Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Supply Chain Risk Management Practitioner Guide

JUNE 2020

Introduction

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has produced this guidance to inform cyber security practitioners, procurement officers and supply chain decision 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 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.

Organisations can use this guidance to frame the correct questions with relation to SCRM and vendors that are considered high risk.

Executive summary

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.

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.

Specific Government direction related to supply chain. Government may provide explicit direction where there is legitimate concern over significant non-sovereign ability to control or influence a nationally critical system. Specific SCRM direction by Government should be well understood and not applied out of context or avoided.

Consistently approach supply chain risk management. The following four steps are common to managing complex risk consistently:

- **Know your system.** An organisation must determine criticality of their systems, with regard to sensitivity and business value, especially in a national security context, in order to inform appropriate risk activities.
- **Understand your supply chain risk.** Make relevant system risk assessments by knowing the systems well, including how they can be exploited and keeping informed of the relevant current threats.

- **Manage your supply chain risk.** Objectively manage supply chain alongside other system cyber security risks**.** 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.
- **Monitor your supply chain and the controls.** Your supply chain and the systems they support will change over time. Regularly monitor and review your SCRM and the controls. Ensure that the whole organisation supports a secure supply chain and any incidents are reported in a consistent manner.

Cyber supply chain

Cyber supply chain includes the design, manufacture, delivery, deployment, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisations cyber ecosystem. Supply chain must consider the whole life of an IT product or service in an organisation.

An organisation must determine criticality of their systems with regard to sensitivity and business value, in order to inform appropriate risk activities.

Cyber supply chain risks refer to the combination of vulnerabilities in an organisation's cyber supply chain, the threats that the vulnerabilities are likely exposed to, and the impact of a realised risk.

Roles in supply chain risk management

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***[1] defines what critical infrastructure is and grants provision for specific SCRM direction by Government where National Security interests exist.

The Australian Government does have existing process and resources to support aspects of supply chain risk management:

- The Department of Home Affairs runs the Critical Infrastructure Centre (CIC). The CIC provides supply chain risk advice and assessments for Critical Infrastructure and Telecommunications providers under the ***Security of Critical Infrastructure Act 2018***
- The Department of Finance provides government procurement guidelines. This guidance primarily covers appropriate use and accountability for public monies. Of note are security clauses that can be considered where there is a legitimate security concern.
- The Attorney-General's Department publishes the ***Protective Security Policy Framework*** (PSPF). This guidance covers protective security considerations and mitigations for people, information and assets.
- The Attorney-General's Department manages the ***Foreign Influence Transparency Scheme Act 2018***[2]. The scheme comes into effect in 2019 and although not focussed on cyber security, the scheme may provide some means of determining foreign influence in certain circumstances.
- The Australian Security Intelligence Organisation (ASIO), primarily through the Business and Government Liaison Unit (BGLU), provide protective security advice to government, business and critical infrastructure[3].

[1] https://www.legislation.gov.au/Details/C2018A00029
[2] https://www.ag.gov.au/Integrity/foreign-influence-transparency-scheme/Pages/default.aspx
[3] https://www.asio.gov.au/protective-security.html

- The Australian Signals Directorate (ASD) through the ACSC, provides cyber security advice and assistance to government, business and critical infrastructure[4]. As part of this role, the ACSC co-ordinates and investigates cyber security incidents that impact national security.

Extrajudicial direction, interference and high risk vendors

Foreign interference in supply chain. Your system may be subject to enduring interest of another nation that does not respect the sovereignty of that system. This risk cannot necessarily be mitigated by technical controls alone.

Extrajudicial control over a vendor. Describes organisations who are likely subject to extrajudicial directions from a foreign government and those directions likely conflict with Australian law or interests. The organisation is likely headquartered in the country of concern and the government of that country is able to exert significant control or influence. A nation may choose to exert this influence where its own laws, policies or powers require access or control over a certain type of data. Be aware that the restraint or oversight in exercise of those powers can differ significantly from nation to nation.

Extrajudicial influence over a vendor. Describes organisations who are likely subject to extrajudicial directions from a foreign government. The organisation is likely headquartered in another country but is required to operate in accordance with foreign laws in order to operate in that country.

Interference by a Foreign Intelligence Service (FIS) in a supply chain. Describes the actions of FIS or foreign military to meet intelligence collection or effect requirements by interfering with your supply chain. A nation state may choose this path if supply chain exploitation provides significant breadth of access to multiple targets or the target was unable to be exploited by other means.

Know your vendors and their related dependencies

Understanding if **another country's laws and intent pose a specific threat to an Australian interest** requires understanding the specific country's likely interest in the system and their historical relationship with Australia.

