NO. 2024-06, NOVEMBER 2024
ISSN: 2086-8154

Economic Research Institute for ASEAN and East Asia

Policy Brief

Strengthening ASEAN's Cybersecurity: Collaborative Strategies for Enhanced Resilience and Regional Cooperation

Mahirah Mahusin and Hilmy Prilliadi

Key Messages:

- Effective cybersecurity requires strong cooperation between governments, private sectors, and international bodies, with a focus on regional strategies and information-sharing mechanismse.
- Strengthening and updating legal frameworks are essential for combating cybercrime and adapting to evolving threats.
- A standardised cybersecurity taxonomy across ASEAN will improve coordination during incidents, enhancing regional response effectiveness.
- Increased investment in cybersecurity capacity-building, particularly for MSMEs, will strengthen resilience and improve compliance with international standards.

As ASEAN's digital economy continues to expand, the region faces escalating cybersecurity risks with significant potential costs. This policy brief examines ASEAN's current cybersecurity landscape, underscoring the need for enhanced cooperation and comprehensive strategies to address the rising threat of cyberattacks. The economic impact of cyberattacks in ASEAN is already substantial, affecting both public and private sectors. This brief reviews existing efforts such as the ASEAN Cybersecurity Cooperation Strategy 2021–2025 and the ASEAN Regional Computer Emergency Response Team (ASEAN CERT), recommending the establishment of a shared cybersecurity taxonomy, capacity-building initiatives, and legal framework updates to bolster cybersecurity. Key policy recommendations encourage robust multi-stakeholder collaboration at national and regional levels.

Mahirah Mahusin
Manager for Digital Innovation and Sustainable Economy at ERIA

Hilmy Prilliadi
Reseach Associate at ERIA

The global cost of cyberattacks is projected to escalate from US$9.22 trillion in 2024 to US$13.82 trillion by 2028 (Statista, 2024). In ASEAN, cyber threats are also rising, driven by increased connectivity, the integration of advanced technologies like artificial intelligence and cloud computing, and the region's growing geopolitical importance. By July 2023, economic losses from data breaches in ASEAN had reached US$3.05 million, an increase from US$2.87 million in 2022 (IBM, 2023). At the country level, Singapore saw a 174% surge in phishing attempts from 2021 to 2022, while cyberattack costs in Indonesia reached US$4.79 billion in 2022, with projections nearing US$6.5 billion by 2028 (Statista, 2023a).

Cyberattacks not only impose economic burdens but also erode public trust and tarnish the utations of both public and private sector providers. These attacks can target governments and critical information infrastructure (CII) – including energy, telecommunications, finance, transportation, defense, and government agencies – as well as private entities and individuals. SMEs, which account for 43% of cyberattack targets (Brooks, 2022), are particularly vulnerable, often lacking the technical resources needed to protect themselves. ERIA's ASEAN digital divide survey reveals that only 68.5% of small firms have adopted cybersecurity software, leaving a large number unprotected (Kasih, 2023).

Addressing cyberattacks requires robust, multi-stakeholder cooperation in cybersecurity. This involves enhancing the incident response capabilities

of national entities, strengthening inter-agency collaboration for threat identification and mitigation, and fostering workforce development in cybersecurity. While some ASEAN Member States (AMS) have established comprehensive emergency-response networks with private sector involvement, others lack complete plans and rely on government-private sector information-sharing networks. Many AMS remain in early stages of cybersecurity development, without robust mechanisms for public–private partnerships (PPPs) in cybersecurity information sharing (Cheng and Chow Mae, 2023).

The ASEAN Cybersecurity Cooperation Strategy 2021–2025 outlines five key pillars for building a secure and resilient cyberspace, including promoting cyber readiness, strengthening regional policy coordination, enhancing trust, developing capacities, and fostering international collaboration.

Alongside bilateral coordination, the ASEAN Regional Computer Emergency Response Team (ASEAN CERT) provides a platform for region-wide information sharing on cyber incident response, supplementing national CERT operations within each AMS. This mechanism supports commitments under the ASEAN Digital Economy Framework Agreement (DEFA) and can facilitate the development of an ASEAN CERT Information Exchange Mechanism and an annual ASEAN cybersecurity threat landscape ort, offering insights into emerging threats, trends, and best practices. However, the ASEAN Cybersecurity Coordinating Committee's (Cyber-CC) annual meetings reveal a gap in real-time coordination and response, necessitating ad-hoc meetings as needed for urgent incident responses.

A shared cybersecurity taxonomy across ASEAN would enable uniform assessment of cyber incident impacts across AMS. Currently, AMS definitions for incidents vary; while some AMS categorise incidents into levels, terms like 'widespread disruption' and 'crisis' lack consistent definitions. Some AMS have defined criteria for 'serious cyber information-security incidents,' triggering coordinated national responses, but several AMS have yet to establish similar definitions (Sari, 2023).

A shortage of skilled cybersecurity professionals further challenges AMS' operational capabilities, with demand for expertise in areas like behavioral analytics and digital forensics remaining high even in digitally advanced countries (APCERT, 2022). To address these needs, ERIA is developing an Internet Infrastructure Health Metrics Framework for AMS. This framework provides insights into AMS internet health, helping to identify areas requiring capacity building to support secure, sustainable digital infrastructure (CyberGreen, 2021).

