

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)

Cybersecurity Information Sharing Partnership, United Kingdom

The Cybersecurity Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential, and dynamic environment, increasing situational awareness and reducing the impact on UK businesses. The success of this approach depends on the eagerness of members to share information and to be transparent regarding their needs.

The involvement of a national agency such as CERT-UK, assures members that the information sharing platform is secure, and continuously monitored and tested. CiSP produces a wide range of products to cater for organizations at all levels of cyber maturity. These include, but are not limited to:

- Alerts and advisories, including those from national and international partners

- Best practice and guidance documents on common themes
- Quarterly reports on threat trends
- Malware and phishing email analysis

“There are two major obstacles to sharing intelligence. First, there is the difficulty in understanding the benefits of collaborating and sharing what may be deemed as highly confidential information. Second, high volumes of raw data pose a challenge to filtering and classifying what is important.”

—land transportation authority, ASEAN country