To understand the risk posed by the interaction of a nation and a vendor, you need to consider:

- What country has primary influence over that vendor? This is usually determined by the primary nationality of the vendor.
- To what extent the vendor is influenced by the state. This may even differ for different companies in the same country. Realistically this may be very difficult to determine, however where very high impact is determined, such as with nationally critical systems, assistance can be sought from some of the contacts in this document.
- What other nations influence the vendor? This occurs if the vendor provides services to, or manufactures its product in another country. It may be of particular interest if your data is located in a country considered high risk through a service used or provided by the vendor.
- What are their internal cyber security practices like? If a vendor cannot secure itself, it is open to exploitation by any actor interested in exploiting an organisation through the trust given to a vendor.
- What significant dependencies does a vendor have for the delivery of their product or service? Sub-contracting is very common, and an organisation may find its data being stored or accessed by another vendor it did not expect to be involved.

[4] https://www.cyber.gov.au/

- The broader perspective of a specific vendor's activity in Australia. For large vendors, nation-wide level influence is feasible. Look at other activity undertaken by that vendor in your region to determine if there is any unexpected influence to your system.
- Where there is a nationally critical system, it is useful to know the experience of others with that vendor, including whether it has successfully positioned itself in another aspect of your cyber supply chain or influencers.

For information on specific countries in relation to Australia; especially those which Australia has explicit sanctions against, see the Department of Foreign Affairs country briefings[5].

The outcome of **determining obvious foreign nationality** of a vendor includes determining if the vendor may be subject to extrajudicial influence. However, determining the nationality of a specific vendor can be non-trivial, especially where the organisation is a multinational corporation. Generally nationality is determined by where the company is incorporated, where central management is located and the nationality of those who control voting in the company[6]. Techniques captured below are not intended to determine the legitimacy of a vendor deliberately masquerading as something it is not. Basic techniques to determine nationality include:

- Research the organisation using data they publish about themselves. Find out where their headquarters are, ask where they are incorporated and find out who controls the organisation.
- Use publicly available information to validate the organisation's own data.
- Look for technical validators, for example, research the domain 'WHOIS' registration details for their internet services such as their public website.

Nation specific service provision considerations. Using extrajudicial influence, a country may require a vendor, considered to have nationality in another country, to implement country specific controls in order for that vendor to legally operate a service in that country. These are not always negatives and in many cases improve the security of the vendor's service. However, be aware what this may mean for your data, if for example operation of a certain piece of equipment in another country means the data must be stored in that country, thus is subject to extrajudicial control, or cannot be accessed legally for oversight by the customer, due to local privacy laws.

Cyber security of the supply chain and the system. Is the vendor, system, or interconnected system vulnerable to some means of technical exploitation? This vulnerability is likely mitigated by technical controls.

Physical and personnel considerations of supply chain management are also critical aspects of SCRM. However, they are not covered in any depth in this document. For more information, see resources provided by the Attorney-General's Department related to protective security and the UK National Cyber Security Centre (NCSC), referenced at the end of this document.

Case study 1: UK NCSC advise 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.'

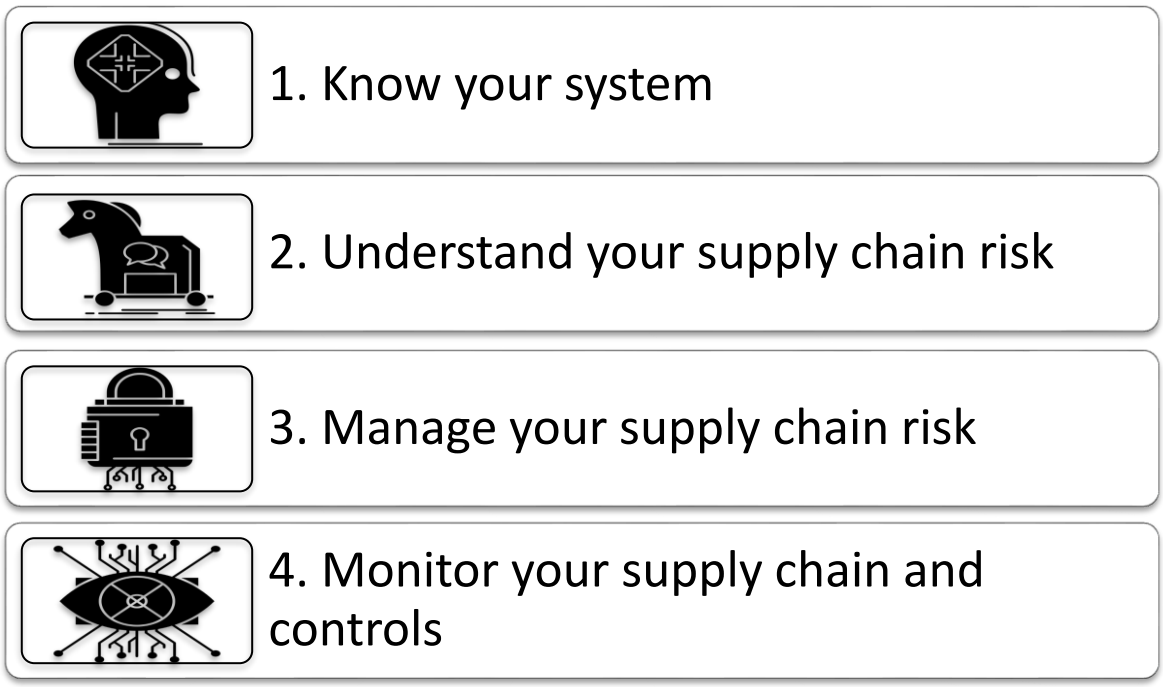
The UK NCSC noted that if 'access to the information by the Russian state would be a risk to national security, a Russian-based AV should not be chosen.'

