Executive Summary

The ASEAN region is a prime target for cyberattacks

The digital economy in the Association of Southeast Asian Nations (ASEAN)[1] has the potential to add $1 trillion to GDP over the next 10 years. However, cyber risks could impede trust and resilience in the digital economy and prevent the region from realizing its full digital potential. ASEAN countries have already been used as launchpads for attacks, either as vulnerable hotbeds of unsecured infrastructure or as well-connected hubs to initiate attacks.

The region's growing strategic relevance makes it a prime target for cyberattacks. Cyber resilience is generally low, and countries have varying levels of cyber readiness. Specifically, there is a lack of a strategic mindset, policy preparedness, and institutional oversight relating to cybersecurity. The absence of a unifying framework makes regional efforts largely voluntary, leads to an underestimation of value-at-risk, and results in significant underinvestment. In addition, because cyber risk is perceived to be an information technology (IT) rather than a business problem, regional businesses do not have a comprehensive approach to cybersecurity. The region's nascent cybersecurity industry faces shortages of home-grown capabilities and expertise along with fragmented products and solutions and few comprehensive solution providers. Multiple vendor relationships and product deployments are creating operational complexity and, in some cases, increasing vulnerability.

The situation will escalate over time

The increase in trade, capital flows, and cyber linkages across ASEAN countries imply that the cyber threat landscape will generate even greater complexity in the future, further escalating the region's cybersecurity challenges:

- Growing interconnectedness will intensify the systemic risk, making the region only as strong as its weakest link.
- Diverging national priorities and varying paces of digital evolution will foster a pattern of sustained underinvestment.
- Limited sharing of threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.
- Rapid technological evolution makes threat monitoring and response more difficult, especially with the rise of encryption, multi-cloud operations, the proliferation of the Internet of Things (IoT), and the convergence of operation technology (OT) and IT.

Because of these factors, the top 1,000 ASEAN companies could lose $750 billion[2] in market capitalization, and cybersecurity concerns could derail the region's digital innovation agenda—a central pillar for its success in the digital economy.

[1] The ASEAN region includes Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.

[2] Based on erosion in market capitalization for corporations that have been victims of mega data breaches