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.

> "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.