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

[5] https://dfat.gov.au/geo/Pages/countries-and-regions.aspx
[6] https://www.ato.gov.au/Business/International-tax-for-business/In-detail/Residency/Residency-requirements-for-companies,-corporate-limited-partnerships-and-trusts/

An approach to Supply Chain Risk Management

SCRM requires an understanding of the context in which the system will be used, the most likely vulnerabilities and threats to the system, and the impact of a realised risk. The following four aspects of SCRM will assist you with managing supply chain risk.



Step one: Know your system

Good SCRM in an organisation requires knowing what your most important systems are from a business and security perspective.

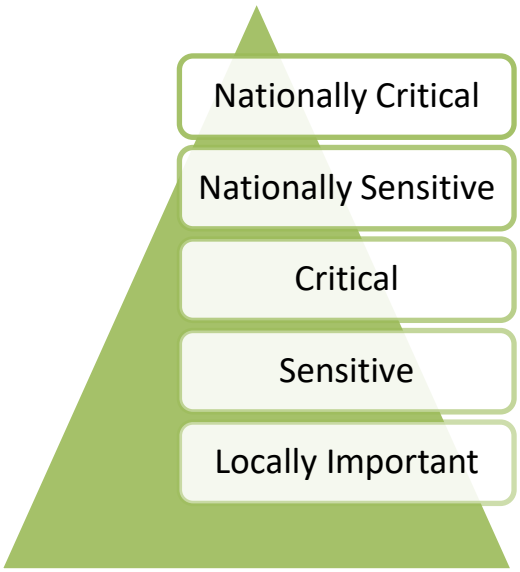
To enable assessment of the criticality, sensitivity and business value of a system, consider the following elements of the system:

- **National Criticality**. Does the nation depend on the system or service in some significant way? For example, if it is a warfighting capability or critical infrastructure in a time of war, what will be affected if the systems confidentiality, integrity and availability (CIA) cannot be trusted?
- **Threat to life**. Do real threat to life concerns exist if the system is vulnerable to a threat in some way?
- **Immediate data access and data sensitivity**. Know the sensitivity and amount of data the system immediately handles. If this system is compromised, what would it immediately expose? Some considerations include:
  - Is the data classified? If so, it has explicit sensitivity.
  - Does the system handle Personally Identifiable Information (PII) or Intellectual Property (IP)? If so, what impact would exposure have?
- **Interdependency of the system**. Knowing what could be exposed or enabled if the system is compromised, helps to identify critical systems. This is a pre-requisite to correctly assess what could and would likely be achieved by a supply chain threat. Four considerations for assessing the impact of a system compromise include:

- **Level of access the system has to other systems**. If the system or service is one or more steps removed from the data of a sensitive system, then it may be used to access or control the actual sensitive system of concern.
- **Dependency of other internal systems on this system or service**. If the system is acting in a critical administration or security enforcing role , or it is the main backbone of your entire network, then it provides a critical failure point for the control of data that is in that system.
- **Dependency of external systems on this service - who else is impacted**? If your service is taken offline, or loses data - who else will it impact?

- **Longevity or lifespan**. The longer a system is in operation in a specific state, exposure to supply chain risk increases. For example, a system expected to have a life span of a decade or more presents a much greater opportunity for interference compared to a short term deployed system.

