> "Sophistication of threat vectors is increasing. We are seeing supply chains of leading multinational companies (MNCs) being increasingly targeted with a view to get to the real crown jewels: the MNCs' high-value assets."
>
> **—global cyber insurance company**

Small organizations are often targeted because they are more vulnerable, represent a single point of failure, or have disproportionate access to valuable information given their size within a supply chain.

To build resilience, it is important to institutionalize a multi-stakeholder supply chain risk assessment process that engages as many members of the supply chain as possible. Critical business relationships must be graded according to the consequences of losing their services and be regularly reviewed for relevance and interactions between subsequent supply chain members identified. This is technically challenging and some of the most complex supply chains have so many external partners they may be unable to assess the risk of doing business with each one. The adoption of a security-by-design mindset can help to avoid piecemeal implementation of cybersecurity solutions and the need for costly and often ineffective retrofitting at a later stage. Additionally, aggressive monitoring of data flows across supply chain links can help reveal potential indicators of compromise and provide insight into potentially risky behavior. Businesses across ASEAN can benefit significantly by adopting a security-by-design mindset as part of their cybersecurity strategy.

Building resilience across the supply chain requires a five-step vendor management program as detailed below:

a. Identify the most significant vendors.

b. Specify the primary touch points with each vendor.

c. Establish guidelines that are consistent with a risk-centric mindset.

d. Integrate with the organization's risk management and audit practices.

e. Aggressively monitor data flows across supply chain links.

3.3.4 Forge public–private partnerships and industry alliances

The public and private sectors can benefit from working together on cybersecurity initiatives. The private sector controls much of the critical infrastructure that is vulnerable to cyber threats. Some companies that own such infrastructure have already defined cybersecurity strategies and governance, giving them unique expertise and experience in dealing with potential threats.

Cooperation between industry and governmental agencies on joint cybersecurity initiatives can leverage the unique yet complementary strengths of both sectors. According to the Intelligence and National Security Alliance, the mission of cybersecurity PPPs is threefold. First, these partnerships must identify and detect behaviors of concern. Second, PPPs must ensure that actors from both sectors comply with the standards of the partnership. Third, and most importantly, PPPs must provide a mechanism for response after a cyber threat; this entails conducting examinations of an attack and addressing any necessary shortcomings in the current defense system. Furthermore, effective PPPs should ensure that cybersecurity