Choosing secure and verifiable technologies: executive guidance

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
PART OF THE GCSB

Introduction

The security of an organisation's supply chain for the digital products and services they operate is paramount in a growing threat environment. Applying secure-by-design practices and principles to the procurement of digital products and services will assist organisations in continuing to build their supply chain maturity.

When security is seamlessly integrated into the procurement process, it can enhance efficiency, customer trust and ultimately the success and reputation of the organisation. Strong senior leadership is essential to building robust security cultures within organisations to increase supply chain maturity and cyber resilience.

This paper provides a summary of the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) led co-sealed guidance Choosing Secure and Verifiable Technologies, alongside an understanding of the threat environment that requires a greater focus on these issues. The publication provides summarised guidance on procuring secure digital products following secure-by-design practices and principles, and outlining the responsibilities and actions necessary to support execution of the advice.

The ASD's ACSC and the following international partners provide the recommendations in this guide:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- New Zealand's National Cyber Security Centre (NCSC-NZ)
- Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Centre (NCSC)

Audience

This paper is written for **organisational senior leaders** who procure and leverage digital products and services and for **senior leaders of manufacturing organisations** that develop digital products and services. This publications provides information to support better-informed assessments, decision making and the increased development of secure technologies.

This document assumes a moderate level of computing and cyber security knowledge on the part of the reader.

Objectives

ASD's ACSC developed this guide to assist senior leaders in understanding the threat environment contributing to the need to be diligent when procuring digital products and services. This guide will also highlight the areas in pre-and post-purchase procurement that senior leaders must consider.

By following the guidance in the Choosing Secure and Verifiable Technologies publication and by having the support of senior leaders, organisations will benefit from the following:

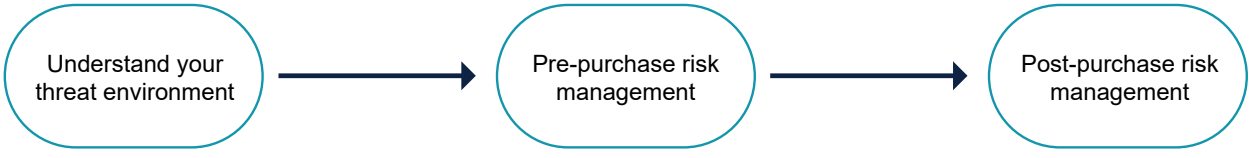
- procuring technologies with fewer or no vulnerabilities
- lowering costs through products requiring less maintenance, administration and reduced incident costs
- reducing organisational risk, both likelihood and impact, through more resilient and secure technologies
- increasing the organisation's reputation with its end users or customers.

Understanding the risk of technology procurement

Cyber attacks continue with increasing frequency worldwide, presenting significant challenges for organisations to defend their information environments from persistent and capable threat actors. The procurement of any digital product or service increases the attack surface of an organisation's information environment. It is critical to **understand the threat environment** and the possible supply chain attack vectors so organisations can identify and manage the risks through **pre-purchase and post-purchase risk management**.

Visibility of the risks associated with a chosen digital product or service is needed to ensure any identified risks do not exceed the organisation's risk tolerances. If a digital product or service does exceed the organisation's risk tolerance, the appropriate risk treatment option should be enacted (i.e. accept, transfer, avoid or mitigate).

This paper outlines 3 steps for choosing secure and verifiable technologies, including the responsibilities and actions in each.



Understand your threat environment

Knowing the current and emerging threat environment when procuring digital products and services informs decision making to appropriately manage the risks that an organisation faces. There are many opportunities for malicious actors to compromise digital products or services through the supply chain. Understanding the ways in which malicious actors can compromise digital products or services, empowers organisations to demand that technology manufacturers provide evidence of mitigations against potential threats.