Assessing the criticality of a system should be considered where it fits into national security priorities. This assists in determining how much the supply chain risk should be consulted wider than the organisation itself. With regard to system sensitivity, five broad categories can be defined from 'nationally critical' to 'locally important':



- **Nationally Critical**. The system is recognised as critical to the function of the nation, and underpins the security of systems nationally and the wellbeing of the nation. Some national critical infrastructure will be in this category.
- **Nationally Sensitive**. The system if compromised would impact national security, but not cause the significant undermining of other systems. This may include some nationally classified systems.
- **Critical**. A compromise of the system would have significant but localised impact to the security of many systems. This may include some smaller critical infrastructure.
- **Sensitive**. The system contains data important to national security, but impact is localised. This may include stores of PII.
- **Locally Important**. The system is important for the owner of the data primarily, with little impact beyond the organisation itself.

As a system sensitivity trends from locally important to nationally critical, more consideration to all aspects of supply chain risk needs to be considered.

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.

Step two: Understand your supply chain risk

The information security of a cyber-system is typically considered with respect to incident impact on the confidentiality, integrity and availability (CIA) of the system and the data it holds.

Knowing the breadth of influence, and depth of access of a system informs real world impact of any incident on the system, either from physical, supply chain, or system compromise breach sources. Knowing real world impact upfront will inform a proportionate evaluation of threat and vulnerabilities.

Determine overall risk by overlaying where your system is vulnerable, with real threat to the system. This will ultimately determine and appropriately prioritise supply chain risk.

Consider the most realistic, likely, and high impact risks first. Supply chain risk management should not detract from managing more immediate risks.

Understand components of your supply chain

Managing supply chain risk in your system is a whole of product or service life undertaking. In order to understand the breadth of cyber supply chain risk, be aware of four primary aspects in a product's life:

- **Vendors**. The potential for the vendors to introduce unique vulnerability, either during design, manufacture, supply or the aftercare of the product they are responsible for.
- **Delivery and deployment.** As the product is in transit from a vendor to the customer there is a risk of tampering or data extraction, enabling immediate or future malicious operations.
- **Service**. The ongoing service and administration of equipment and services deployed in an organisation is a significant vector for risk. For example, the compromise of managed service providers from 2016 – 2018 was one of the most commonly observed realised risks in ACSC cyber investigations. The relatively low cost of exploitation, extensive access provided, difficulty of detection and complexity of remediation makes this one of the simplest means for criminal groups to exploit multiple victims.
- **Decommissioning.** As a product or service is moved to end of life, there is potential for the old product or service to contain sensitive information or enable access to the new system in some way. For example, there is a good reason second hand hard drives can sell for more than their new counterparts.

Across the above four control points of supply chain, cyber security risk is introduced in two main ways:

- **Interference risk**. The vendor can be influenced to conduct adverse actions on behalf of another party. This risk is enduring and relevant where the vendor is subject to extrajudicial control or influence.
- **Technical risk**. Where the vendor does not apply adequate quality control over their products and services. Technical risk includes not just the inherent security of the product or service, but also the vendor's ability to secure their own systems from unintended external influence. Low quality products and services is a commonly realised risk due to the cutting of security costs by a vendor in order to deliver a more cost competitive product.

Case Study 3: Multinational companies offering nation specific service provision to comply with local legislation

In 2018, Apple announced a new data centre will be utilised within China, operated by a Chinese company, in order to meet new Chinese data protection legislation for data generated within China. In this case the country is able to influence extrajudicial law, which may be in contradiction to Australian law. Reuters noted Apple as saying "The addition of this data centre will allow us to improve the speed and reliability of our products and services while also complying with newly passed regulations."

This is not specific to Apple, but applies to other service providers too. Google's rumoured project 'dragonfly', a customised search engine for China is another example. It is too early to know the actual impact to Australians in China, but it may be assumed that if the data was generated in China, it will likely fall under a separate set of capabilities, and legislation, to the data generated in Australia. This is despite the fact that the owner, and possibly user, of a service is not Chinese.

Source: https://www.reuters.com/article/us-china-apple-idUSKBN19X0D6

The vector for supply chain interference, targeted and/or non-targeted, can come through either software, service provision or hardware.

Be cautious of making decisions solely based on nationality of a vendor. A vendor from a country whose laws are not likely contrary to Australian law, does lower the immediate elevation of risk associated with likely adverse extrajudicial control in nationally critical systems. However:

- If the vendor is from a country of possible concern, and considered "high risk", that alone should not rule out the vendor unless there is specific Government direction to do so in the circumstance. Instead, consider the actual role of the system under question relative to critical data and complimentary security controls.
- Conversely, if a vendor is not from a country of concern with regard to extrajudicial influence, this should not immediately rule them as a lower risk option with regards to overall cyber supply chain risk. There are still cyber security vulnerabilities that must be considered.

