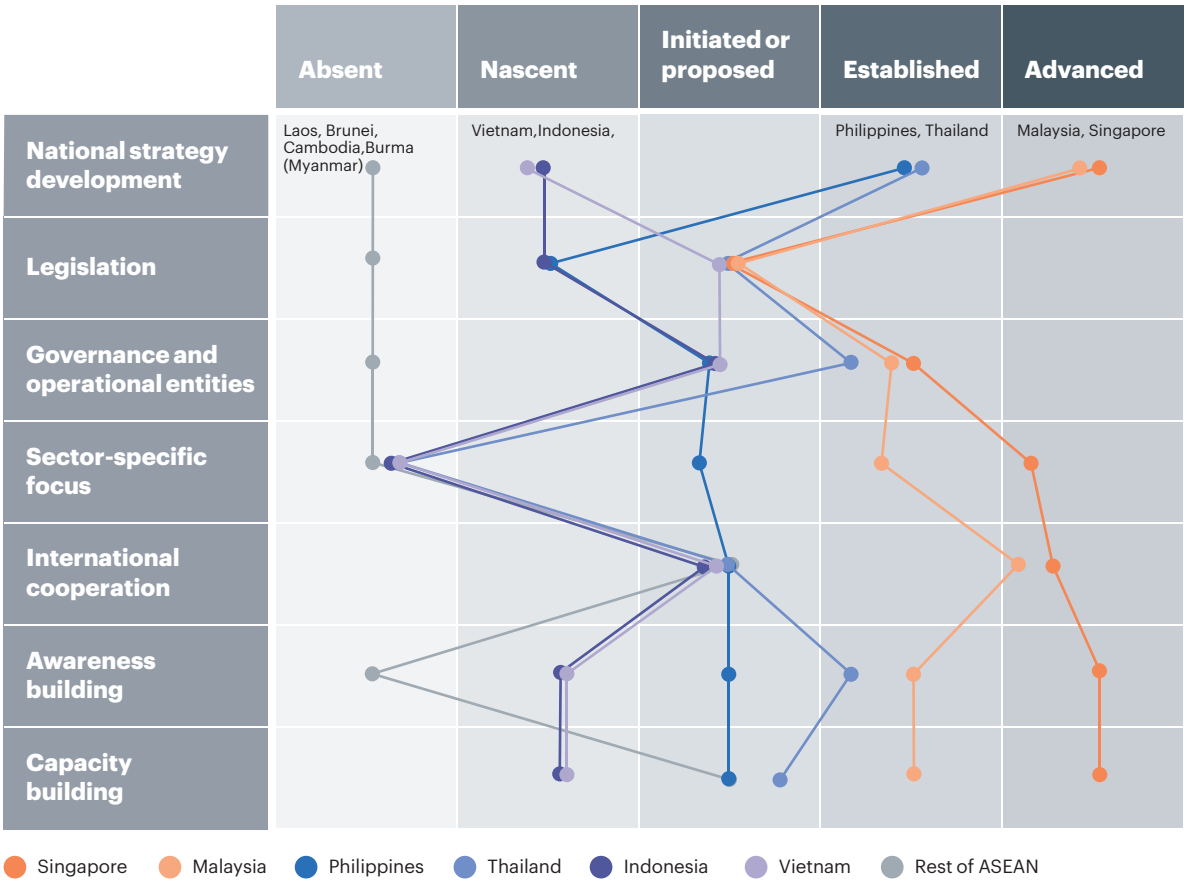
Figure 5

Cybersecurity policies vary widely across the ASEAN region



Sources: government websites, press clippings; A.T. Kearney analysis

Cybersecurity governance and policies are undeveloped in the region. National cybersecurity strategies have been laid out by Singapore, Malaysia, Thailand, and the Philippines. A few countries have set up national agencies to consolidate and coordinate cybersecurity agendas. These include Singapore (Cyber Security Agency of Singapore), Malaysia (CyberSecurity Malaysia), and the Philippines (Department of Information and Communications Technology). Indonesia has established a national cyber and encryption agency, Badan Siber dan Sandi Negara (the Cyber Body and National Encryption Agency), and Thailand has proposed a national cybersecurity committee. Although other countries do not have dedicated agencies, their national computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs) currently play the role of national cybersecurity agencies.

The lack of sector-specific governance and policies is a region-wide issue, resulting in limited transparency and a lack of sharing of threat intelligence. One exception is the Monetary Authority of Singapore and the global Financial Services Information Sharing and Analysis Center, which have announced plans to set up the Asia Pacific Regional Intelligence and Analysis Center. This platform aims to provide deeper capabilities in cyber intelligence gathering and analysis for enhanced in-region support, specifically for financial services.

Although Singapore, Malaysia, Thailand, and Vietnam drafted cybersecurity bills in 2017, limited progress has been made across the rest of ASEAN. Cybercrime laws have also been passed in