Economic Research Institute for ASEAN and East Asia

NO. 2026-5, JULY 2026
ISSN: 2086-8154

ERIA POLICY BRIEF

Safeguarding ASEAN's Digital Resilience through Cyber Insurance

Key Messages:

- Cyber threats and losses across ASEAN are escalating, yet cyber insurance uptake remains negligible, leaving most firms financially exposed and without a meaningful safety net when incidents occur.
- Interconnected digital supply chains mean that a single cyber incident can cascade across borders, creating correlated risks too large for any one firm or national insurer to absorb alone.
- Aligning coverage standards across ASEAN markets will help firms better understand what their cyber insurance covers. Shared definitions, stronger disclosure requirements, and comparable policy language can build the confidence needed to grow the market.
- A shared regional platform for recording cyber incidents and their consequences – the proposed ASEAN Cyber Resilience Observatory – would provide insurers and policymakers with the evidence base needed to price coverage more accurately and to advance comparable standards through the Digital Economy Framework Agreement (DEFA) and the ASEAN Insurance Council.

Cyber incidents across Southeast Asia are causing financial losses that are growing in scale and increasingly threaten entire systems, not just individual firms. Cross-border supply chains and shared service providers compound the risk because, when many firms rely on the same providers, a single incident can affect them all simultaneously, producing losses too large for any one firm to absorb. Yet cyber insurance penetration across ASEAN remains negligible, owing to constraints on both the demand and supply sides of the market. On the demand side, fragmented coverage standards, low awareness, and gaps between perceived and actual protection prevent informed decision-making. On the supply side, scarce regional loss data and divergent regulatory frameworks limit insurers' confidence in pricing coverage. Importantly, cyber insurance complements rather than substitutes for cybersecurity investment. It finances recovery after an incident and, by conditioning coverage on minimum security controls, encourages stronger defences from the outset. Because ASEAN's economies differ widely in digital maturity, governments should adopt a gradual approach. They can advance convergence on coverage standards, establish a shared platform for recording cyber incidents, and develop a regional mechanism to cover large-scale events that exceed any single country's capacity.

Cyber Insurance as ASEAN's Financial Safety Net

The growing frequency and severity of cyber incidents are testing the resilience of firms across Southeast Asia. When these incidents go unaddressed, they can cascade into operational shutdowns, compensation claims from affected parties, penalties under data protection laws, and long-term damage to business confidence that erodes productivity and competitiveness across entire sectors. Investing in cybersecurity lowers the likelihood of a breach, but cyber insurance is what helps keep a firm financially whole when one occurs despite those defences. Indeed, a study of organisations of various sizes found that the average cost of a data breach in the region reached US$3.67 million in 2025, though typical losses for smaller firms are relatively lower (IBM, 2025), and a study of more than 132,000 cyber events found that extreme losses occur far more often than standard risk models would predict (Shevchenko et al., 2023).

Cyber risk in ASEAN is increasingly systemic, with single incidents now able to disrupt many services and firms simultaneously rather than one organisation in isolation. In June 2024, a ransomware attack on Indonesia's national data centre disrupted 282 public services across more than 200 government agencies, including immigration and airport systems. In March 2025, a ransomware attack on Malaysia's Kuala Lumpur International Airport disrupted flight information, check-in, and baggage systems. In July 2025, Singapore disclosed that an advanced persistent threat actor was actively targeting its critical infrastructure, including all four major telecommunications operators.

Cyber insurance is a necessary complement to cybersecurity, absorbing the financial losses that even strong defences cannot eliminate. Beyond absorbing these losses, it also reinforces the defences that prevent them by conditioning coverage on minimum security controls, requiring firms to meet baseline standards before obtaining or renewing a policy. This encourages

Please cite this content as:

ERIA (2026), 'Safeguarding ASEAN's Digital Resilience Through Cyber Insurance'. *ERIA Policy Brief 2026-5*. Jakarta: ERIA. Available at: https://www.eria.org/publications/safeguarding-asean-s-digital-resilience-through-cyber-insurance

firms to strengthen their cybersecurity from the outset, as stronger security becomes a precondition for coverage and often a route to lower premiums. More importantly, cyber insurance provides the liquidity firms need to recover, resume operations, and protect the livelihoods that depend on them. While cyber insurance strengthens resilience, it is not a panacea. Coverage limits, exclusions for certain forms of cyber conflict, incomplete risk data, and uncertainty surrounding large-scale systemic events continue to challenge insurers and remain amongst the constraints shaping cyber insurance markets worldwide.