Determining the **cyber security posture of a vendor** is at minimum, asking for evidence of compliance with commonly known standards they would already have to comply with for the different regions they operate in. In the absence of that, ask for demonstration that the vendor has complied with best practice guidelines such as the ACSC Essential Eight. Be aware that a multinational corporation may struggle to provide some of these assurances beyond a local level and compliance is no guarantee that the system is secure.

Knowing if a sub-contractor is used should be part of negotiations and contractual agreement. A vendor must notify you if any of your data or service delivery is outsourced to another party. If you deem your data or service is critical or sensitive, it is your organisation and reputation at risk. Sub-contracted services are becoming practically difficult to determine where there is increasing dependency on abstracted cloud services, however it remains a legitimate and important consideration if the system or data is deemed sensitive.

Case Study 4: Defence data stolen through sub-contractor breach

In 2016, sensitive but unclassified data on a Defence project was stolen through a sub-contractor. The ACSC investigation found the sub-contractor had been employed by a service provider to Defence, rather than directly by Defence. This is not uncommon, however the security controls in the sub-contractor did not meet the expectations the department had of the service provider.

Given the sub-contractor did not provide "classified" services, they would not have fallen subject to the same controls as the service provider. To raise awareness of an increased risk, the client should define what data is 'sensitive' and provide a contractual obligation to inform them if the provider outsources the handling of any sensitive data. Once aware of their involvement, to mitigate this activity, the sub-contractor should have demonstrated a certain level of cyber security maturity to the client and provider.

Know the likely supply chain threats – intent and technical means

Pervasive supply chain threats are a combination of foreign interference intent and technical capability.

Determining the likelihood of a threat being realised is backed by historical evidence. Look for historical targeting in two main areas:

- **History of your organisation being targeted by cyber adversaries**. This information may be sensitive within the organisation. However, if the system is of critical sensitivity, an understanding of historical security incidents must be asked of the relevant area in the organisation. Know if the organisation has had ongoing targeting or even successful compromise, especially where there is indication it was targeted by a nation state. Previous targeted incidents represent a real targeting requirement of the organisation by a nation state that is unlikely to cease. Previous incident data will also inform the systems of interest to the defender and the intruder. Be mindful that the tradecraft used in the last attempt is not necessarily the tradecraft used to gain access the next time.

- Know **what targeting looks like in your sector**. Through trusted forums and reporting, an organisation can learn from the experience of others. Additionally, public reporting, by security companies or victims of target activity, provide a lot of information regarding what real 'Advanced Persistent Threat' or nation state activity looks like and what they target.

Threat to supply chain is not limited to extrajudicial influence. Foreign interference is not just related to a vendor's country of origin. As the case studies demonstrate, it is usually simpler to compromise another product or service in the supply chain without lawful interference, in order to achieve the required outcome.

In addition to extrajudicial control resulting in technical interference, consider the **risks posed by people with privileged access**. 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.

In order to accomplish some objective on the system of interest, a malicious cyber actor has multiple technical options. Some **categories of technical threats** to supply chain include:

- Unauthorised access – which ultimately enables a malicious actor to do almost anything at any time to the system.
    - Temporal unauthorised access to data on a system. This may come in the form of abuse of an authorised access, such as a contracted service provider, to a temporal opportunistic access such as uncontrolled physical access to a device as it is in transit.
    - Persistent unauthorised access to a system. A 'backdoor' in the system that enables unauthorised future access any time. This is one of the most commonly feared threats, perhaps because it is easily understood, invasive, and unwanted.
- Passive snooping or modification of data or the system. Outside of unauthorised access, data access can occur if the system exposes opportunity to view, create, or modify data in transit or at rest, resulting in snooping or manipulation of data.
- Denial of service. The deliberate or accidental, disruption of the system through some vulnerability. Whatever the motivation, service disruption is a significant consideration for nationally critical systems, particularly where there may be threat to life. It may be enabled by the above two threats, or even by poor quality components in supply chain, such as the case with counterfeit technology.

Obsolescence. Although it may not be a deliberate attempt to compromise system security, the incorporation of unmaintainable hardware and/or software in a system is a persistent threat for critical systems. Consider the enduring risk of non-updatable software deployed into critical systems that are now internet-connected.

Case study 5: 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

Source: https://www.ccleaner.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users

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

Step three: Manage your supply chain risk

Treat high 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.

Transferring or accepting significant risk must be well understood if considered viable. This must be a conscious and documented decision, and may require consultation with external parties who will also be affected by the risk if realised. Be aware that you may also be transferring risk to your customers.

