Figure 30

Stakeholder view of the call to action

Call-to-action agenda	Regional	National
Elevate cybersecurity on the regional policy agenda	• Set up regional cybersecurity coordination platform • Track national progress via the ASEAN Secretary-general's annual report	• Implement the 12-point Rapid Action Cybersecurity Framework • Establish sector-level governance mechanism
Secure a sustained commitment to cybersecurity	• Track cybersecurity investments against the agreed commitment • Report on national cybersecurity spend	• Engage with private-sector stakeholders to stimulate cybersecurity investment • Set up a cyber-hygiene dashboard for crucial sectors to define and track key performance indicators at the sectorial level • Recommend standards for voluntary adoption
Fortify the ecosystem	• Adopt voluntary certification of vendors and develop recommended lists • Foster cross-border cybersecurity cooperation across the region and around the world • Encourage public–private partnerships across the region	• Adopt voluntary certification of vendors, and develop recommended lists • Establish and incentivize trusted sharing mechanisms • Set up security maturity assessments as a formal cyber certification for the private sector • Set-up industry alliances • Encourage public–private partnerships
Build the next wave of cybersecurity capabilities	• Develop cross-border capabilities to prevent cybercrime • Support regional start-ups to boost development of advanced solutions and address white spaces • Set up regional R&D fund for cybersecurity with contribution from member countries	• Align the cybersecurity talent strategy with the national workforce planning agenda • Identify and plan for skills in demand • Develop career pathways around cybersecurity • Foster R&D around emerging threat vectors • Anchor world-class capabilities to facilitate knowledge exchange

Source: A.T. Kearney analysis

market capitalization, this is a small price to pay, especially since other items on the fiscal budget such as defense account for up to 3.4 percent of the region's annual GDP.[30]

Corporate boards and chief information security officers (CISOs) have important roles to play in creating a defense-in-depth culture in their organizations (see figure 31 on page 48). These roles include elevating cybersecurity on the board of directors' agenda and establishing the CISO function as an independent reporting function. CISO responsibilities include establishing group-wide strategies, governance, and conducting value-at-risk assessments. In addition, cybersecurity resilience needs to be extended to business partners through a continuous process of education and inclusion in internal risk audit assessments.

Forging industry alliances and engaging with educational institutions to develop industry-relevant cybersecurity courses will help build a stronger local industry and address capacity and capability gaps.

[30] World Bank based on data for Malaysia, Singapore, Indonesia, Thailand, Vietnam, and Philippines