These limitations are one reason governments have a foundational role in cyber insurance markets. Across many economies, functioning cyber insurance markets rest on public foundations such as incident-reporting regimes, public–private threat intelligence sharing, catastrophe backstops, and national cyber resilience strategies, all of which improve the data and confidence on which insurers depend. The role of ASEAN governments is therefore to build this enabling foundation and backstop risks that the market cannot absorb alone, while leaving the pricing and provision of routine coverage to insurers.

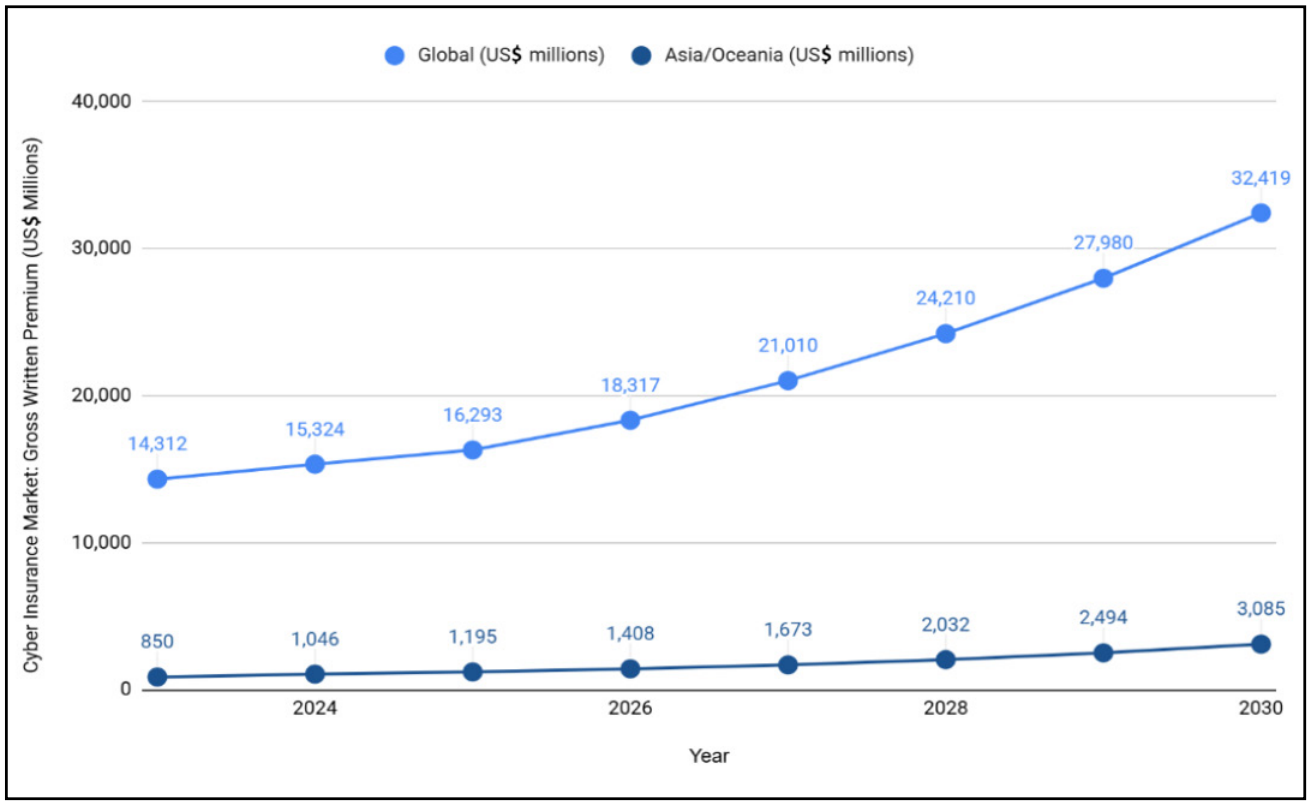
ASEAN's cyber insurance market remains underdeveloped on both the demand and supply sides. On the demand side, most firms either lack cyber insurance entirely or hold policies that cover far less than the risks they face. In fact, fewer than one in ten small and medium-sixed enterprises (SMEs) in the region hold any form of cyber insurance (Swiss Re, 2024). Furthermore, many firms believe their existing general insurance policies already cover digital losses, but when making a claim they often find that cyber-related events are excluded (Woods et al., 2025). Even firms that seek dedicated cyber coverage face another challenge: policies differ so widely in how they define key terms, what they exclude, and what triggers a payout that most buyers cannot compare products in any meaningful way (Romanosky et al., 2019).

