access to a multitude of product vendors and service providers, security solutions are often not tailored to specific industry needs.

Although the service landscape is also highly fragmented, vendors tend to be more localized. Very few service providers have a regional presence, and most operate only in their country of origin. As one of the fastest-growing segments in the ICT landscape, cybersecurity could be a significant economic opportunity for ASEAN countries. Encouraging innovation in cybersecurity through partnerships with global vendors and greater mobility of talent could generate significant gains for the region (see sidebar: CyberSecurity Malaysia as a Vendor Certification Authority). Other countries such as the United Kingdom and Israel are leveraging cybersecurity as a source of competitive advantage.

1.3.2 Paucity of skilled talent magnifies the challenge

Even with a comprehensive cybersecurity strategy and budget, security leaders are likely to face a shortage of skilled and qualified cybersecurity professionals to implement their cybersecurity agenda. Challenges exist in both capacity and capabilities. The shortage of skilled cybersecurity talent represents a global challenge, with the US Information Systems Audit and Controls Association (ISACA) citing a global shortage of more than 2 million professionals by 2019 (see figure 9 on page 13). In ASEAN, Malaysia, for instance, currently has 6,000 cybersecurity professionals but requires 10,000 by 2020.[15]

From a capability perspective, certain specific skill sets such as systems architecture design, behavioral analytics, and digital forensics are acutely in short supply, and there is a large and growing demand for industry-specific cybersecurity talent. Executives we interviewed cite subtle nuances related to a compliance mindset needed in the financial services industry as opposed to the recognition of real risk of physical damage to life and assets applicable in the manufacturing or oil and gas industry. There is also inadequate expertise in cybersecurity support sectors, such as cyber insurance, where both effective frameworks and sufficient knowledge are needed to accurately assess the value-at-risk.

To address this, some ASEAN countries are undertaking capacity building initiatives with a strategic view. Malaysia and Singapore have comprehensive strategies to develop cybersecurity professionals. The Philippines has also outlined its approach in the recently released National Cybersecurity Plan 2022, while Thailand is working with Japan's government to develop

CyberSecurity Malaysia as a Vendor Certification Authority

As the national cybersecurity agency of Malaysia, CyberSecurity Malaysia consolidates potential vendors and solutions, then offers recommendations to public and private bodies based on the National Institute of Standards and Technology (NIST) framework and end-user needs, ensuring a well-balanced cybersecurity approach (see section 1.4).

Even more recently, CyberSecurity Malaysia has developed a stringent certification process for local vendors, including a comprehensive evaluation methodology. This is complemented with various training initiatives to improve capabilities and ensure compliance with global standards as part of ongoing efforts to recommend world-class, comprehensive solutions whilst supporting the development of the local cybersecurity ecosystem.

[15] Malaysia Digital Economy Corporation, October 2017