for specific, complementary roles. Rather than seeking one-size-fits-all solutions, each forum can contribute a distinct piece to the broader puzzle of regional cyber governance.
- With such an approach, we look for specific areas in cybersecurity regulation that can be standardised and be mutually recognised as 'adequately compliant'. Those areas could then serve as centres of gravity for countries to coalesce around. Each centre of gravity would require its own institutional bedding.
- Multilateral mechanisms, such as ASEAN, APEC and the OECD, offer platforms to facilitate harmonisation. While pursuing harmonisation through those platforms may carry the risk of further fragmentation, a strategically coordinated, multispeed and politically sensitive approach across those forums can instead deliver incremental yet coherent progress towards cybersecurity harmonisation.

The latticework of cyber governance in the Indo-Pacific

Association of Southeast Asian Nations

ASEAN represents an important legitimising platform for regional policy initiatives. Through its multilevel engagement platforms, at levels of leaders, ministers, senior officials and technical experts, the regional organisation can coordinate among the ASEAN-10 while serving as a central convening point for dialogue partners, and vice versa. The new iteration of the ASEAN Cybersecurity Cooperation Strategy, currently being drafted, provides a capstone for the work of the ASEAN Cybersecurity Coordinating Committee and its newly announced regional computer emergency response team (CERT) mechanism.

This constellation provides critical groundwork for confidence building, information sharing, forging cross-border operational readiness, and channel capacity-building. Furthermore, the pending Digital Economy Framework Agreement offers opportunities to align rules on data governance and interoperability. ASEAN's consensus-based decision-making model, paired with varied cyber capacities among its members, means that new policy issues take time to take root and will remain voluntary and non-binding. Therefore, it's also worth exploring the frontrunner roles of individual members, such as Singapore, which hosts the annual ASEAN Ministerial Conference on Cybersecurity and manages the ASEAN–Singapore Cybersecurity Centre of Excellence.

Asia–Pacific Economic Community

APEC, the regional forum promoting economic integration, has historically succeeded in embedding international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework into regional practice. Its Cross-Border Privacy Rules (CBPR) system, Mutual Recognition Arrangement for Telecommunications Equipment (TEL MRA), and cloud security recommendations demonstrate an ability to support sectoral progress in regulatory coherence. While APEC

can't enforce harmonisation, it plays a vital role in building shared principles and practical interoperability, in particular in telecommunications, insofar as it supports regional economic integration.

The Quad

The Quad grouping, consisting of Australia, India, Japan and the US, through its Senior Cyber Group, has articulated high-level standards of practices in software security, critical infrastructure protection and information sharing. It has published joint principles for secure software development and critical infrastructure protection. Yet, translating those into implementable, cross-border rules remains a challenge, particularly given internal divergences. For instance, India's distinct legal framework and strategic outlook complicate consensus. The Quad is most influential as an advanced group laying the groundwork for future regional discussions in ASEAN or APEC, for instance around mutual recognition of certifications and cyber incident response templates.

AUKUS and the G7

AUKUS and the G7 represent two high-trust, high-capacity forums. Initiatives undertaken for AUKUS Pillar 2, such as the recent exemptions to the US's International Traffic in Arms Regulations, show potential for streamlining regulation enabling technology sharing and setting standards for vendor assurance and emerging technologies, such as artificial intelligence and quantum computers. While exclusive to Australia by design, discussions are underway to share AUKUS outputs more widely, as technical blueprints, with partners such as Japan.

The G7 provides political momentum and regulatory diplomacy, especially through its Cyber Expert Group. So far, it has laid a foundation for financial sector cybersecurity and ransomware resilience. However, those initiatives require adaptation for an Indo-Pacific context. Similar to the Quad, there's a risk that AUKUS/G7-labelled initiatives will receive little buy-in from Indo-Pacific states because of broader geostrategic considerations.

Organisation for Economic Co-operation and Development

The OECD, although not a regional body, is a vital source of policy guidance and benchmarking for stakeholders in the Indo-Pacific. Its Best Practice Principles on International Regulatory Cooperation, digital security recommendations and international regulatory cooperation frameworks can underpin baseline harmonisation.

Issue-specific minilaterals

Some Indo-Pacific nations have taken global leadership roles on specific cyber issues. For instance, Australia's chairmanship of the International Counter Ransomware Initiative offers a platform to both coordinate policy and develop joint operational responses. Similarly, Australia plays a role in the Global Marine Transportation System Cybersecurity Forum, which comprises a group of like-minded countries' regulators. Such groups are well placed to spearhead urgent operational action, develop operating standards and facilitate information exchange.

Courses of action

The bodies and platforms outlined above each have something discrete to offer in terms of agenda-setting and standards-setting influence over cybersecurity regulation. Advancing a regulatory harmonisation agenda would suggest a strategic calibration of what, by whom, where and when. The following provides a practical starting point.