Avoiding the risk may be possible through re-architecture of a system or process in order to minimise the impact of a realised risk. Look to change the impact factors for a product or service. For example, if an untrusted network equipment component is utilised, it may be possible to architect around the product so that other trusted components handle encryption, authorisation, and audit; thereby reducing the dependency on that component to enforce whole of system security. However, a cost benefit analysis should be conducted to determine if this actually increases complexity of the system outside reasonable ability to implement and maintain the system.

Case study 6: Re-architecture avoiding supply chain risk

In 2018 an organisation requested ASD assistance, regarding 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.

Where risk cannot be avoided by re-architecture or policy control, consideration must be made for **another service that carries lower risk**. For example, privileged security enforcing software running on every system is inherently difficult to change the level of impact without at least reducing the scope of deployment to non-critical systems and utilising a more "trusted" product in critical systems.
Risk may be treated or reduced through **additional controls around the service**. Where a high residual risk remains with the current proposed solution, the cost of additional controls must be considered in total cost, and must be realistically maintainable. A vendor may offer transparency, and the ability to audit their security, however if the customer is unable to provide the ongoing resourcing to audit the vendor, it is unsustainable treatment.

A common risk treatment is to ensure monitoring. However, practical implementation must be thought through as to what will actually be detected, and who is doing the monitoring. Your security team or operations centre must be consulted to ensure that monitoring will fit in with existing processes, or at least identify a viable change to process.

In circumstances and national security contexts of unacceptable or undeterminable, significant and widespread impact, exclusion of a specific vendor in certain circumstances may be warranted. If so, you need to:

- Conduct a cost benefit analysis of excluding the vendor. Direct cost may be financial and in the millions but if the system is exposed to high risk, is a nationally critical system and the vulnerabilities are difficult to mitigate, the impact of a realised risk may be much higher.
- In some circumstances pertaining to nationally critical systems, Government guidance may be provided to assist the decision making.
- Ensure compliance with relevant financial legislation and policy. There are vendor exclusion criteria in the security considerations for government procurement policy and arrangements. To support those requirements, this document details a method to determine justifiable national security exclusion, particularly for Government organisations. A sound risk-based decision methodology will avoid unjustifiable vendor exclusion based solely on the fact of foreign ownership.

Step four: Monitor your supply chain and controls

Ensure **records of procurement decisions** around SCRM are recognised and recorded.

Maintain asset lists. What systems are deployed where? If an issue does arise, how will you identify the systems affected? For example, if specific routers are affected, can you locate all of them in your organisation?

Review critical systems through their lifetime. Additional information may become available at a later date about a vendor or product. Although it may be too late for a specific procurement or even architecture, it will inform a realistic and accurate understanding of impact and likelihood that can be communicated to the system owner and stakeholders.

Ensure that security operations centres (SOC) or security teams monitoring systems, know the critical systems, and have the appropriate **capability to monitor those systems** for any cyber security incidents.

Raise awareness. Make ownership of your cyber supply chain security a whole of organisation responsibility.

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. For example, Australian government, critical infrastructure and large business dealing with sensitive systems, must report any cyber security incidents to the ACSC.

Case study 7: 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 investigations 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 information

Cyber supply chain guidance

Further cyber supply chain guidance can be found in the following resources:

- Australian Critical Infrastructure Centre, P***rotecting 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.
- NIST, ***Framework for Improving Critical Infrastructure Cybersecurity*** https://www.nist.gov/cyberframework/framework.
- US NIST, ***SP 800-161 Supply Chain Risk Management Practices*** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

Cyber security guidance

Further cyber security guidance can be found in the following resources:

- The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. 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.
- ***How to Manage Your Security When Engaging a Managed Service Provider*** https://www.cyber.gov.au/acsc/view-all-content/publications/how-manage-your-security-when-engaging-managed-service-provider.
- ***Managed Service Providers: How to Manage Risk to Customer Networks*** https://www.cyber.gov.au/acsc/view-all-content/publications/managed-service-providers-how-manage-risk-customer-networks.

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.

Annex A: Frequently asked questions

My organisation has a new project and has determined there is significant impact to national security if our system is subjected to a supply chain incident. Who in government do I contact to elicit any current critical infrastructure supply chain guidance?

- The first point of contact is to visit the Critical Infrastructure Centre (CIC)[7].

Our vendor says they are compliant with a certain cyber security standard. Does this mean they are not a supply chain threat?

- It is great that the vendor has a commitment to cyber security and can demonstrate they are actively seeking to secure their environment. However, even the most secure organisation can be subject to extrajudicial influence, so consider extrajudicial influence possibilities if your system is nationally critical.

