Convention on Cybercrime, proposed by the Council of Europe in 2001, which includes provisions for cross-border assistance between law enforcement agencies on cybercrime separate from the more cumbersome Mutual Legal Assistance Treaty arrangements. Despite the Philippines having committed to the Budapest Convention, none of the other ASEAN countries has signed. Adopting an ASEAN-initiated multilateral regime around cybercrime consistent with the Budapest Convention could bring about strategic and operational benefits to the region, particularly in the area of rapid law enforcement cooperation.

Information sharing among stakeholders is a powerful mechanism to better understand a constantly changing environment. Sharing views on emerging threats, risks and vulnerabilities together with aspects related to national security, provides powerful insight into how the threat landscape is evolving. In this context, it is important to properly define the information sharing mechanism and the underlying rules that govern it, including non-disclosure agreements, traffic-light protocol, antitrust rules, and law enforcement access. A sectorial approach to information sharing is a good start, but this should be extended to encourage cross-sector communication as there are many interdependencies between sectors, for example between the banking and telecom sector for mobile payments.

National cybersecurity agencies have a pivotal role to play in driving adoption and harmonization of **standards** across the region. A start could be made with standards such as ISO 27001 and the NIST Cybersecurity Framework. Collaboration at the sectorial level to share best practices around specific concerns such as IT-OT convergence and wider adoption of standard specifications for sharing threat intelligence such as STIX and TAXII can significantly benefit the region.

Raising awareness about threats and vulnerabilities and their impact on society has become vital. With greater awareness, individual and corporate users can learn how to behave in the online world and protect themselves from risks. Defining the target of awareness-raising campaigns and identifying mechanisms to address them is a joint responsibility of both the public and private sectors. Initiatives such as Safer Internet Day, International Youth Day, and ENISA's security month have helped tremendously to increase social awareness and modify online behavior.

Apart from the above, it is vital that the region adopts a forward-looking **talent strategy** aimed at addressing the capacity and capability gaps highlighted earlier. Cross-regional collaboration efforts at training together with industry can enable countries to tap into each other's strengths to quickly boost the talent level.

3.1.2 Elevate cybersecurity to the top of the agenda in regional economic dialogue

In addition to the Ministerial Conference, a regional operational coordination platform is needed to interface with various national agencies. This facilitates the creation of awareness, cross-border cooperation, and market development activities, including adoption and harmonization of standards (see figure 20 on page 31). A coordination platform can help improve capabilities across the cybersecurity life cycle by facilitating information sharing to improve threat detection, enable region-wide deterrence, provide counter-strategies, and enabling the development of national cybersecurity capabilities. Identification of cyber safe trading partners based on their ability to meet minimum threshold requirements in a timely manner will help to significantly elevate cybersecurity on the economic agenda.

Most importantly, the scope of the annual report provided by the ASEAN secretary-general should be expanded to include a report on the progress of each country based on the Rapid Rapid Action Cybersecurity Framework and foster attention and progress across the region.