### 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**

### 3.3.3 Extend cyber resilience across the supply chain

As discussed, cyber criminals often use SMEs’ low levels of readiness to infiltrate the partnerships these companies have with larger organizations. Because of this, the cybersecurity lens must be extended across the entire supply chain.

Building cyber resilience across the supply chain requires a consideration of supply chain, managed services, and cloud services vendor management practices. The supply chain represents a significant cybersecurity risk because there are many ways a supply chain breach could occur. For example, a software manufacturer could be breached via malware that modifies source code that is then distributed to enterprises that use the software. Another common compromise vector is the theft of a vendor’s credentials that grant remote access to an enterprise the vendor works with, leading to infiltration of the enterprise network from a trusted source. High-profile breaches have included Target, Home Depot, and the US Office of Personnel Management. In addition, ICT services and support are often outsourced to reduce costs and streamline operations.