Organisations can stay informed by following these advisories and alert services:

- https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories
- https://www.cisa.gov/news-events/cybersecurity-advisories

When procuring digital products and services, supply chain risks are not just that of the supplier but that of the supplier's supply chain. All technology manufacturers will have their own suppliers who in turn have their own suppliers, all of whom are susceptible to the same risks as the technology manufacturer supplying to the end technology consumer. Compromise at any of these points in the supply chain can result in the compromise of the end consumer.

The diagram below details the points in the digital product or service procurement supply chain at which a malicious actor may attempt to cause compromise. The diagram simplifies the supply chain down to a single use open-source software (OSS) source and a single third-party technology supplier. In nearly all situations the supply chain will have many OSS sources and proprietary technology providers in their full supply chain. However, the points of attack will be the same between each of the additional links within the supply chain.

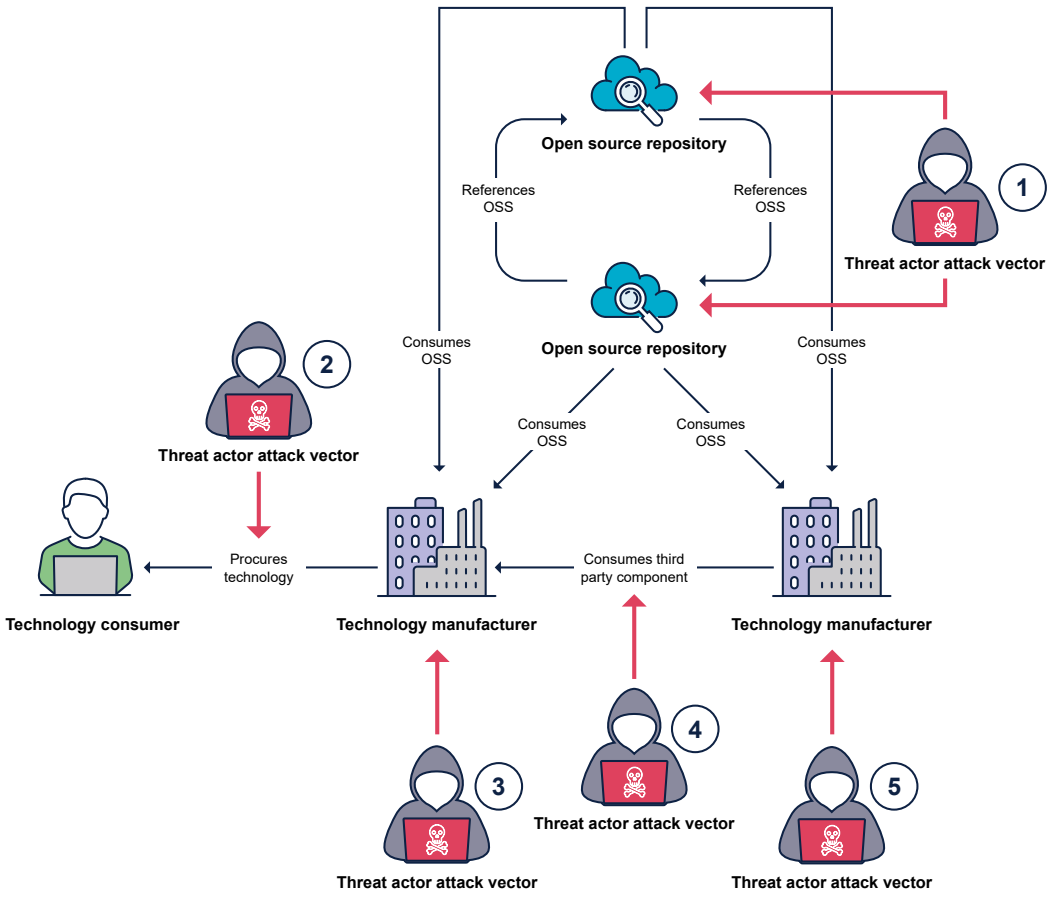


Figure 1. Digital Supply Chain Threat Environment

Malicious actors may attempt to compromise an end consumer using multiple tactics and at multiple points in the supply chain. The below table outlines some of the possible malicious actions per attack vector.