On the supply side, cyber insurers face their own constraints. Roughly 50%–65% of global cyber insurance premiums were ceded to reinsurers in 2022 because even established insurers considered this category of risk too volatile to retain in full (Cremer et al., 2024). Taken together, these demand- and supply-side barriers widen the protection gap at precisely the moment ASEAN's digital economy needs it to narrow.

Figure 1 shows global cyber insurance gross written premiums and the share contributed by Asia and Oceania. Global gross written premiums are projected to more than double, with average annual growth exceeding 10%. The market in Asia and Oceania, which includes ASEAN, is expanding even faster in relative terms than the global market. Regional premiums are projected to rise from US$1,046 million in 2024 to US$3,085 million in 2030, representing growth of 195%, compared with 112% globally over the same period.

ASEAN has made significant progress in regional cybersecurity co-operation, creating a strong foundation for extending that work into cyber insurance. The Digital Economy Framework Agreement (DEFA), which reached substantial conclusion in October 2025, includes

Figure 1. Global Cyber Insurance Market: Gross Written Premium, Historical and Projected, 2023–2030 (US$ millions)



Source: Authors' synthesis based on Munich Re (2025).

cybersecurity amongst its nine core negotiating areas and establishes obligations relating to data protection and online safety. The ASEAN Regional Computer Emergency Response Team (CERT), launched in October 2024, strengthens the region's capacity to detect and respond to cyber threats collectively. The Southeast Asia Disaster Risk Insurance Facility (SEADRIF), which delivered parametric payouts to Lao PDR in 2023 and 2024, demonstrates ASEAN's ability to pool risk regionally. Although cyber risk is more difficult to model, the same principles of risk pooling and regional governance could be adapted to this domain.

These initiatives provide a strong institutional foundation. The next step is to connect cybersecurity co-operation with insurance market development so that the data, standards, and trust being built across ASEAN can also support more accessible and affordable cyber coverage for firms throughout the region.

The regulatory environment across ASEAN directly shapes how insurers assess and price cyber risk. Specifically, where data protection rules clearly define liability, mandate breach reporting, and establish enforcement mechanisms, insurers can design coverage with greater confidence and offer more competitive terms. Conversely, where those rules are still evolving, insurers face greater uncertainty and tend to price coverage more conservatively or limit its scope.

Table 1 illustrates how ASEAN Member States currently approach penalties for failures to protect customer data. As the table shows, the variation across the region is significant. Singapore and Brunei Darussalam, for instance, have introduced penalties of up to 10% of annual turnover, whilst Indonesia applies fines of up to 2% of annual revenue. A more comparable regulatory foundation, built through co-operation rather than uniformity, would give underwriters the consistency they need and make cyber insurance more accessible to firms across the region.

