

Figure 20

Regional cybersecurity governance framework

Regional

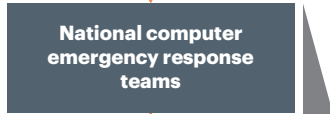


- Drive awareness, cross-border cooperation, intelligence sharing, incident response coordination, and market development activities
- Provide support, and report on progress against Rapid Action Cybersecurity Framework

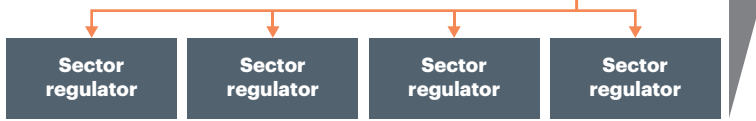
National



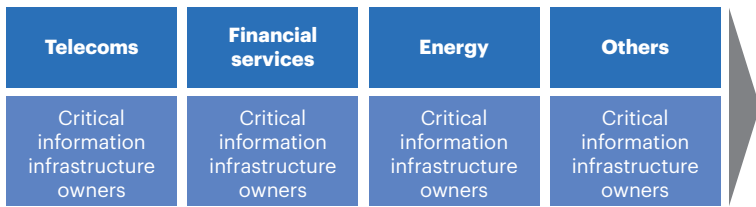
- Implement Rapid Action Cybersecurity Framework



- Interface with regulators and sector-level CERTs to share intelligence and provide early warning signals



- Establish trusted intelligence sharing mechanisms



- Implement cyber-hygiene dashboard in select sectors
- Adopt standards
- Implement defense-in-depth framework
- Share best practices

Private and public sector

Source: A.T. Kearney analysis

3.2 Secure a sustained commitment to cybersecurity

Two initiatives can help secure sustained commitment to cybersecurity:

- Pursue a commitment to address the cybersecurity spending gap.
- Define and track cybersecurity metrics through a sector-level cyber-hygiene dashboard.

3.2.1 Pursue a commitment to address the cybersecurity spending gap

Coupled with the region’s digital divide, differing national priorities and the perception about the value-at-risk results in a suboptimal allocation of funds to address cybersecurity.

Among ASEAN countries, three potential clusters of countries could emerge over time:

- Leaders: those with strong digital momentum, established institutional frameworks, and near- benchmark levels of cybersecurity spend
- Steady risers: those that exhibit strong momentum around digital and are in the process of building institutional frameworks around cybersecurity
- Breakout performers: those with the potential to leapfrog the rest of ASEAN but with no legal or institutional frameworks for cybersecurity