developments in the private sector and their policy implications are well understood by policy makers. PPP programs have supported numerous objectives including sharing of best practices and threat intelligence, harmonization of standards, greater inclusion of SMEs and research and development into emerging threat vectors. Singapore, for example, has developed several PPP programs, including the Singtel Cybersecurity Institute, the Cybersecurity Centre of Excellence, and the Cyber Risk Management Project. PPPs have tended to focus on three objectives: workforce development, research and development, and information sharing. The main private-sector parties in these partnerships generally come from institutes of higher learning, research institutes, and cybersecurity solution vendors, including cyber insurance.

Industry alliances have also emerged around niche areas such as IoT security, which regional companies could benefit from. These alliances are largely focused on solving security concerns around IoT through collaborative research and shaping of standards. ASEAN countries should look to align with these global industry alliances or explore regional alliances focused on their specific needs. Some of the key alliances that have emerged include the IoT Cybersecurity Alliance, the Industrial Internet Consortium, and the Cyber Threat Alliance. In addition, Cisco has co-founded the Trusted IoT Alliance, a consortium of 17 companies to help establish a protocol for a blockchain-based IoT. The mission of this new alliance is to set the standard for an open-source blockchain protocol in major industries worldwide.

3.4 Build the next wave of cybersecurity capability

Cybersecurity presents a significant economic opportunity for the region, given that it is one of the fastest-growing segments in the ICT space. A concerted effort at encouraging the development of the local industry will allow regional companies to take advantage of these opportunities. Countries in the region need to continue to drive the growth of ASEAN cybersecurity workforce capability and develop frameworks that ensure greater mobility across the vendor ecosystem.

Building the next wave of cybersecurity capabilities will require a focus on four areas:

- Develop the next generation of cybersecurity professionals.
- Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players.
- Foster R&D around emerging threat vectors.
- Anchor world-class capabilities to facilitate knowledge exchange and capability building.

3.4.1 Develop the next generation of cybersecurity professionals

Because of the gap in both capacity and capabilities, the region needs more people to pursue cybersecurity careers with a tailored development of skills to meet the needs of individual industries. In this context, it is important to raise the profile of cybersecurity and develop a clear policy framework for capacity and capability development (see figure 27 on page 41). National agencies in charge of driving the cybersecurity agenda need to lay out a clear strategy around cybersecurity workforce planning aimed at elevating the occupation as a strategic occupation critical to support the digital economy. This requires closer coordination with a range of public-sector agencies, including education ministries, workforce development agencies, and economic development agencies. There is also a need to constantly monitor and track specific cybersecurity skills, such as OT security. Developing forecasts of skills that are in demand and identifying plans to address them is integral to the development of the local industry.