Figure 1 presents fourteen key attributes that significantly influence cybersecurity policy development.

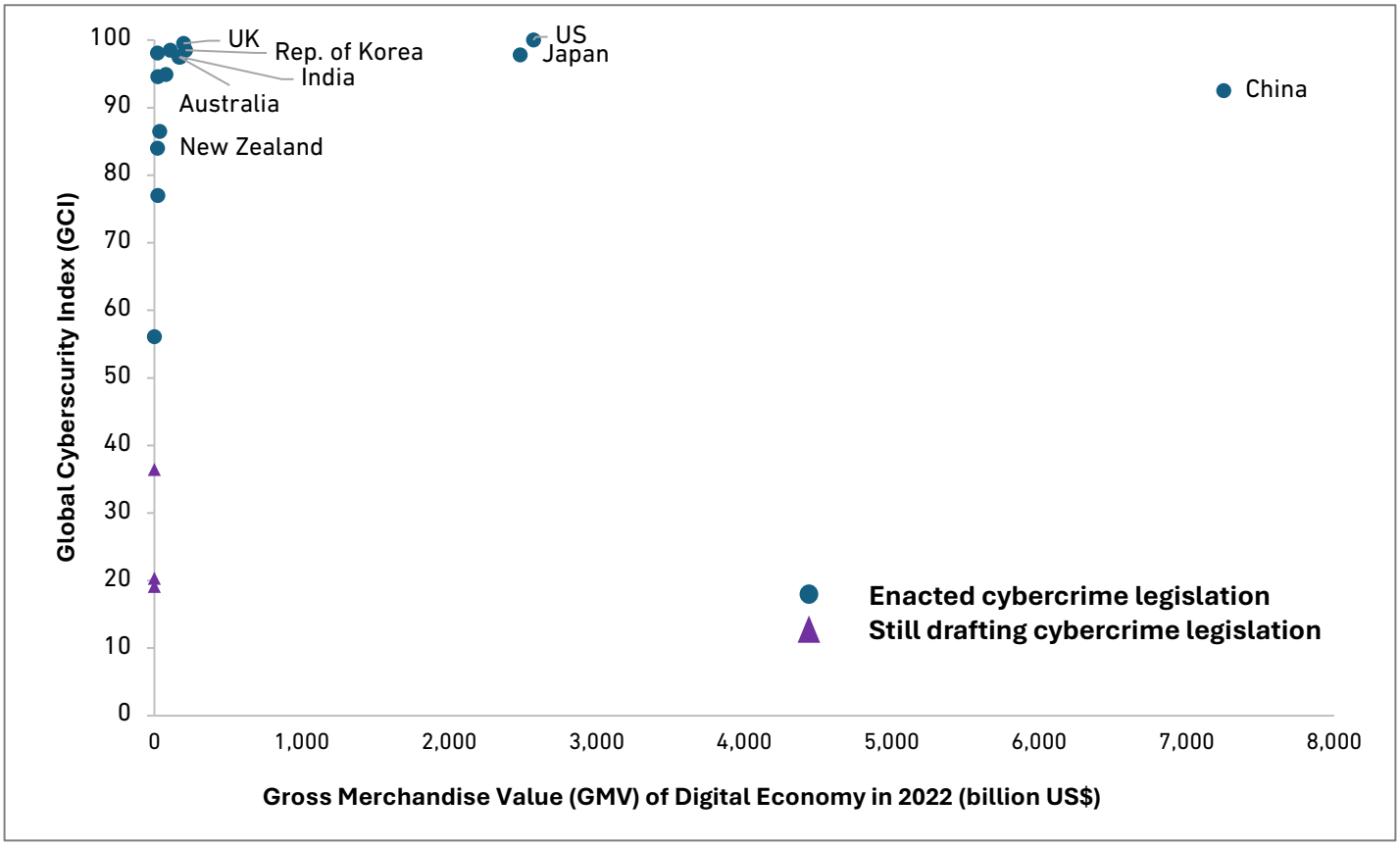
Figure 1: Attributes Impacting Cybersecurity Policy Development

Source: Authors based on Mishra et al., 2022.

These attributes are dynamic and must adapt to the continuously evolving cybersecurity landscape. They provide valuable guidance for improving policies, as a single policy cannot accommodate all stakeholders or situations. ASEAN Member States can leverage these attributes to develop comprehensive regional cybersecurity strategies essential for secure cyberspace. Beyond enhancing cybersecurity, these attributes impact AMS economies. The private sector closely monitors each nation's cybersecurity and data policies due to their potential effects on digital trade.

Figure 2 shows that countries with high Global Cybersecurity Index (GCI) rankings often demonstrate significant Gross Merchandise Value (GMV) in their digital economies. This correlation highlights the importance for countries to prioritise and invest in comprehensive cybersecurity strategies to support digital economic growth. Notably, three AMS still lack adequate cybersecurity legislation.