1. *Harmonise definitions by developing a shared lexicon*—for example, what qualifies as 'critical infrastructure', a 'cyber incident' or an 'essential service'. Legal differences pose challenges, so ASEAN and APEC should not only draft common terms but support translation into domestic law via model laws or guidance. Quad and OECD experts can aid by mapping local definitions to regional standards, easing legal interoperability.
2. *Standardise thresholds for incident reporting*, which will enhance the effectiveness and expediency of incident responses across the region. Many states lack enforceable mechanisms for timely private-sector reporting. The Quad could pilot harmonised protocols to test enforceability. ASEAN's Regional CERT, Asia-Pacific CERT (APCERT) and Pacific Cyber Security Operational Network (PacSON) could develop shared templates—covering compliance incentives, timelines and penalties—while promoting mutual recognition of reporting standards to strengthen legal interoperability.
3. *Promote best practice information security guidelines*, for instance on the basis of the Australian Government's *Information security manual*. Coalescing around an existing credible and authoritative baseline will help foster interoperability without overriding national sovereignty. Those standards offer scalable, risk-based templates that emerging economies can tailor to their capacities. Australia, through its various regional cyber diplomacy channels, could lead or coordinate such an effort.
4. *Coordinate supply-chain risk-management approaches*. As supply chains become increasingly politicised, the coordination of approaches to risk management is instrumental so that each vendor is assessed to the same type of security assessment and transparency criteria. Given its previous work on common standards and principles and the risk acceptance of its members, the Quad is well placed to lead on this.
5. *Harmonise data-protection obligations*—especially around personal data—to unlock secure cross-border digital trade. APEC's CBPR and ASEAN's Model Clauses align with global norms. Implementation needs technical support and guidance on interoperability, such as impact assessments and adequacy decisions. Regional dialogues and bilateral cooperation can address enforcement gaps, such as cross-border redress and jurisdictional authority.
6. *Synchronise cyber capacity building* so that the great variety of investments in people, products, infrastructure and institutions across the Indo-Pacific is designed with similar strategic aims and principles in sight, while addressing operational capacity shortfalls on the basis of regional appropriateness and convergence.
7. *Advance reciprocity agreements* advanced to enable mutual recognition of cybersecurity certifications, reporting duties and compliance across overlapping jurisdictions. The OECD or APEC could operationalise this by identifying aligned frameworks and piloting sector-specific schemes. Elevating mutual recognition from principle to action would help to deliver concrete progress towards regulatory harmonisation, particularly in finance, telecommunications and critical infrastructure.

