Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Cyber Supply Chain Risk Management

**First published:** November 2019
**Last updated:** October 2021

# Introduction

All organisations should consider cyber supply chain risk management. If a supplier, manufacturer, distributor or retailer (i.e. businesses that constitute a cyber supply chain) are involved in products or services used by an organisation, there will be a cyber supply chain risk originating from those businesses. Likewise, an organisation will transfer any cyber supply chain risk they hold to their customers.

Effective cyber supply chain risk management ensures, as much as possible, the secure supply of products and services for systems throughout their lifetime. This includes their design, manufacture, delivery, maintenance, decommissioning and disposal. As such, cyber supply chain risk management forms a significant component of any organisation's overall cyber security strategy.

# Managing the cyber supply chain

Cyber supply chain risk management can be achieved by identifying the cyber supply chain, understanding cyber supply chain risk, setting cyber security expectations, auditing for compliance, and monitoring and improving cyber supply chain security practices.

## Identify the cyber supply chain

The first step in cyber supply chain risk management is to identify the cyber supply chain. This includes all suppliers, manufacturers, distributors and retailers, and where possible, their sub-contractors. Furthermore, it is important organisations know the value of information that their systems process, store and communicate, as well as the value of any information that may be entrusted to other businesses.

As a starting point, organisations should establish a list of suppliers, manufacturers, distributors and retailers they have business arrangements with. While an exhaustive list of such businesses, especially their sub-contractors, may not be possible, the identification of those responsible for products or services with security enforcing functions, privileged access or handling particularly sensitive information should be prioritised.

## Understand cyber supply chain risk

Following the establishment of a list of suppliers, manufacturers, distributors and retailers that organisations have business arrangements with, organisations should seek to understand the cyber supply chain risk that those businesses pose through established risk management practices. In many cases, cyber supply chain risk will be the result of foreign control or interference, poor security practices, a lack of transparency, or enduring access. More information can be found on these topics in the Australian Cyber Security Centre (ACSC)'s *Identifying Cyber Supply Chain Risks* publication.

While the determination of cyber supply chain risk will often be the responsibility of individual organisations, in some cases the Government may deem a particular supplier, manufacturer, distributor or retailer, or one of their products or services, to be a national security concern. In such cases, there may be a specific direction issued in relation to managing the associated cyber supply chain risk. In particular, for critical infrastructure providers, the *Security of Critical Infrastructure Act 2018* grants provision for specific direction to be issued by the Government where national security concerns exist.

As a result of understanding their cyber supply chain risk, organisations should be able to develop both a prioritised list of suppliers, manufacturers, distributors and retailers that present a high risk to their organisation along with an associated cyber supply chain risk management plan. It is important to note though that organisations should not only consider the cyber supply chain risk posed by other businesses but also the cyber supply chain risk that they pose to their customers.

## Set cyber security expectations

Regardless of which suppliers, manufacturers, distributors or retailers are deemed a high risk at any given time, organisations should seek to establish cyber security expectations with all of these businesses. As part of this, cyber security expectations should be clearly documented in contracts or memorandum of understandings in order to ensure that businesses are appropriately managing their own security posture, including their cyber supply chain risk. Furthermore, it is critical that such agreements stipulate the requirement for any cyber security incidents to be openly and transparently reported to their customers and appropriate authorities in a timely manner.

In many cases, cyber security expectations set out in contracts or memorandum of understandings should not be excessively restrictive; except where suppliers, manufacturers, distributors or retailers are involved in the provision or support to highly classified systems. Rather, cyber security expectations should be justifiable, achievable and proportional to the information being entrusted to them or the role that their products or services play in an organisation's systems. For example, organisations may seek businesses to demonstrate good faith efforts to implement the ACSC's *Cyber Security Principles* and/or the *Essential Eight Maturity Model*.

## Audit for compliance

Once cyber security expectations have been established with suppliers, manufacturers, distributors and retailers, it is important that organisations have confidence that those expectations are being met. One way to achieve such assurances is through routine audits or other forms of technical assessments. Provisions for such activities should be stipulated within contracts or memorandum of understandings (often referred to as a 'right to audit' clause) and can serve as a way to gain independent assurances of the security posture of businesses.

## Monitor and improve cyber supply chain security practices

Ultimately, effective cyber supply chain risk management is based upon trusted partnerships between suppliers, manufacturers, distributors, retailers and their customers. Such partnerships can be strengthened through common cyber security goals, information sharing arrangements (such as sharing best practices and threat intelligence), assisting each other with responding to cyber security incidents and involving each other in cyber security exercises.

# Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information on cyber supply chain risk management is available in the following ACSC publications:

- *Identifying Cyber Supply Chain Risks*
- *How to Manage Your Security When Engaging a Managed Service Provider*
- *Questions to ask Managed Service Providers*
- *Cloud Computing Security Considerations*
- *Cloud Computing Security for Tenants*.

Further information on cyber supply chain risk management is also available from the following sources:

- the Attorney-General's Department's *Protective Security Policy Framework*, *Security governance for contracted goods and services providers* policy
- the National Cyber Security Centre's supply chain security guidance
- the National Institute of Science and Technology's NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* publication.

# Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).