My product has undergone a security or cryptographic evaluation of some kind, such as common criteria. Does that make it ok?

- A cryptographic evaluation is an evaluation of a specific product in order to determine if it meets minimum technical assurance requirements. It is an assessment of a product, not of a vendor's vulnerability to extrajudicial control.

A vendor I trust is supplying a product manufactured in another country, with componentry from a country that may be subject to extrajudicial control in contradiction to Australian law. Does this alter the risk assessment?

- Consider what role that component plays in the overall system, and if that component by design allows enduring criticality to the security of the system. For example, if the component is the encryption chip for all communications, that is very different to the antennae of a wireless system.
- Secondly, consider the ability to influence or tamper with the component going into the specific devices you are using.

How do I asses the security posture of another organisation?

- Practically this can be very difficult. However, at a minimum you should have your cyber security subject matter expert ask some direct questions about how that organisation manages their cyber security.

What indicators of compromise should I look for, to see if a supply chain risk has been realised?

- Capturing logs and auditing for a supply chain compromise will require understanding the most likely threats and vulnerabilities. For example, if unauthorised remote access is considered an enduring risk by a vendor that maintains the system, ensure the access is fully logged and that those logs are monitored by a security operations centre.

Where can I get information on trusted forums I can participate in?

- Different (cyber security) forums exist for specific sectors. Participation in these forums is useful for frank sharing of experience, a broader understanding of the threat environment and specific supply chain experiences. More information can likely be found through the ACSC Joint Cyber Security Centres[8].

[7] https://cicentre.gov.au/
[8] https://www.cyber.gov.au/acsc/view-all-content/programs/joint-cyber-security-centres

Annex B: 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	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.
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 cyber 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.
Vendor	A vendor is typically the organisation that supplies a product or service to the customer.
Vulnerability	A cyber vulnerability is a weakness in a system that can be exploited by a threat, ultimately compromising the security of the system.

Annex C: Worked case studies

These scenarios work through common situations observed by ASD-ACSC. Each scenario will follow the outlined SCRM process; examine the situation/scenario, impact assessment, vulnerabilities, threats, treatment of risk, and monitor.

Case 1: Open source software components

Situation

A government organisation is building a web platform to manage interactions with their customers, the Australian public. The preferred option is to use a public open source technology to deliver a large part of the solution. The supply chain risk of the open source software will be considered.

Assessment

- Step one – understand and determine value of data and system.
- The open source product manages the front end interactions, data processing, storage and application programming interfaces (API's). The platform has a plugin architecture that allows extension of the platform.
- The system will handle data that is not nationally classified, however it will contain up to millions of records of personally identifiable information (PII) about Australian citizens.
- The original architecture stores the data in the PROTECTED area of the corporate network because of its overall amount of PII stored. Therefore this system is interconnected to the PROTECTED network.
- Overall there is high value in the data held and interconnectivity of the system. The system is considered sensitive.

Step two – what are the specific supply chain risks?

- Vendor There is no specific vendor for the proposed open source technology. It appears to be primarily coordinated by a collection of individuals and companies from around the world, primarily European.
    - Dependencies - The project utilises other open source projects – so there are sub-dependencies to consider. Given the plugin architecture – there is likelihood of separate plugins being developed and managed outside the main project.
    - Security posture - The platform is known publically to have software vulnerabilities that have been actively exploited in the past. These vulnerabilities have given full remote code execution to unauthorised parties.
- Any actor, state or criminal, could have significant influence over the software source code, sub dependencies, or plugins now and ongoing. This influence could modify any aspect of the code.
- There is no immediate known intent to target his data set. However, criminal and state groups are known to target large PII data sets.
- There is overall high risk from the products supply chain.

Step three – manage the risk.

- With the high supply chain risk and the large store of personal data held by Government, even though there is no immediate indication of intent to target the data, any breach would be nationally concerning.
- Risk options include:
    - Reduce the risk by employing a team of software engineers to provide a software security code review of all source code, dependencies, and plugins, now and for any future changes.

- Reduce the risk by adding a wrapper in front of the software, so that all communications are validated before they are passed to the software, and only necessary functions of the software are exposed.
- Reduce risk to the corporate environment of running the software by hosting it independently of the corporate network.
- Avoid the risk by investigating a different software solution.

Step five – review, monitor, report.

- The solution must log activity and be reviewed for any evidence of abuse.
- If a code audit process is established, the efficacy of the process must be reviewed.

Outcome

This is a complex and common scenario. It is easy to assume that because a product is open source, that it has more source code review than a closed source product. Recent publically known major vulnerabilities in open source software have proved this assumption incorrect.

