Identifying Cyber Supply Chain Risks

JANUARY 2021

Introduction

This guidance has been developed to assist organisations in identifying risks associated with their use of suppliers, manufacturers, distributors and retailers (i.e. businesses that constitute their cyber supply chain).

A cyber supply chain is a complex series of interactions across the lifecycle of all products and services used by an organisation. Every time an organisation interacts with a supplier, manufacturer, distributor or retailer there is an inherent risk. As such, these businesses can affect the security of an organisation's systems and their own products or services. If products or services access valuable systems, operate with privileged access or have control over a large portion of a cyber supply chain, they may represent a weakness that could be exploited by an adversary. In such cases, this could have wide-reaching and harmful consequences.

Foreign control, influence and interference

Nationality considerations

The nationality of suppliers, manufacturers, distributors and retailers is critical to the ability of organisations to assess their cyber supply chain risks. Organisations should determine the nationality of businesses involved in their systems, products and services' design, manufacture, delivery, maintenance, decommissioning and disposal.

It can be difficult to identify the nationality of suppliers, manufacturers, distributors and retailers, particularly for multinational corporations. As such, organisations should research businesses using data they publish about themselves in official documents (such as annual reports) and validate this information using reliable third-party sources. Generally, nationality is determined by where a business is incorporated, where central management is located and the nationality of those with control over voting rights.

Publicly available information may not be sufficient in determining a business' legitimacy if they are deliberately masquerading as something they are not. If operating critical infrastructure or systems of national significance, seek Australian Government assistance on these matters.

Foreign control

Foreign control is when a supplier, manufacturer, distributor or retailer is subject to foreign government laws. In such cases, businesses may have to comply with directions that conflict with Australian laws or interests. Further, such businesses based in foreign countries may be subject to powers granting a foreign government control over that business or access to its information holdings.

Foreign influence and interference

Foreign influence is when a foreign government attempts to influence Australian society in a way that benefits their interests. For example, activities such as political lobbying are conducted openly and in a transparent manner, and are not of concern. However, when conducted covertly, it is deceptive, corrupting or threatening in nature, and when it is contrary to Australia's sovereignty and interests, it is classified as foreign interference.

Identifying cyber supply chain risks

Organisations should identity components and services relevant to the security of their own products, services and systems. As such, organisations should review each supplier, manufacturer, distributor and retailer in order to assess the potential increase to their security risk profile. The following questions can assist with this process.

Risks due to foreign control or interference

- **How likely is the business to be subjected to foreign control or interference?**
  - What access might a foreign government gain in controlling or interfering with the business?
  - What access does the business' products or services have within their customers' environments?
- **To what extent might the business be controlled or interfered with?**
  - Where does the business operate?
  - Where is the business headquartered?
  - Who has controlling shares in the business?
  - What are the nationalities of board members and key employees?
  - What ties do board members and key employees have to the government of countries they operate in?
  - Is there any evidence of corrupt or criminal activities by board members or key employees?

Risks due to poor security practices

- **Does the business demonstrate good cyber security practices?**
  - Does the business follow a cyber security standard for their own systems?
  - Has the business made a commitment to secure-by-design practices for their products and services?
  - Does the business use secure coding practices?
  - Does the business deliver secure-by-default products and services?
  - Has the business made a commitment to maintaining the security of their products and services?
  - Does the business have a vulnerability disclosure policy?
- **Does the business protect their own cyber supply chain?**
  - Has the business identified all third-parties and their role in delivering their products and services?
  - Does the business actively manage risks in their own cyber supply chains?

- **How does the business manage their employees?**
  - Does the business conduct background checks on individuals before they are employed?
  - Does the business have a program to detect malicious insiders?
- **How does the business handle cyber security incidents?**
  - Has the business, or their products or services, been compromised previously?
  - Is there any negative reports of the business' handling of cyber security incidents?

Risks due to lack of transparency

- **Is penetration testing supported and encouraged?**
  - Can penetration testing be conducted on the business' products and services?
  - Will the business share results of any previous assessments against cyber security standards?
- **Do contracts explicitly address cyber security risks?**
  - Can cyber security requirements be specified in contracts?
  - Is mandatory cyber security incident reporting included in contracts?
  - Is the right to audit contractual cyber security requirements included in contracts?
- **Is the delivery of genuine products guaranteed?**
  - Can the delivery path of products be guaranteed?
  - Does the business offer anonymity for purchasers if products are sourced from overseas?
  - Are measures implemented to assist in detecting counterfeit products?
  - Do counterfeit versions of the business' products exist on the open market?

Risks due to access and privileges

- **Is access and privileges used by products and services justifiable?**
  - What is the extent of access that products and services will have to systems and data?
  - Do products and services operate with privileged access?
  - Do products and services minimise unnecessary privileges?
  - Do products and services require enduring access to the internet?
- **Is enduring access to products and services by the business justifiable?**
  - Does the business require enduring access to their products, or their customers' systems or data?
  - Will systems or data be accessed from anywhere other than from a low-risk nation?
  - Will data be stored anywhere other than in a low-risk nation?
  - What security measures are used to protect any forms of enduring access?

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. The ***Guidelines for Outsourcing*** in particular contain additional guidance on the procurement of outsourced services. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

For further information on cyber supply chain risk management, see the ***Cyber Supply Chain Risk Management*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.