Singapore, Malaysia, Thailand, the Philippines, and Brunei. Five of the ASEAN-6 countries have enacted data protection or privacy laws, with Vietnam being the exception.[10] Vietnam does not have a unified law regarding privacy; instead, it is informed by different laws and decrees.

Apart from Singapore and Malaysia, few ASEAN countries have made progress in all areas. However, national agencies that are working on their cybersecurity strategies and policies have rich experiences to draw upon both from their regional counterparts and from other parts of the world.

1.2.2 Absence of a unifying framework at the ASEAN level

The challenge is exacerbated by the absence of an overarching governance or legal framework that member states adhere to or a regional regulatory body to enforce policies. Unified strategy development, readiness assessments, and incident reporting are missing, limiting the collective preparedness of the region and its ability to capitalize on shared knowledge. Effective prevention and combatting cybercrime requires international cooperation because of its non-physical, cross-border nature. Without a structured ASEAN cooperative framework to address cybercrime, the region remains vulnerable.

ASEAN faces challenges in pulling together a unifying framework, largely because of the inherent absence of a power to legislate or veto budgets and appointments. The ASEAN Inter-Parliamentary Assembly has only the power of moral suasion. In contrast, the European Union, with a strong legislative framework and a powerful secretariat has placed cyber resilience very high on its agenda and has developed a cohesive regional cybersecurity strategy (see sidebar: The EU Approach to Cybersecurity on page 9). The General Data Protection Regulation (GDPR), which becomes enforceable in 2018 across the EU, requires a personal data breach[11] to be reported to the competent national supervisory authority and, in certain cases, to be communicated to the individuals whose personal data has been affected by the breach. The GDPR also provides for stringent penalties for enterprises that fail to comply.

In the past year, cybersecurity was a highlight on the ASEAN agenda, beginning with a focus on capacity building. Singapore is taking a leading role in coordinating cybersecurity cooperation by organizing the annual ASEAN Ministerial Conference on Cybersecurity, the second of which was held in September 2017 in conjunction with Singapore's International Cyber Week. Singapore has also codeveloped the ASEAN Cyber Capacity Program, an initiative to build capabilities across the region through tailored training programs, public–private partnerships, and discussions on policy and legislation.

1.2.3 Businesses underestimate value-at-risk, leading to underinvestment in cybersecurity

Adopting a value-at-risk mindset is crucial for effective threat mitigation because it drives senior-level decision-making and ensures more efficient resource allocation and mobilization. Assessing value-at-risk involves identifying high-value assets that may be at risk from a cyberattack and assessing the potential impact of a breach. Current assessments are based on historical average data, which do not account for complex, powerful attacks such as those seen recently with Target, Yahoo!, and Equifax.[12]

[10] ASEAN-6 refers to the region's top six economies: Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam.

[11] Defined under Article 4(12) of the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

[12] The financial cost of cyberattacks considers the following parameters: the number of top companies segmented by sector and country (2,700) and the value-at-risk (grown by GDP contribution growth by sector and by country), the cost per cyberattack segmented by sector, the likelihood of a specific company being attacked, and the frequency of cyberattacks. Data sources include Ponemon Institute's *Cost of Cybercrime* and *Cost of Data Breach* studies, the World Bank, the Economist Intelligence Unit, and security analyst reports.