Table 1. Penalties for Failure to Protect Customer Data in ASEAN

Country	Monetary penalties	Non-monetary penalties
Brunei Darussalam	Up to 10% of annual turnover in Brunei Darussalam where turnover exceeds BND 10,000,000; otherwise up to BND 1,000,000.	Directions to stop non-compliant processing or destroy data; civil action for loss or damage without a statutory cap.
Cambodia	Up to KHR 4,000,000 under E-Commerce Law data-protection obligations. Legal entities may be fined twice as much, up to KHR 8,000,000.	Imprisonment of one to two years for responsible individuals; legal entities may face dissolution, court surveillance, activity prohibition, and publication or broadcast of the decision.
Indonesia	Up to 2% of annual income or annual receipts.	Administrative sanctions including written warnings, temporary suspension, deletion or destruction of data, and compensation claims without a statutory cap.
Lao PDR	Up to LAK 15,000,000 under the electronic data protection framework for relevant electronic-data violations.	Warnings, re-education measures, civil liability, and possible criminal sanctions depending on severity.
Malaysia	Up to MYR 1,000,000 for breach of the Security Principle. Failure to notify the Commissioner of a personal data breach may carry up to RM 250,000.	Imprisonment of up to three years for responsible individuals for breach of the data protection principles, and up to two years for breach-notification failure.
Myanmar	Up to MMK 10,000,000 for failure by the person responsible for personal data to manage it in accordance with the Electronic Transactions Law.	Imprisonment from one year to three years for responsible persons.
Philippines	Up to PHP 5,000,000 per single act for administrative infractions involving failure to secure personal data or notify a breach. Criminal fine up to PHP 4,000,000 may apply for negligent access to sensitive personal information.	Imprisonment, corporate officer liability, and possible suspension or revocation of corporate rights.

Table 1. *Continued*

Country	Monetary penalties	Non-monetary penalties
Singapore	Up to SGD 1,000,000 or 10% of annual turnover in Singapore, whichever is higher, where annual turnover in Singapore exceeds SGD 10,000,000.	Directions to stop or rectify non-compliant processing, deletion or destruction orders, and private right of action for court-awarded damages without a statutory cap.
Thailand	Up to THB 3,000,000 for failure to implement security measures or notify a personal data breach.	Compensation for damages and punitive damages up to two times the actual compensation.
Timor-Leste	For e-commerce merchants, up to USD 100,000 for breach of secure-technology and related e-commerce obligations. For legal persons, the maximum is increased by one-third, up to US$ 133,333.33.	Seizure of goods, closure of establishment, or revocation of certificate may apply.
Viet Nam	Up to VND 3,000,000,000 for general personal-data-protection violations. If the incident also involves cross-border transfer violations, up to 5% of previous-year revenue.	Compensation where damage is caused and possible criminal prosecution.

BND = Brunei dollar; KHR = Cambodian riel; LAK = Lao kip; MMK = Myanmar kyat; PHP = Philippine peso; MYR = Malaysian ringgit; SGD = Singapore dollar; THB = Thai baht; US$ = US dollar; VND = Vietnamese dong.
Source: Authors' compilation based on national data protection, e-commerce and cybersecurity laws. Updated 5 May 2026.

Policy Recommendations

ASEAN should treat cyber insurance as a core pillar of digital resilience that complements cybersecurity investment. Yet low uptake, fragmented standards, and scarce loss data continue to hold the market back. Three recommendations would help close this gap through existing regional channels.

1. Advance convergence on cyber insurance standards across ASEAN.

Greater convergence on core definitions and disclosure practices would help firms compare products with confidence and build trust on both the demand and supply sides of the market. The ASEAN Insurance Council, working in close consultation with national insurance regulators, is well placed to take this work forward in a manner that respects national circumstances and existing supervisory traditions.

2. Establish an ASEAN Cyber Resilience Observatory.

A shared platform for recording cyber incidents and their financial consequences would give insurers and policymakers a more accurate picture of regional cyber risk. It could be anchored in different national institutions depending on each country's governance structure. In some countries, it might build on a national Computer Emergency Response Team (CERT), and in others on a designated cybersecurity authority under a relevant ministry, with the ASEAN CERT connecting them. The experiences of Singapore and the United States show that both mandatory and voluntary reporting models can succeed. Reporting could begin on a voluntary basis and become mandatory as confidence grows, supported by clear ASEAN guidelines on data confidentiality and common reporting standards under the Digital Economy Framework Agreement (DEFA).

3. Build a regional safety net for systemic cyber risk.

Some cyber events, including widespread cloud outages, attacks on critical infrastructure, and incidents affecting multiple jurisdictions, exceed the capacity of individual firms or national markets to absorb. Although cyber risk evolves more rapidly and is harder to model than natural catastrophe risk, SEADRIF demonstrates that ASEAN can build shared risk-pooling institutions. Its governance, capital structure, and use of reinsurance and development partners provide a model that a regional cyber facility could adapt.