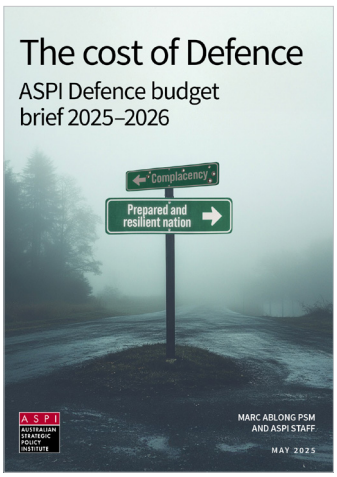
Notes

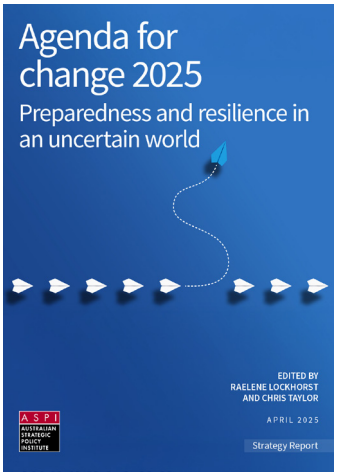
1 'A Call to Action to Maximize Cyber Defenses by Better Aligning Cybersecurity Regulations,' *Microsoft*, April 2025, online.
2 Joshua Goldfarb, 'The Hidden Cost of Compliance: When Regulations Weaken Security,' *Security Week*, 27 February 2025, online.
3 Trevin Edgeworth, 'Failure, Rinse, Repeat: Why do Both History and Security Seem Doomed to Repeat Themselves?,' *Security Week*, 27 February 2025, online.
4 Pangambam S, 'Transcript: Commisars and Capitalists: Politics, Business and New World Order at Raisina Dialogue,' *The Singju Post*, 22 March 2025, online.
5 Atsushi Teraoka, 'Japan tech companies scramble to comply with EU cybersecurity laws,' *Nikkei Asia*, 4 December 2024, online; Monica Behura, 'Big Tech pushes for delay in India's DPDP Rules on Children's Data, Cross-Border Transfers,' *The Economic Times*, 20 March 2025, online.
6 'Roundtable: Cyber Resilience in the Indo-Pacific,' *Asia Policy* vol. 20:2 (April 2025), online.
7 Broadly, the cybersecurity community refers to national cybersecurity agencies, computer emergency response teams (CERTs), incident-response teams, and private-sector cybersecurity communities. While sharing similar duties, CERTs and incident-response teams have different scopes and structures. CERTs are formal, often institutionalised, teams established to handle cybersecurity incidents within a specific entity. Incident-response teams are broader, more informal, networks that collaborate to respond to and learn from cyber incidents.
8 On internet penetration rates, see 'Individuals using the internet (% of population)—Australia', World Bank, online. The broader category of 'digital activity', as measured by the Australian Bureau of Statistics, accounted for roughly 6.1% of Australia's total value added in 2020–21 and remained stable at around 6.3% through 2021–22. See Australian Bureau of Statistics, 'Digital activity in the Australian economy, 2021–22', Australian Government, 27 October 2023, online.
9 For instance, Australia is considered a 'role model' in the International Telecommunications Union's Global Cybersecurity Index, with its legal measures scoring as among its greatest strengths. See 'Global Cybersecurity Index 2024, 5th edition', International Telecommunications Union, online.
10 Bart Hogeveen, 'Qantas data breach shows compliance doesn't always mean protection and resilience', *The Strategist*, 4 July 2025, online.
11 Australian Prudential Regulation Authority, 'APRA takes action against Medibank Private in relation to cyber incident', Australian Government, 27 June 2023, online.
12 Office of the Australian Information Commissioner, 'OAIC takes civil penalty action against Medibank', Australian Government, 5 June 2024, online.
13 'Japan: Impact of the Economic Security Promotion Act on overseas businesses that provide services to Japanese companies designated as essential social infrastructure service providers in Japan', *Lexology*, 9 August 2024, online.
14 For instance, *Keidanren* published its own declaration of cybersecurity management in March 2018. See 'Declaration of Cyber Security Management', *Keidanren*, March 2018, online.
15 'Japanese personal data compliance: APPI, cross-border transfers & global governance', *Japan Compliance*, 6 May 2025, online.
16 Kwang Bae Park, Sunghee Chae, Hyein Lee, 'Korea's cybersecurity regulations and enforcement related to security incidents', *International Cybersecurity Law Review*, 2021, 2:47–55, online.
17 'Strengthening cybersecurity and resilience of critical infrastructure: insights from the Republic of Korea and other digital nations', *World Bank*, December 2023, online.
18 Gatra Priyandita, 'Indonesia', in 'Roundtable: Cyber Resilience in the Indo-Pacific', *Asia Policy*, April 2025, 20(2), online.
19 'Adequacy decisions', European Commission, online.
20 'Data protection & privacy 2025: Indonesia', Chambers and Partners, 11 March 2025, online.
21 'How has GDPR influenced the evolution of data protection in APAC?', A&O Shearman, 24 May 2023, online.
22 On APPI, see article 10–4. On Indonesia's Ministry of Communication and Digital Affairs Regulation no. 20/2016, see article 5(4)(a). On Australia's Privacy Act, see section 15, Schedule 1, ss. 1.2–1.6, 11.1.
23 Office of the Australian Information Commissioner, *Chapter 1: Australian Privacy Principle 1—Open and transparent management of personal information*, Australian Government, July 2019, 5, online.
24 See, for example, National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, US Government, 26 February 2024, online.
25 CICI Act, article 13(1); EFT Act, article 21–5.
26 SOCI Act, ss. 5 (definition of 'approved staff member of the authorised agency'), 35BB.
27 SOCI Act ss. 5 (definition of 'constable'), 35BB(1)(c)-(d), 35BC, 35BE; *Crimes Act 1914* (Cth) s 3(1) (definition of 'constable').

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
APEC	Asia–Pacific Economic Cooperation
APPI	Act on the Protection of Personal Information (Japan)
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASEAN	Association of Southeast Asian Nations
BSSN	National Cyber and Crypto Agency (Indonesia)
CBPR	Cross-Border Privacy Rules
CERT	computer emergency response team
CNI	critical national infrastructure
CSF	cybersecurity framework
EIT Law	Electronic Information and Transactions Law (Indonesia)
EU	European Union
GDP	gross domestic product
GDPR	General Data Protection Regulation (EU)
ICT	information and communications technology
IoT	internet of things
KISA	Korea Internet and Security Agency
METI	Ministry of Economy, Trade and Industry (Japan)
MSIT	Ministry of Science and ICT (South Korea)
NIS	National Intelligence Service (South Korea)
NISC	National Centre of Incident Readiness and Strategy for Cybersecurity (Japan)
NIST	National Institute of Standards and Technology
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
PDP Law	Personal Data Protection Law (Indonesia)
PIPA	Personal Information Protection Act (South Korea)
PIPC	Personal Information Protection Commission (South Korea)
R&D	research and development
RUU KKS	Cybersecurity Resilience Bill (Indonesia)
SBOMs	software bills of materials (Japan)
SOCI Act	*Security of Critical Infrastructure Act 2018* (Australia)
TEL MRA	Mutual Recognition Arrangement for Telecommunications Equipment
TTPs	tactics, techniques and procedures

Some recent ASPI publications





ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

ISSN 2200-6648