Figure 27

Address gaps in cybersecurity capacity and capabilities

Design a national cybersecurity workforce planning strategy	Identify and plan for skills in demand	Develop occupational standards	Develop pathways to professional development	Strengthen industry–academia interface	Design curriculum and infrastructure
• Identify cybersecurity as a **strategic occupation** needed to support the economic growth agenda • **Coordinate with national agencies** around formulation and implementation of policies	• Map current **skill sets** • Regularly **track demand and supply in the cybersecurity labor market** • Develop **forecasts of cybersecurity skills in demand** • Identify funding mechanisms for skills in demand	• Develop **workforce qualification standards** for the cybersecurity industry, including job roles and required competencies • **Accredit and promote** professional **training institutions**	• Develop **pathways** for a career in cybersecurity (foundational, secondary, university, vocational education, and continuing professional education)	• Encourage **industry-academia partnerships** to make cybersecurity courses sector-relevant • Establish sector cybersecurity skill councils to map sector needs and design courses	• Increase the **breadth and depth of cybersecurity programs** • **Strengthen "ships"** (mentorships, scholarships, and internships) as part of the support mechanism • Encourage **partnerships**

Make cybersecurity an integral part of the national careers services framework

Source: A.T. Kearney analysis

Setting up occupational standards for cybersecurity includes identifying job roles and competencies as well as accreditation of training programs and approved suppliers. A vital aspect of cybersecurity capacity is developing multiple educational pathways, ranging from classes that provide foundational skills to higher-level courses:

- **K–12.** Create awareness via outreach programs to educate the public, including children.

- **Universities.** Promote cybersecurity as a career using industry-linking programs, targeted university courses, and innovation opportunities.

- **Industries.** Scale up cybersecurity professional development via specialized skill-building and conversion programs for professionals.

Encouraging engagement between industry and academia will ensure that programs are tailored to specific industries. Setting up cybersecurity skill councils with representation from industry can be an effective way to increase engagement between industry and academia. MDEC has a three-tier capacity-building program that targets youth, university students, and the workforce (see figure 28 on page 43).

Global technology companies such as Cisco with a strong presence in the region are leading the way in developing the next wave of cybersecurity professionals (see sidebar: Cisco Networking Academy Cybersecurity Courses on page 42).

3.4.2 Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players

Our value chain analysis across select ASEAN markets revealed the presence of many global vendors in the products and solution portion of the value chain. While the services part of the value chain has seen some evidence of localization, the potential of the local industry remains largely untapped. Fragmentation of the vendor landscape and lack of regional mobility are major challenges to the local cybersecurity industry participating more fully to address cybersecurity