3 Call to Action: The Need for an Active Defense Mindset

Trust and resilience are the cornerstones of growth in a digital economy. This section provides an agenda for policy makers and the private sector to work together to heighten awareness about cybersecurity and adopt a stance of active defense. The US Department of Defense defines active defense as the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. For cybersecurity, active defense is about flipping the asymmetry between defenders and attackers via cooperation among defenders. Cybersecurity programs often defend infrastructure in silos, even though vulnerabilities extend across peer companies and vendors. Meanwhile, adversaries plan and execute sophisticated attacks across several targets at once. Active defense means working together to defend and take advantage of the region's collective resources. Following this active defense mindset, an urgent four-point agenda is needed as part of the region's cybersecurity defense playbook (see figure 18).

3.1 Elevate cybersecurity on the regional policy agenda

The region's policy makers have agreed on the importance of closer coordination. However, given the varying levels of preparedness and vastly differing national priorities, there is a need to elevate cybersecurity on the regional and national policy agenda through the following actions:

- Steer the implementation of a Rapid Action Cybersecurity Framework.
- Elevate cybersecurity to the top of the agenda in regional economic dialogue.

Figure 18
Regional cybersecurity defense playbook

Elevate cybersecurity on the regional policy agenda	• Concerted coordination to steer the implementation of a Rapid Action Cybersecurity (RAC) Framework • Elevate cybersecurity to the top of the agenda in economic dialogue (for example, establish a regional coordination platform and multilateral agreement to have "cybersafe" trading partners)
Secure a sustained commitment to cybersecurity	• Pursue a commitment to address the regional cybersecurity spending gap • Define and track cybersecurity metrics through a cyber-hygiene dashboard
Fortify the ecosystem	• Foster a risk-centric mindset in the corporate sector • Instill a culture around sharing threat intelligence • Extend cyber resilience across the supply chain (i.e. to business partners) • Implement regional public–private partnerships and encourage industry alliances
Build the next wave of cybersecurity capability	• Develop the next generation of security professionals • Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players • Drive R&D around emerging threat vectors, including artificial intelligence and blockchain • Anchor world-class capabilities

Source: A.T. Kearney analysis