Conclusions

Cyber insurance should not be viewed solely as an insurance product, but as part of ASEAN's broader digital resilience architecture. As digital integration deepens under DEFA, the ability to absorb, recover from, and learn from cyber incidents will become as important as preventing them. Building a trusted and sustainable cyber insurance market can therefore strengthen not only individual firms, but also the resilience of ASEAN's digital economy as a whole.

Acknowledgements

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

References

Cremer, F., B. Sheehan, M. Mullins, M. Fortmann, S. Materne, and F. Murphy (2024), 'Enhancing Cyber Insurance Strategies: Exploring Reinsurance and Alternative Risk Transfer Approaches', *Journal of Cybersecurity,* 10(1), tyae027.

IBM (2025), Cost of a Data Breach Report 2025. IBM Security.

Munich Re (2024), Munich Re Global Cyber Risk and Insurance Survey 2024: Bridging the Gap in Cyber Protection. Muenchener Rueckversicherungs-Gesellschaft.

Munich Re (2025), Cyber Insurance: Risks and Trends 2025. Muenchener Rueckversicherungs-Gesellschaft.

Peak Re (2025), Peak Re Consumer Survey 2025. Peak Reinsurance Company Limited.

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones (2019), 'Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?', *Journal of Cybersecurity*, 5(1), tyz002.

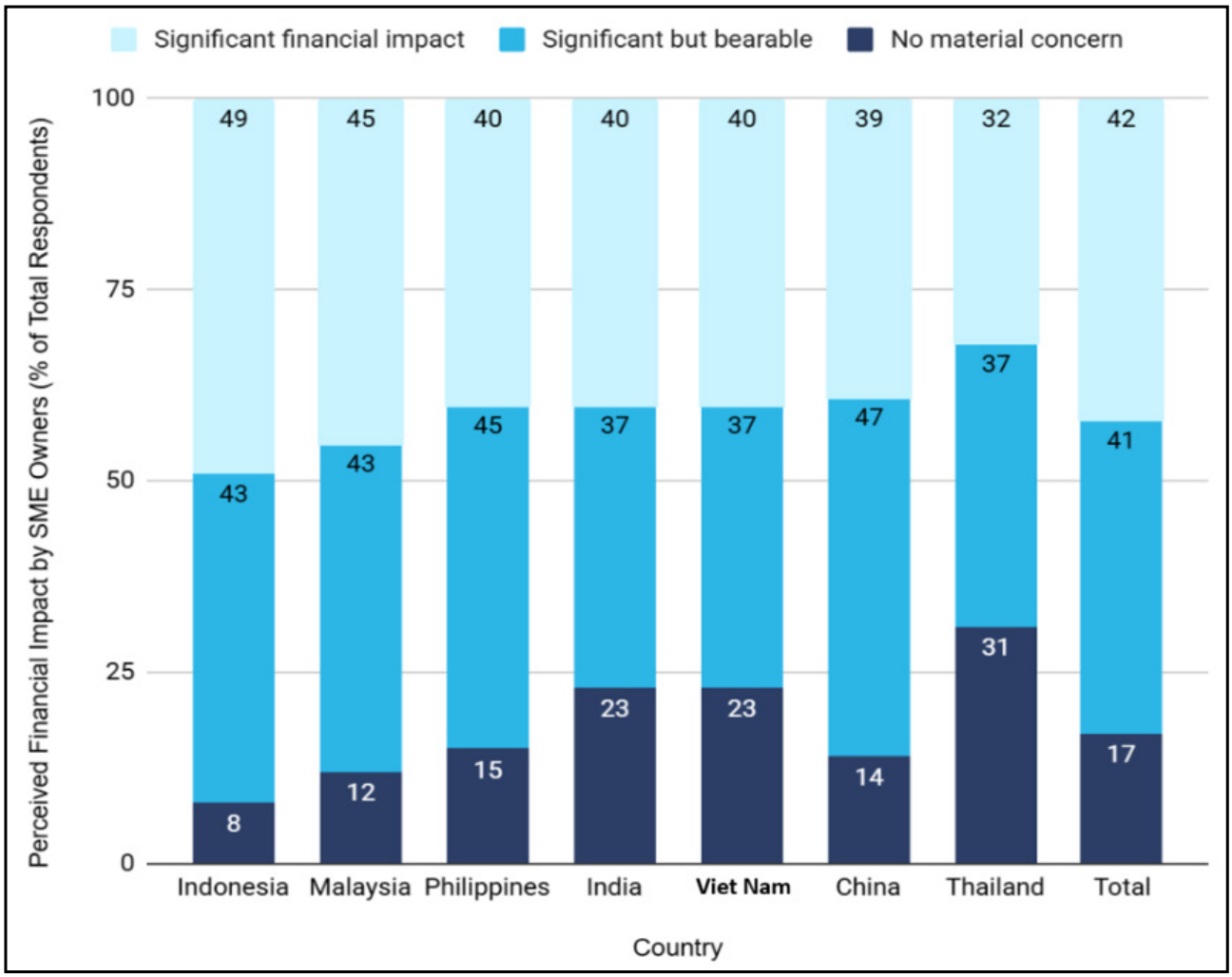
Shevchenko, P.V., J. Jang, M. Malavasi, G.W. Peters, G. Sofronov, and S. Trück (2023), 'The Nature of Losses from Cyber-Related Events: Risk Categories and Business Sectors', *Journal of Cybersecurity*, 9(1), tyac016.