Figure 2: Relationship between Cybersecurity Readiness and GMV in Selected Countries



Source: Authors based on UNCTAD, 2021; Statista, 2023b; UNESCAP, n.d.

The EU and the US each take distinct approaches to cybersecurity regulation. In 2013, the EU launched its cybersecurity policy, proposing the Network and Information Security Directive to address the growing need for information security in the face of increased ICT use. This directive was complemented by the establishment of the European Cyber Crime Centre to assist in protecting citizens and businesses through crime analysis and awareness initiatives on emerging cyber-attack trends. Meanwhile, the US undertook a Cyberspace Policy Review in 2009 with short- and mid-term goals that emphasised building essential cybersecurity infrastructure and reducing cyber threats. The US approach favours optional government intervention in cybersecurity, encouraging private sector self-regulation and viewing public–private partnerships as recommended rather than required.

Policy Recommendations:

- **Develop comprehensive cybersecurity strategies** at both national and regional levels, with immediate emphasis on implementing the ASEAN Cybersecurity Cooperation Strategy 2021–2025.
- **Enhance enforcement capacity and update laws** to effectively combat cybercrime. Stronger enforcement and regular updates to legal frameworks are crucial to deter, prosecute, and adapt to cyber threats.

- **Create balanced cybersecurity policies and legal frameworks** that foster a supportive environment for digital economic growth and innovation while effectively addressing cybersecurity risks.
- **Continue progress towards operationalising UN cyber norms** to build a cyber-emergency response capability tailored to regional needs.
- **Establish a regional cybersecurity taxonomy** to ensure clarity and consistency in communication during cyber emergencies. This should include consensus on the sectors to be categorised as critical information infrastructure (CII).
- **Operationalise the ASEAN CERT** to facilitate assistance requests by AMS and assemble expertise across AMS and external partners to respond to cyber threats, with each AMS contributing based on capacity.
- **Promote public–private partnerships** (PPPs) in cybersecurity through collaborative mechanisms and integrated orting platforms to enhance cyber risk detection and response.
- **Invest in regional cybersecurity capacity-building initiatives** like the ASCCE (ASEAN-Singapore Cybersecurity Centre of Excellence) and AJCCBC (ASEAN–Japan Cybersecurity Capacity Building Centre).
- **Develop cost-effective cybersecurity guidelines** for MSMEs, supported by training on cybersecurity's importance. This can be reinforced with government-backed cybersecurity certification for SMEs demonstrating high standards, particularly those aiming to meet international norms.

Conclusion

Enhanced cybersecurity is crucial for ASEAN's digital economy growth. By adopting a collaborative approach across public and private sectors, ASEAN can build a resilient and secure digital landscape that supports both economic growth and national security. Continued commitment to regional cooperation, legal framework updates, and capacity-building efforts will position ASEAN as a secure and trusted region for digital innovation.

References

APCERT (2022), *Annual ort 2022*. https://www.apcert.org/documents/pdf/APCERT_Annual_ort_2022.pdf

Brooks, C. (2022, 24 January), *Cybersecurity in 2022* – A Fresh Look at Some Very Alarming Stats. Https://Tinyurl.Com/4jfyvd2b.

Cheng, J.H. and Chow Mae (2023, 6 November), *Strengthening Cyber Resilience in Southeast Asia*. https://Tinyurl.Com/3urkhhd5.

CyberGreen (2021), *Internet Infrastructure Health Metrics Framework* (IHMF).

IBM (2023), *Cost of a Data Breach ort 2023*. https://www.ibm.com/orts/data-breach

Kasih, M.C. (2023), 'Fostering ASEAN's Digital Future through Cybersecurity Policies and Human Empowerment', *ERIA Policy Brief 2023-02*. https://www.eria.org/publications/fostering-aseans-digital-future-through-cybersecurity-policies-and-human-empowerment

Mishra, A., Y.I. Alzoubi, M.J. Anwar, and A.Q. Gill (2022), 'Attributes Impacting Cybersecurity Policy Development: An Evidence From Seven Nations', *Computers & Security*, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Sari, M.N. (2023), ASEAN's Regional Effort on Cybersecurity and Its Effectiveness. *Keio SFC Journal*, 23.

Statista (2023a, 4 September), *Estimated Annual Cost of Cyber Crime in Indonesia From 2018 to 2028*. https://Tinyurl.Com/4newc863.

Statista (2023b, 22 November), *Annual Gross Merchandise Value (GMV) of the Internet Economy in Indonesia From 2015 to 2023 With a Forecast for 2025, by Sector*. https://Tinyurl.Com/2c3b9d6y.

Statista (2024, 22 February), *Cybercrime Expected To Skyrocket in Coming Years*. https://Tinyurl.Com/248su3nd.

UNCTAD (2021), *Cybercrime Legislation Worldwide*. https://Unctad.Org/Page/Cybercrime-Legislation-Worldwide.

UNESCAP (n.d.), *Cybersecurity Development in Lao PDR*. Retrieved 4 February 2024, from https://tinyurl.com/55nwz796

Sentral Senayan II, 5th, 6th, 15th floors
Jalan Asia Afrika No. 8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460 Fax: (62-21) 57974463
E-mail: contactus@eria.org