Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Supply Chain Risk Management Executive companion

JUNE 2019

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has produced this guidance to inform executives and supply chain policy makers in government, critical infrastructure, and large organisations, about key cyber security issues related to Cyber Supply Chain Risk Management (SCRM).

All organisations need to consider some element of Cyber SCRM. If another party is involved in the delivery of a product or service to your organisation, then there will likely be an induced cyber security risk from that entity. Additionally, your organisation will transfer any untreated supply chain risk to your customers.

Cyber supply chain

- **Understand your cyber supply chain.** Holistic supply chain management governs a secure supply of products or services to your system, ensuring business continuity and in some cases, national security. SCRM is a whole of system life undertaking. Your supply chain includes the design, manufacture, delivery, support and decommissioning of hardware, software and related services in your systems. The cyber security component of your supply chain is a significant component of an overall SCRM strategy, due to the impact and extent of cyber supply chain exploitation vectors on business.
- **Good SCRM is realistically proportionate**. Ensure you consider SCRM alongside other relevant cyber security risks. If your organisation's cyber security posture is vulnerable to non-targeted intrusions, those uncontrolled risks must be addressed. Consider complimentary advice such as ASD's ***Strategies to Mitigate Cyber Security Incidents***.

Extrajudicial direction, interference and high risk vendors

- **Know what makes a vendor high risk.** A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of your system. That vendor can be subject to adverse extrajudicial direction or the vendor's poor cyber security posture means they are subject to adverse external interference. In both cases, if not managed, the vendor can transfer unreasonable risk to your system.
- **Extrajudicial control**. Describes an organisation who is (likely) subject to directions from a foreign government and those directions (likely) conflict with Australian law or interests.
- **Extrajudicial influence**. Be aware that organisations will be subject to some level of extrajudicial influence when providing a service in a foreign country, due to obligations to comply with local laws.

- **Foreign interference**. Describes the actions of foreign intelligence service (FIS) or foreign military to meet intelligence collection or effect requirements, through affecting your supply chain. This could be achieved through extrajudicial direction or through covert compromise of a provider in your supply chain. ASD has frequently responded to incidents where security flaws in providers are covertly exploited to compromise multiple high value victims.
- **Why an adversary will target your supply chain.** A cyber adversary may choose to utilise a supply chain vector rather than directly compromise the target, due to the likely extensive access to multiple targets and difficult to detect nature of the vector.
- **Vendor nationality.** Understanding if another country's laws and intent pose a specific threat to an Australian interest through a vendor requires understanding the specific country's likely interest in the system, the country's historical relationship with Australia or similar nations, and the specifics of the vendor themselves. There is no simple absolute like 'if the vendor is headquartered in country x, there is a definite risk for all systems'.
- **Remember security of personnel.** People are involved in your supply chain. Persons with privileged access to your system are a risk that must be considered. If a person servicing your equipment is a citizen of another country, even if they reside in Australia, they may be compelled under that country's law to conduct actions on behalf of that nation.

Case study 1: UK NCSC advice to UK government to avoid Russian antivirus companies for critical systems

In 2017 the UK NCSC wrote to the UK government informing them that the risk posed by Russian antivirus to official and nationally critical systems could only be mitigated by avoiding those products. The UK was fully aware of a real threat posed by a specific country and product 'Russia has the intent to target UK's central Government and the UK's national critical infrastructure.'

The UK NCSC noted that if 'access to the information by the Russian state would be a risk to national security, a Russian based AV should not be chosen.'

Source: https://www.ncsc.gov.uk/information/letter-permanent-secretaries-regarding-issue-supply-chain-risk-cloud-based-products

Know your system

- **Identify your most important systems**. Know the systems from a business and security perspective. Know if your system is nationally critical and where multiple other national systems depend significantly on the system.
- **Understand your key systems well.** If you know a system is critical, a sound understanding of the system including its key components and interdependencies is critical to making informed SCRM decisions. Consider roles of components in the system by asking key questions. For example, does the component perform a security enforcing role in that system? Does it allow a privileged level of access to the system? What else does this component depend on for its function?
- **Determining national level criticality or sensitivity.** If your system has a widespread, significant impact to national security if compromised, it should be considered nationally critical or sensitive. Systems may also be considered

critical or sensitive but without national scale impact of compromise. If impact of compromise is local to your organisation only, then it should be considered locally important.