Sophos (2024), *Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leaders*. Sophos Ltd.

Swiss Re (2024), Cyber Insurance: Strengthening Resilience for the Digital Transformation. Swiss Re Institute.

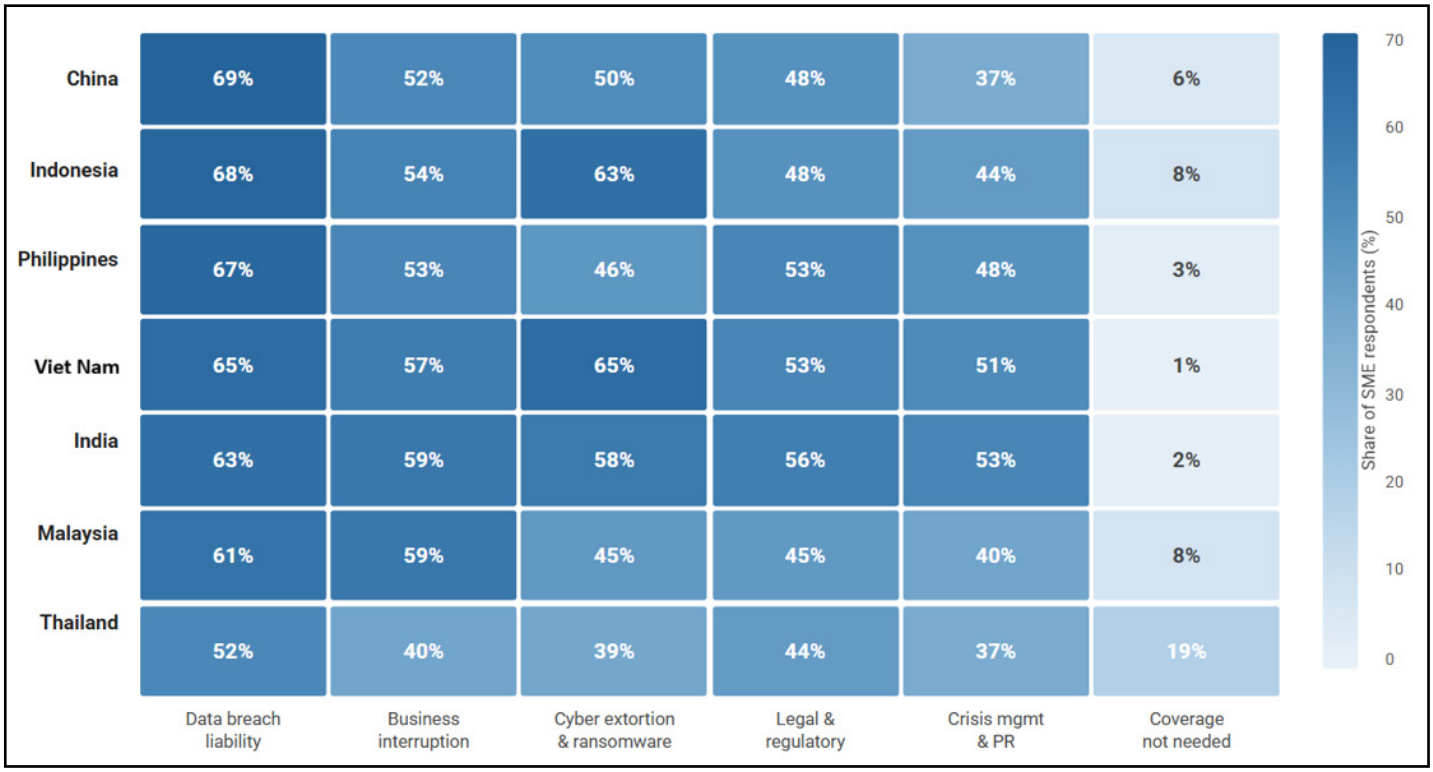
Woods, D.W., R. Boehme, J. Wolff, and D. Schwarcz (2025), 'Consumer Cyber Insurance: Market Structure and Policy Implications', *Journal of Cybersecurity*, 11(1), tyae031.

