Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cyber supply chain risk management

First published: November 2019
Last updated: May 2023

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 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 cybersecurity 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 cybersecurity 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 for an organisation is to identify their cyber supply chain. This includes identifying all suppliers, manufacturers, distributors and retailers, and where possible, their sub-contractors. Furthermore, it is important organisations know the value of data they process, store and communicate, as well as the value of any data they entrust 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, handling sensitive data, or will be used in sensitive locations 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, enduring access, or poor business practices. More information can be found on these topics in the *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 non-corporate Commonwealth entities and critical infrastructure providers, the *Protective Security Policy Framework* and the *Security of Critical Infrastructure Act 2018* respectively grant provisions for directions 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 list of trusted suppliers, manufacturers, distributors and retailers that can be used as well as a list of high risk suppliers, manufacturers, distributors and retailers that should not be used. 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 cybersecurity expectations

Regardless of which suppliers, manufacturers, distributors or retailers are used, organisations should seek to establish cybersecurity expectations with all of these businesses. As part of this, cybersecurity expectations should be clearly documented in contracts or memorandum of understandings where possible 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 cybersecurity incidents to be openly and transparently reported to their customers and appropriate authorities in a timely manner.

In many cases, cybersecurity 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 sensitive systems or facilities. Rather, cybersecurity expectations should be justifiable, achievable and proportional to the data being entrusted to other businesses or the role that their products or services play in an organisation's systems or facilities. For example, organisations may seek businesses to demonstrate good faith efforts to implement the *Information security manual*'s *Cybersecurity principles* and/or the *Essential Eight maturity model*.

Audit for compliance

Once cybersecurity 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 cybersecurity goals, data sharing arrangements (such as sharing best practices and threat intelligence), assisting each other with responding to cybersecurity incidents and involving each other in cybersecurity exercises.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information on cyber supply chain risk management is available in the following 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 for executives*
- *Cloud computing security for tenants*.

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

- the Department of Home Affairs' *Protective Security Policy Framework* as well as directions issued by the Secretary of the Department of Home Affairs to manage protective security risks to the Commonwealth
- 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).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate