Figure 22

Focus the cybersecurity agenda on relevant metrics

Function	Management perspective	Metrics
Incident management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean time to incident discovery • Number of incidents • Mean time between security incidents • Mean time to incident recovery
Vulnerability management	How well do we manage the organization's exposure to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability scanning coverage • Percent of systems with no known severe vulnerabilities • Mean time to mitigate vulnerabilities • Number of known vulnerabilities
Patch management	How well are we able to maintain the patch state of our systems?	• Patch policy compliance • Patch management coverage • Mean time to patch
Application security	Can we rely on the security model of business applications to operate as intended?	• Number of applications • Percent of critical applications • Risk assessment coverage • Security testing coverage
Configuration management	How do changes to system configurations affect the security of the organization?	• Mean time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions
Corporate spending	What is the level and purpose of spending on information security?	• IT security spending as percent of IT budget • IT security budget allocation

Sources: Centre for Internet Security; A.T. Kearney analysis

> "Regulators need to acknowledge that industries have different business needs and organizational constraints, and thus it would be difficult to mandate cybersecurity metrics in a one-size-fit-all approach."
>
> **—land transportation authority, ASEAN country**

A cyber-hygiene dashboard should be an integral part of the corporate performance monitoring system, tracking internal readiness on strategy, culture, technology, processes, and organization (see figure 23 on page 34).

3.3 Fortify the ecosystem

The active defense mindset needs to be extended across the ecosystem in each country by not only implementing best practice guidelines in the corporate sector, but also raising cyber awareness across business partners. Four moves can help fortify the ecosystem:

- Foster a risk-centric mindset around cybersecurity for the corporate sector.
- Instill a culture of transparency in sharing threat intelligence.