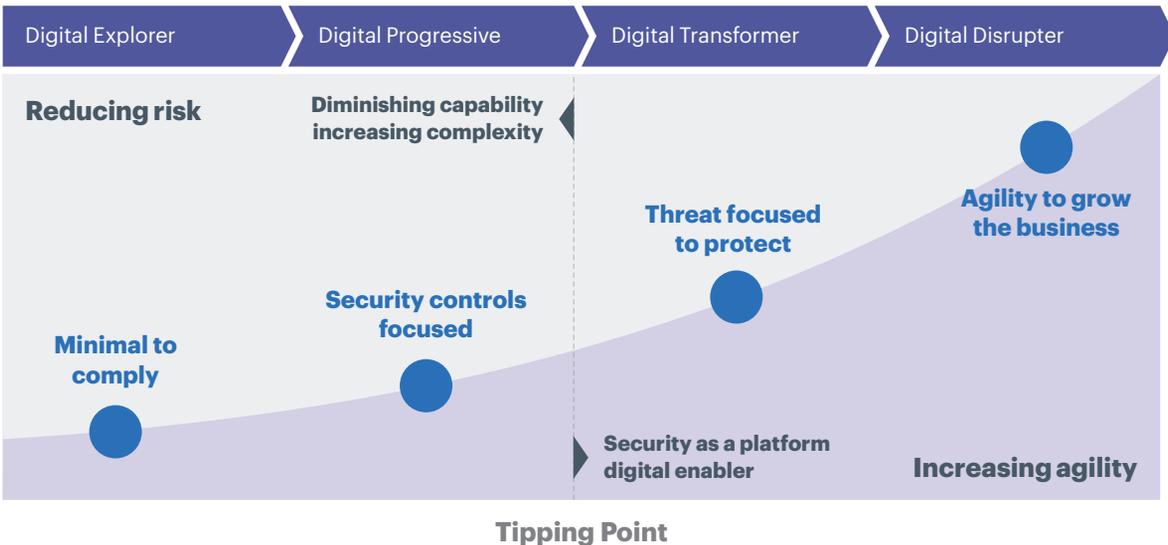


As digitalization grows, security must also mature (see figure 26). An organization’s evolution across the various stages of cyber excellence could be measured and tracked, providing a useful measure of cyber readiness. A security maturity model can help map an organization’s digital transformation journey against its security profile (see Appendix A on page 50). For smaller organizations looking to partner with large multinationals or CII owners, performance on the security maturity model should be a threshold requirement for doing business. This will raise the profile of cybersecurity among all business partners and promote resilience across the supply chain. Singapore’s Cybersecurity Bill calls for regular system audits by an approved third party. For CII owners, a maturity model can help identify cybersafe business partners.

Figure 26
Security as a digital enabler



Source: A.T. Kearney analysis

Cyber insurance companies are increasingly looking at an organization’s strategy, policy, and governance while pricing cyber insurance. Depending on the sector, a vulnerability scan or a penetration test may also be carried out in addition to reviewing the size of the security budget in relation to the total IT budget. Putting in place a comprehensive, layered cybersecurity strategy can help businesses reduce their insurance spend.

3.3.2 Instill a culture of transparency in sharing threat intelligence

Defending a country’s digital assets requires close cooperation across a range of stakeholders, including government agencies, the private sector, and end users. Despite general agreement about the need to do this, information-sharing remains inadequate both globally and in the region. Legal impediments—some real, some perceived—are obstacles to more robust information sharing among private-sector entities and between the private sector and the government. The US Cybersecurity Information Sharing Act aims to improve cybersecurity by giving private companies liability protection when they share relevant information with federal or private entities, allowing companies to remove information that identifies someone who is not directly related to a threat.