Open Source products form a valuable part of the IT ecosystem, but be aware they do carry their own supply chain risk.

Case 2: The cellular network dongle

Situation

A critical infrastructure provider would like to provide remote working staff and contractors with a 4G dongle to connect remotely to the corporate and operations networks.

The best value for money dongle is made and supported by a foreign country which has been publically exposed as responsible for nation state level compromises of critical infrastructure.

Operation of the dongle requires installation of custom drivers and utility software from the vendor.

Assessment

Step one – determine value of data and system.

- The dongle itself is intended to provide a gateway to the internet. It does require software to be installed in order to function, and that software would be installed on a corporately issued device that connects by VPN over the internet as a trusted device on the network.
- The system it will be installed on will have full access to operational or corporate environments of the critical infrastructure provider whilst connected to the internet.
- The overall corporate and operational system would be considered nationally critical.

Step two – what are the specific supply chain risks.

- Vendor nationality – the vendor is headquartered in a country that is likely to have extrajudicial control over the vendor. The vendor supplier the hardware, software, and ongoing software updates for the dongle. The vendor could be considered 'high risk'.
- The dongles driver and/or application software could be modified to allow unauthorised access to the laptop.
- There has been specific public evidence that the vendor's country has targeted specific critical infrastructure in other countries.
- Overall the solution presents a high supply chain risk to the system if there are no mitigating and complimentary controls.

Step three – manage the risk.

- Avoid the risk – use a dongle, it could be from the same manufacturer that provides a Wi-Fi hotspot that the laptop can connect to. Using an alternative architecture, direct exploitation risk by the device software is avoided. Use of appropriate cryptographic protocols on the VP will mitigate traffic interception risk.

Step four – review, monitor, report.

- Ensure the remote access devices are monitored for any anomalous logins.
- Record the decision and reasons corporately.

Outcome

More complex measures in this case are not warranted where the cost to avoid the risk is low. It should be realised that any solution that deploys additional software on a device adds risk, so this mitigation could apply to any brand dongle.

Case 3: The national infrastructure project

Situation

A major Australian city is establishing autonomous car infrastructure. This requires the use of a wireless command and control network.

One tender response is from a country publically reported to have active state sponsored cyber hacking campaigns against Australia. The tender is significantly cheaper than the next closest tender from a vendor headquartered in another country.

Assessment

Step one – determine value of data and system.

- The overall system would be considered nationally critical infrastructure, and there is some threat to life if the system does not fail gracefully. In a time of war the system will provide valuable support to logistics, and may be a target.
    - The wireless system itself.
    - Could be used to view, modify, deny or degrade the command and control environment.
    - Will not handle nationally classified or PII data.
    - Is not connected to other classified or sensitive systems other than the operational network that runs the autonomous infrastructure.
    - Has is some capacity to transmit messages to users in cars.

Step two – what are the specific supply chain risks.

- Vendor – given they are headquartered in a country that is actively hacking Australia, there is at minimum extrajudicial influence risk and possible extrajudicial control risk.
    - The equipment manufacture and assembly is opaque to the purchaser. It is possible devices with malicious function are wittingly supplied to the project.
    - The vendor requires ongoing access to the equipment in order to support it. They proposed this occur over an encrypted internet connection.
    - Dependencies - the vendor utilises open source software in the specific hardware quoted. It is not clear if sub-contractors are utilised for the ongoing service of the equipment.
    - Cyber security posture – the organisation has a public demonstration of commitment to cyber security and cites secure development standards in use in the organisation.
- Threats - there is no known state intent to interfere with the autonomous vehicle capability.

Step three – manage the risk.

- Reduce the risk of the ongoing remote access. Further investigate how the remote access is implemented, and determine if any complimentary security controls can be implemented to provide the organisation with ultimate control over the remote access.
- Reduce the risk of supply tampering by purchasing through a third party. Realistically this will be non-trivial for a large infrastructure project.

- Avoid the risk - look to another vendor but realise that similar vulnerabilities and threats exist. With a different vendor you will look for demonstration of commitment to cyber-security, and likewise mitigate the remote access service risk.

Step four – review, monitor, report.

- Ensure that all remote access is reviewed on an ongoing basis for legitimate need to access. All actions taken during remote access should be logged.

Outcome

This scenario is not uncommon across infrastructure projects. Be aware that as complexity of the system increases, the opportunity for targeted access to the system increases, which comes not primarily from a vendor whose state is known to target Australia, but from the security interdependencies of the whole system. For example, with this infrastructure project, there may be greater vulnerability if the operational system is connected to a management network that is connected to a poorly secured internet-connected corporate network.