

ERIA POLICY BRIEF

Measuring Cyber Risk Together: Strengthening ASEAN Cybersecurity Information Sharing

Key Messages:

- ASEAN's uneven cybersecurity capabilities and growing digital interdependence make regional information sharing essential to prevent cyber risks from cascading across borders.
- ASEAN should strengthen national cybersecurity statistics systems and develop a Common Cybersecurity Statistics Framework to produce comparable, decision-ready evidence.
- Implementation should be phased, beginning with pilots amongst more advanced member states and supported by capacity building, trusted intelligence sharing, and participation across the region.

ASEAN's growing digital integration is increasing exposure to cross-border cyber risks, but cybersecurity data remain fragmented across jurisdictions and sectors. Differences in definitions, reporting requirements, and institutional capacity make it difficult to compare risks, identify regional vulnerabilities, and develop evidence-based policies. This policy brief proposes a two-level approach: strengthening national systems for collecting and analysing cybersecurity statistics, and establishing an ASEAN Common Cybersecurity Statistics Framework to make national data comparable. It also recommends strengthening trusted regional intelligence-sharing mechanisms and sequencing implementation according to member states' different levels of capacity. Together, these measures would help ASEAN move from fragmented incident reporting towards a more systematic regional understanding of cyber risk.

ASEAN's Cyber Risk Demands Better Information Sharing

Digital integration multiplies economic opportunity, but it also multiplies the channels through which cyber risk can spread. As ASEAN's economies grow more interconnected, a ransomware attack on a logistics provider in one member state can disrupt supply chains across several others, and a data breach in one financial system can erode investor confidence region-wide. In 2024 alone, businesses in the region faced more than 135,000 ransomware attacks (Kaspersky, 2025), while the average cost of a data breach in ASEAN rose from approximately US\$2.71 million in 2020 to an estimated US\$3.67 million in 2025 (IBM, 2025).

These regional challenges mirror a global trend. Cybersecurity risk worldwide is accelerating, fuelled by advances in artificial intelligence (AI), geopolitical fragmentation, and the growing complexity of supply chains, with AI in particular strengthening defences while enabling more sophisticated attacks. Reflecting these pressures, the WEF Global Risks Report 2026 places cyber insecurity amongst the top ten global risks by potential impact.

Managing this risk requires evidence that flows from individual incidents to policy decisions. When organisations report incidents, those reports should feed into national statistics and analysis, which can then be combined into comparable regional data to guide policymaking. The chain therefore runs from incident reporting to national statistics and analysis, from national analysis to comparable regional statistics, and from those statistics to strategic evidence and intelligence for policy makers. Across ASEAN, this chain breaks at the start. Cybersecurity statistics remain fragmented,

Please cite this content as:

ERIA (2026), 'Measuring Cyber Risk Together: Strengthening ASEAN Cybersecurity Information Sharing', *ERIA Policy Brief 2026-8*. Jakarta: ERIA. Available at: <https://www.eria.org/publications/measuring-cyber-risk-together--strengthening-asean-cybersecurity-information-sharing>

©ERIA, 2026.

DISCLAIMER:

All rights reserved. Material in this publication may be freely quoted or reprinted with proper acknowledgement.

use different definitions, and rarely move beyond national borders, so governments cannot compare their exposure, spot shared vulnerabilities, or base regulation and investment decisions on solid evidence.

To close this gap, each member state would benefit from a national institution responsible for cybersecurity statistics, one that sets common metrics, brings together reporting from all sectors, and produces the analysis needed for sound policy and regional co-operation. This statistical chain is distinct from the operational one, in which real-time threat intelligence flows between Computer Emergency Response Teams (CERTs) to support immediate incident response. The two are complementary, since statistical institutions would measure systemic risk over time while Computer Emergency Response Teams continue to manage individual incidents, and neither can substitute for the other. Strategic evidence and intelligence for policymakers are the endpoints of the statistical

chain, just as incident response is the endpoint of the operational one. Strengthening both would allow ASEAN to act on immediate threats while understanding the systemic risks that lie behind them.