Annex Figure 1. Perceived Financial Impact of a Cyberattack on Small and Medium-Sized Enterprises (SMEs) in Selected Emerging Asian Economies, 2025



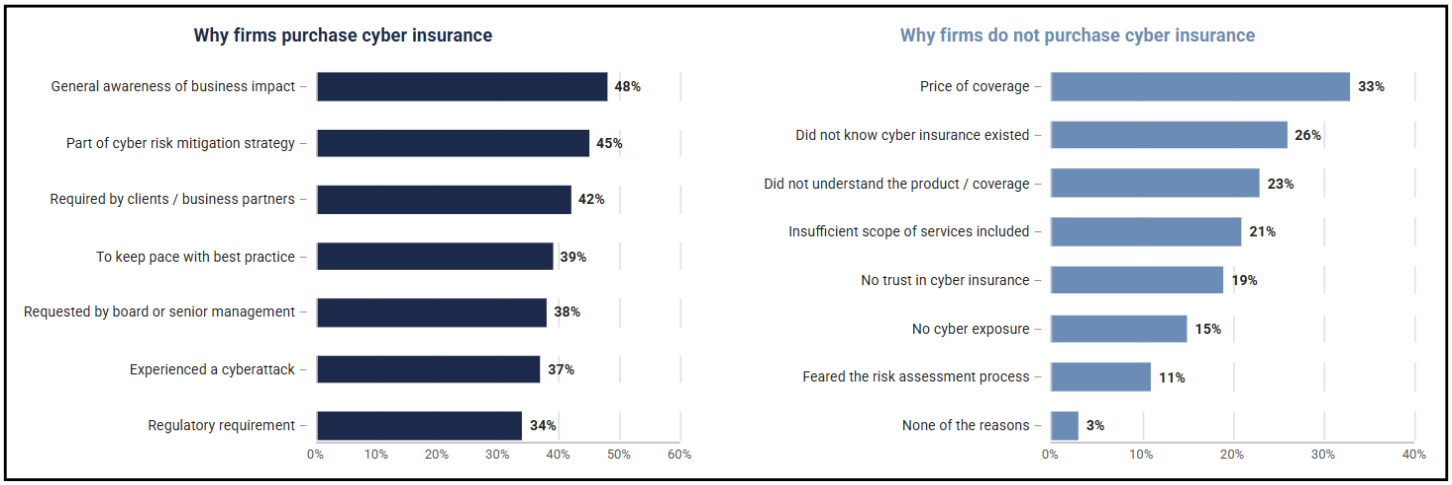
Source: Authors' synthesis based on Peak Re (2025).

Annex Figure 2. Types of Cyber Insurance Coverage Most Relevant to Small and Medium-Sized Enterprises (SMEs) in Selected Emerging Asian Economies, 2025



Source: Authors' synthesis based on Peak Re (2025).

Annex Figure 3. Drivers of and Barriers to Cyber Insurance Uptake Amongst IT and Cybersecurity Leaders, 2024



Source: Sophos (2024). N = 5,000 respondents, 14 countries.

Source: Munich Re (2024). N = 7,500 respondents, 15 countries.

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