- **Know who owns the risk**. The owner of a system is the ultimate owner of risk to that system, however be aware any untreated risk is transferred to others who depend on your system or business. For critical infrastructure providers, the ***Security of Critical Infrastructure Act 2018*** grants provision for specific SCRM direction by Government where National Security interests exist.

Case Study 2: Demonstrated sensitivity of unclassified but nationally critical data

In 2016 a public announcement was made by the Australian Government that the Bureau of Meteorology (BoM) had been compromised by malicious cyber actors. Australian weather data and predictions are a key dependency for many Australian and overseas services, and any issue with that service impacts others significantly. The announcement of a cyber compromise caused a significant volume of questions to the Bureau from its extensive range of clients, all concerned they were potentially negatively impacted.

The dependency of external services on BoM was extensive, although there was no loss of weather service, just the potential or perceived impact to other services caused a significant impact.

Understand your supply chain risk

- **Make relevant system risk assessments**. Develop a good understanding of your supply chain and its dependencies in your system. This detailed understanding will identify the key risk components. An assessment made for another system, organisation or context may not suit your system.
- **Know where your supply chain is vulnerable**. Vectors for cyber supply chain compromise can be either hardware, software or service provision. Supply chain exploitation only needs to target a weak link in the supply chain in order to achieve the objective. As with your vendors of hardware and software, ensure your managed service providers are also considered in your SCRM strategy. Be aware that if a vendor has poor quality control and/or cyber security practices, you inherit that risk.
- **Keep informed of current supply chain threats.** Pervasive supply chain threats are a combination of foreign interference intent and technical capability. Determining likely threats can be assisted by looking at historical incidents in your organisation and sector. The ACSC and similar organisations will inform key stakeholders through established means, when significant, unmanaged cyber threats are identified.

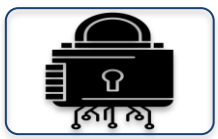
Case study 3: Supply chain manipulation to compromise many to further exploit a targeted few

In 2017 a free system performance tool, CCleaner, was modified to serve malware along with the legitimately distributed and digitally signed CCleaner install file. Once the initial malware was running, it made an automatic check to see if it was running on a specific victim, based on an internal list of targeted domains of interest.

If the malware was running on a victim of interest, it would install a secondary stage of malware. This explicit list of victims for exploitation indicates supply chain interference for some specific and targeted outcome, which can indicate state-sponsored interference, versus an opportunistic cybercrime activity.

Source: https://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

Related: https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers



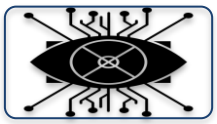
Manage your supply chain risk

- **Avoid or reduce high supply chain risk.** Avoiding risk may be possible through re-architecture of a system or process, in order to minimise the impact of a realised risk. Reducing risk could be accomplished by choosing vendors who have a demonstrated commitment to cyber security from.
- **Be cautious when transferring or accepting high risk.** The decision must be well understood and documented. There should still be some compensating controls, which may require consultation with external parties who will also be affected by the risk if realised. Be aware you may also be transferring risk to your customers.
- **Specific Government supply chain direction.** Where a system is deemed as critical to national security, there may be specific Government direction related to managing cyber supply chain risk, particularly where there is legitimate concern over significant non-sovereign ability to control or influence a nationally critical system.
- **Objectively manage risk**. Be cautious of making decisions solely based on nationality of a vendor. Extrajudicial direction is an aspect of a high risk vendor, however the poor cyber security posture of a vendor can impact you as much, if not more.
- **Build relationships with your vendors and customers**. Managing your supply risk requires a strong partnership and clear understanding between you, your vendors and your customers. Cyber security will need to be part of an upfront and ongoing business relationship.