Table 1 shows that ASEAN's cybersecurity capabilities vary considerably, creating different starting points for regional information sharing. A regional framework therefore needs common minimum standards while allowing implementation to reflect national capacity. ASEAN has recognised these disparities, with the ASEAN Cybersecurity Cooperation Strategy 2021–2025 linking incident response and threat information sharing to wider goals on trust, capacity, and international co-operation. At the ministerial level, the Ha Noi Digital Declaration of January 2026 situates this work within a broader shift from connectivity to connected intelligence, while the ASEAN Digital Masterplan 2030 provides a platform for engagement with dialogue partners and international organisations.

Table 1. ASEAN Cybersecurity Maturity by Pillar and Tier

No	Country	Tier Performance	Legal	Technical	Organisation	Capacity	Co-operation
1	Indonesia	T1: Role-Modelling	20	20	20	20	20
2	Malaysia	T1: Role-Modelling	20	20	18.82	20	20
3	Singapore	T1: Role-Modelling	20	20	20	19.86	20
4	Thailand	T1: Role-Modelling	20	20	19.22	20	20
5	Viet Nam	T1: Role-Modelling	20	20	20	19.74	20
6	Philippines	T2: Advancing	20	19.11	19.51	17.17	17.7
7	Brunei	T3: Establishing	17.2	14.89	11.35	10.76	16.18
8	Myanmar	T3: Establishing	15.34	10.9	13.06	14.42	20
9	Cambodia	T4: Evolving	11.82	4.56	8.3	6.12	6.22
10	Lao PDR	T4: Evolving	10.38	6.18	5.52	2.05	9.61
11	Timor-Leste	T5: Building	6.22	0	2.9	1.01	6.69

Source: ITU Global Cybersecurity Index (GCI), 2024. Notes: GCI scores are formulated based on data provided by ITU member states and contributing partners.

Beyond ASEAN, international experience offers instructive models. The European Union's NIS2 Directive established tiered reporting across 27 member states, supported by the European Union Agency for Cybersecurity (ENISA), which aggregates national incident data into comparable regional statistics, while Australia's Cyber Security Act 2024 introduced a limited use obligation that protects voluntarily shared information from regulatory enforcement, directly addressing the reluctance that deters disclosure. Japan's Active Cyber Defense Act of 2025 created a National Cybersecurity Office with authority to co-ordinate cross-sector intelligence sharing between government and critical infrastructure operators.

Strengthening Cybersecurity Statistics and Breach Reporting in ASEAN

As Table 2 shows, breach-notification obligations are now widespread within ASEAN, but their timelines and scope diverge considerably across member states. The emerging alignment in public company breach notification practice, by contrast, suggests the region is closer to comparability in some domains than in others.

A well-designed reporting framework also requires agreement on what to collect. Table 3 sets out four minimum data categories, the actor involved, the action taken, the asset affected, and the attributes of the incident, which together would enable consistent aggregation across sectors and jurisdictions.

Equally important are the governance principles that shape how information is reported and shared. Table 4 shows four foundations of an effective reporting system, including confidentiality, protection for good-faith reporters, standardisation, and independence

from enforcement, which together encourage earlier disclosure and turn reporting from a static obligation into a dynamic system of digital resilience.

Table 2. ASEAN National Cyber Security Statistics and Breach Notification Requirements

Countries	National Cyber Statistics	Publishing National Authority	CII Breach Notification	Public Company Breach Notification
Indonesia	Annual Cybersecurity Report	Komdigi Computer Security Incident	Mandatory, within 24 hours	Mandatory, within 72 hours
Malaysia	General Incident Classification Statistics	Malaysia Computer Emergency Response	Mandatory, within 6 hours	Mandatory, within 72 hours
Singapore	Singapore Cyber Landscape	Cyber Security Agency of Singapore	Mandatory, within 2 hours	Mandatory, within 3 days
Thailand	Thailand Cybersecurity Landscape	Thai Computer Emergency Response	Mandatory, without delay	Mandatory, within 72 hours
Viet Nam	National Cybersecurity Report	Ministry of Information and Communications	Mandatory, immediately	Mandatory, within 72 hours
Philippines	National CERT Cybersecurity Statistics	National Computer Emergency Response	Mandatory, within 24 hours	Mandatory, within 72 hours
Brunei Darussalam	National Cyber Incident Statistics	Brunei Computer Emergency Response	Mandatory, within a specified period	Mandatory, within 3 days

Source: Authors’ compilation from national cybersecurity legislation, regulations, and publications of respective ASEAN Member States.

