### 3.3.2 Instill a culture of transparency in sharing threat intelligence

Defending a country's digital assets requires close cooperation across a range of stakeholders, including government agencies, the private sector, and end users. Despite general agreement about the need to do this, information-sharing remains inadequate both globally and in the region. Legal impediments—some real, some perceived—are obstacles to more robust information sharing among private-sector entities and between the private sector and the government. The US Cybersecurity Information Sharing Act aims to improve cybersecurity by giving private companies liability protection when they share relevant information with federal or private entities, allowing companies to remove information that identifies someone who is not directly related to a threat.

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

> "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 CIIs. 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