

ENISA suggests three types of approaches to share information on cybersecurity incidents: traditional regulation, self- and co-regulation, and information and education schemes.<sup>29</sup>

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

—Sun Tzu

ASEAN countries must move beyond regulations and trigger education and awareness building. In the initial stages of development, an awareness-building approach focused on value-at-risk and driven by national cybersecurity agencies or national-level CERTs could help create a climate of confidence and trust to share good and bad practices and experiences and discuss preparedness measures. Keeping the sharing group small and using traffic-light protocols or other rules on how information could be shared can inculcate the right behaviors around sharing. Regular table-top exercises, cyber incident drills, and stress testing, currently carried out in Singapore and Malaysia, need to be extended to the rest of ASEAN.

There is also merit in cross-sector communication, given the convergence of sectors in the digital sphere (for example, telecoms and banking). It is also useful to develop an early-warning system for CII. Such systems require the cooperation of a wide range of stakeholders, both private and public, and could be the central capability for handling creeping, slow-burn, and sudden crises. Having a common language for sharing threat information enables greater standardization. For example, STIX and TAXII is an open community-driven effort and a set of free specifications that help with the automated exchange of cyber threat intelligence. One of the key benefits of STIX and TAXII is that it helps to exchange cyber threat intelligence between different systems.

Economic incentives stemming from cost savings such as quicker reaction to threats or anticipating network failures and from the quality, value, and use of shared information should be touted as the main reasons for building a sharing culture. More robust sharing of private and public network security information as well as threat information—in real time—would create a level of situational awareness that would enable operational and strategic decisions to be made about how to better protect them and respond to attackers. In Singapore, threat intelligence sharing is facilitated by three-tiered security operations centers at the national, sectorial and corporate levels that facilitate the mandated collection of data and the monitoring and analysis of cyber threats and act as an early warning system for attacks. Singapore’s Ministry of Home Affairs and the Land Transport Authority have established security operations centers for their sectors, and the Cyber Security Agency (CSA) of Singapore hopes to set up similar centers in every sector. In addition, CII owners and operators in certain sectors must report cybersecurity incidents to the regulator. Depending on the nature of the incident, these may then be reported to CSA. In addition to allowing the regulator and the CSA to determine if the incident is systemic, this creates another means of sharing information that may be useful for other CII sectors. Awareness building and education on cybersecurity also takes place in a voluntary manner, as in the UK cross-sector initiative (see sidebar: Cybersecurity Information Sharing Partnership, United Kingdom on page 38).

<sup>29</sup>Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches, ENISA, December 2015