Table 3. Minimum Data Categories for National Cybersecurity Statistics

Actor	Action	Asset	Attribute
Actor type	Incident type	Data	Timeframe
Target sector	Attack method	Criticality	Impact level

Source: Authors’ synthesis based on VERIS Framework (2026).

Table 4. Main Governance Principles for Effective Cyber Incident Reporting Systems

Confidentiality <i>Secure information</i>	Good-faith Reporting <i>Protection for good-faith reporters</i>	Standardisation <i>Common reporting structure</i>	Independence <i>Separation from enforcement authority</i>
---	---	---	---

Source: Authors’ synthesis based on Ebert et al. (2025), Cyber Threat Alliance and Institute for Security and Technology (2023) and various reports

Policy Recommendations

Closing the cybersecurity statistics gap requires co-ordinated national and regional action, sequenced across four priorities.

First, build national capacity to produce comparable cybersecurity statistics. Each member state should establish or designate a national institution responsible

for cybersecurity statistics, tasked with standardising metrics, consolidating cross-sector incident data, and publishing regular analytical reports. Where Computer Emergency Response Teams manage individual incidents, this function measures systemic risk over time, giving governments the evidence base to price cyber risk and direct investment where it is most needed.

Second, create an ASEAN Common Cybersecurity Statistics Framework. ASEAN should harmonise definitions, taxonomies, severity scales, and minimum data fields while preserving national flexibility. The Framework would act as a translation layer that renders diverse national inputs regionally comparable, enabling benchmarking and co-ordinated policy responses.

Third, connect statistics with trusted operational and sectoral information-sharing mechanisms. A multi-layer system should link strategic oversight with operational response, combining a regional dashboard of aggregated national data for policymakers, formalised multilateral co-operation amongst Computer Emergency Response Teams, and sector-specific platforms for high-risk industries such as finance, energy, and telecommunications.

Fourth, phase implementation according to national capacity. Member states with more advanced capabilities could pilot national arrangements and stress-test the Common Framework, with phased expansion supported by targeted technical assistance and capacity building.

Conclusion

ASEAN cannot manage what it cannot measure. Building national capacity for comparable cybersecurity statistics, connected through a common regional framework, would give member states the shared evidence base that co-ordinated cyber governance requires. As digital integration deepens, the ability to compare and act on reliable cyber risk data will determine whether ASEAN's growth rests on a secure foundation.

Acknowledgements

This policy brief was prepared by Romora Edward Sitorus, Nobuhiro Aizawa, Tunggul Mintara Dharma Wirajuda and Samsu Sempena.

References

- Cyber Threat Alliance and Institute for Security and Technology (2023), *Cyber Incident Reporting Framework: Global Edition*.
- Ebert, N., T. Schaltegger, B. Ambuehl, T. Geppert, A. Trammell, M. Knieps, and V. Zimmermann (2025), 'Learning from Safety Science: Designing Incident Reporting Systems in Cybersecurity', *Journal of Cybersecurity*, 11(1), tyaf019.
- IBM (2025), *Cost of a Data Breach Report 2025: The AI Oversight Gap*. Armonk, NY: IBM Corporation.
- ITU (2024), *Global Cybersecurity Index 2024*. Geneva: International Telecommunication Union.
- Kaspersky (2025), 'SEA Businesses Face 400 Ransomware Attacks Daily in 2024'.
- VERIS Community Database (2026), *VERIS Framework: A Common Language for Describing Security Incidents*.



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

