

An urgent call to action

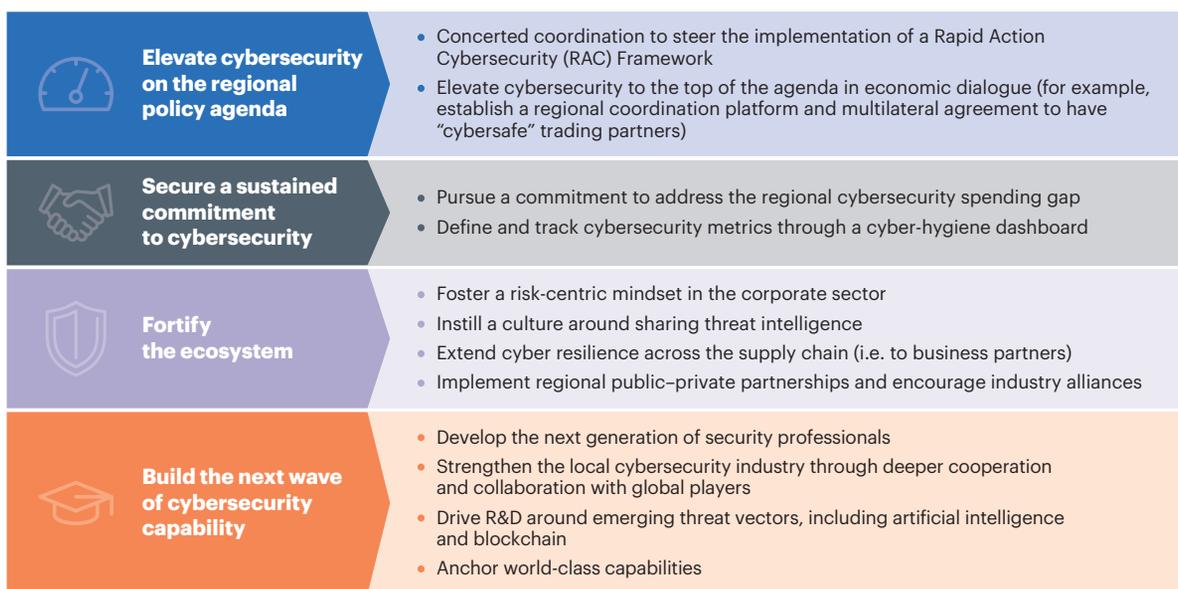
The response to these challenges must be comprehensive, engaging an array of stakeholders to deal with the scale of the threat and to ensure that ASEAN’s leap into the digital economy is unobstructed. An active defense mindset is required to work together to defend and leverage collective ASEAN resources.

The ideal regional cybersecurity defense playbook needs to address a four-point agenda (see figure 1):

- Elevate cybersecurity on the regional policy agenda.
- Secure a sustained commitment to cybersecurity.
- Fortify the ecosystem.
- Build the next wave of cybersecurity capability.

Figure 1

Regional cybersecurity defense playbook



Source: A.T. Kearney analysis

Elevating cybersecurity on the regional policy agenda calls for the immediate implementation at national levels of a Rapid Action Cybersecurity Framework to harmonize cyber resilience across the region. The Rapid Action Cybersecurity Framework is a comprehensive 12-point action agenda for national governments to address gaps in strategy, policy, legislation, and governance related to cybersecurity. In addition, adopting an ASEAN-initiated multilateral regime around cybercrime can bring strategic and operational benefits to the region, particularly in rapid law enforcement cooperation. National governments should take the lead in implementing the framework with support, guidance, and oversight from the ASEAN Ministerial Conference on Cybersecurity (AMCC). The ASEAN secretary-general’s annual report should be expanded to include a scorecard that tracks each country’s progress in achieving milestones set by the Rapid Action Cybersecurity Framework. To **secure a sustained commitment to cybersecurity** and