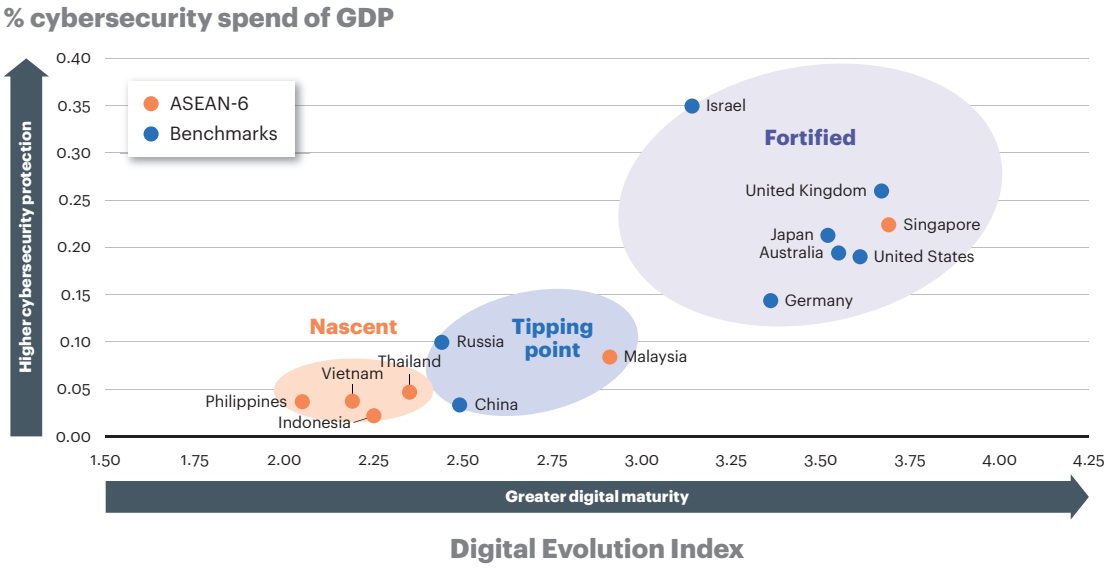
Figure 16

Correlation between digital evolution and cybersecurity spend



Sources: World Bank, Tufts University *Digital Planet 2017*, analyst reports; A.T. Kearney analysis

preparedness. Providing transparent guidance that informs cybersecurity investment decisions can accelerate each country's transition from awareness to action.

2.1.3 Limited threat intelligence sharing because of a lack of trust and transparency will lead to even more porous cyber defense mechanisms

Most ASEAN governments and businesses are reluctant to share incident information or threat intelligence, which is crucial for forensic investigation and prevention. With the growing sophistication and faster pace of cyberattacks (for example, zero-day exploits and advanced persistent threats), sharing intelligence, and best practices along with a joint incident response can help mitigate the region's cyber risk (see sidebar: Cisco and Interpol Collaborate to Combat Cybercrime).

The lack of intelligence sharing is a global issue, stemming from limited mandates to share specific cyber incident information across intelligence agencies. Furthermore, ASEAN lacks a governing framework to introduce incident reviews on a regional level. Efforts are under way in

Cisco and Interpol Collaborate to Combat Cybercrime

Cisco and the International Criminal Police Organization (Interpol) announced an agreement to share threat intelligence as the first step in jointly fighting cybercrime. The alliance will see the two organizations develop a coordinated and focused approach to data sharing. This not only will allow for quick threat detection around the world, but also pave the way for potential collaboration on training and knowledge sharing.

Cisco's agreement with Interpol supports the organization's programs targeting both pure cybercrime and cyber-enabled crimes to assist member countries with identifying cyberattacks and their perpetrators.