Case study 4: Re-architecture avoiding supply chain risk.

In 2018 an organisation requested ASD assistance, regarding the use of a cellular network dongle in a sensitive system. The dongle required the installation of unverifiable software in order to make the dongle work. The software may have been installed with a high level of privilege on that system, and so could undermine security of the business.

ASD recommended re-architecture of the system to remove the need to install the software on the device, by using an alternative technology, thus avoiding the need to install unverifiable software on the sensitive system.



Monitor your supply chain and controls

- **Take control.** Your supply chain and the systems they support change significantly over time. Ongoing monitoring will ensure that controls do not lapse and new risks are identified early.
- **Keep records and track assets**. Good records significantly assist with rectifying any realised supply chain risk. Record SCRM decisions and procurements, and track where those assets are used in the system. Make the records available to those who will monitor the supply chain and related systems.
- **Raise awareness.** Make ownership of your cyber supply chain security a whole of organisation responsibility.
- **Manage cyber incidents effectively**. Ensure a well understood incident reporting chain exists. Any cyber security incidents that have a significant impact must be reported to senior management, and likely to government.

Case study 5: Excellent monitoring detects a targeted cyber security incident.

An organisation reported to the ACSC that they had detected brute force attempts against an internet facing remote access system. The attempts were utilising non-public and correct user names, indicating this was not standard internet based brute-forcing.

Due to well set up logging, monitoring and an understanding of the business, initial investigation demonstrated some level of information leakage already from the internal network. Not long after the initial report, an inauthentic successful user password combination was made, confirming internal network credentials and remote access were compromised. Further investigation revealed a significant APT compromise of the network, but the monitoring and business knowledge meant the incident was self-detected early.

Further reading

- ***Strategies to Mitigate Cyber Security Incidents*** https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
- ***Managing security when engaging MSPs*** https://cyber.gov.au/business/publications/msp-risk-for-clients/

- ***MSP Better Practice Principals*** https://www.cyber.gov.au/publications/msp-better-practice-principles
- Australian Critical Infrastructure Centre, ***Protecting your critical infrastructure asset from foreign involvement risk***, https://www.homeaffairs.gov.au/nat-security/files/cic-best-practice-guidance-supply-chains.pdf
- Department of Finance ***Buying for the Australian Government*** procurement policy https://www.finance.gov.au/procurement/procurement-policy-and-guidance/buying/
- UK National Cyber Security Centre, ***Supply Chain Security Collection*** https://www.ncsc.gov.uk/guidance/supply-chain-security

Glossary of terms

Term	Definition
Risk	Cyber risk is the graded severity of impact to security through realisation of a vulnerability by a threat.
Supplier and Vendor	Generally the manufacturer and/or primary source of a product or service. Multiple suppliers may be used in a product or service. It is generally considered a business to business relationship. In this document vendor covered the term supplier too. A vendor is typically the organisation that supplies a product or service to the customer.
Supply Chain	Supply Chain in general refers to the whole life of an IT product or service in an organisation. It likely includes multiple organisations. Supply chain includes the linked processes of design, manufacture, supply, delivery, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisations ICT ecosystem
Supply Chain Risk	Supply Chain Risk refers to the combination of vulnerabilities in an organisations supply chain, the threats that organisations supply chain is likely exposed to, and the impact of a realised vulnerability by a threat.
Supply Chain Risk Management	Supply Chain Risk Management refers to the process of identifying supply chain threats and vulnerabilities to determine the most likely risks, and ultimately the treatment of high supply chain risks.
Threat	A cyber threat is anything that can or will exploit a vulnerability, intentionally or accidentally, and compromise the security of that system. Threat assessments should remain realistic, with historical evidence providing guidance on the likelihood of a threat existing.
Vulnerability	A cyber vulnerability is a weakness in a system that can be exploited by a threat, ultimately compromising the security of the system.