Table 1: Possible malicious actions per attack vector

Threat actor attack vector	Possible malicious action or attack
1	Malicious code injection into legitimate open-source software packages.
	Development of malicious open-source software package disguised as legitimate packages.
	Misconfiguration or vulnerabilities added by legitimate contributors by mistake to open-source software packages.
	A known class of vulnerability is embedded within the product or service.
2	Delivery of a malicious or vulnerable product or service.
	Delivery of a malicious or vulnerable patch.
	A malicious actor intercepts the transfer process and manipulates the provided content.
3	A trusted insider makes a malicious change to the product or service to be delivered to a technology consumer.
	A known class of vulnerability is embedded within the product or service.
4	Delivery of a malicious or vulnerable product or service.
	Delivery of a malicious or vulnerable patch.
	Delivery of a malicious or vulnerable package or source code.
	A malicious actor intercepts the transfer process and manipulates content for a malicious purpose.
5	A trusted insider makes a malicious change to the product or service being delivered to a supplying technology manufacturer.
	A known class of vulnerability is embedded within the product or service.

Pre-purchase risk management

Procuring organisations can assess the risks of a technology manufacturer and their product or service offering following a two-staged approach: **pre-purchase** and **post-purchase**. Understanding the cyber risks associated with procuring technology will assist in empowering organisational personnel to perform both pre-purchase and post-purchase activities. Following these activities will ensure benefits are realised and maintained throughout the life cycle of the product or service.

The pre-purchase assessment phase is about completing low-cost checks and due diligence before committing to a more extensive evaluations process. It is important for the purchaser to consider the potential consequences of purchasing a product that is not secure and verifiable and which may be outside their organisation's risk tolerance. Key consequences that should be considered include:

- costs and revenue
- reputation
- long-term profitability
- consequential losses.

During the pre-purchase procurement process, the guidance proffered in Choosing Secure and Verifiable Technologies guidance outlines the following areas an organisation should assess about a technology manufacturer and their product before proceeding with a procurement.

- Transparency and reporting
- Secure-by-Default
- Security requirements
- Supply chain risk management
- Open-source software usage
- Data sharing and sovereignty
- Development process
- Geopolitical risks
- Regulated industries
- Manufacturer access
- Insider threat
- Open standards
- Connected systems
- Product value

To assist in achieving the outcomes of the above assessment areas, senior leaders must support their organisation by:

- supporting an organisational shift towards following secure-by-design practices
- allocating resources to support the procurement process with the right skills and tools to assess each of the above areas
- reviewing the proposed product's risks and ensuring they do not exceed the organisation's risk threshold
- remaining informed of new and residual risks, to ensure they are being managed at the correct level
- ensuring the contract meets the organisations security requirements.

Post-purchase risk management

Following the purchase of a product or service, the procuring organisation needs to ensure that their purchase continues to meet the security requirements of their organisation. This requires continuing support and risk management of a product or service throughout its lifecycle.

During the post-purchase procurement process, the guidance proffered in Choosing Secure and Verifiable Technologies guidance outlines the following areas an organisation will need to address to ensure a product or service remains secure.

- Risk management
- Security incident and event management, and security orchestration automation and response
- Maintenance and support
- Contracts, licencing and service level agreements
- Loosening guides
- End of life

To assist in achieving the outcomes of the above areas senior leaders must support their organisation by:

- Providing ongoing organisation support and commitment to secure-by-design practices.
- Providing an authority to operate.
- Being part of the continual risk management process ensuring risks stay within organisational risk tolerances.
- Allocating resources to support the product throughout its lifecycle.
- Reviewing and endorsing supporting security documentation for the proposed procurement, including incident response plans, business continuity plans and disaster recovery plans.

Appendix

Secure-by-Design

Secure-by-design is a proactive, security-focused approach taken by software manufacturers during the development of digital products and services. This requires the purposeful alignment of cyber security goals across all levels of the manufacturing organisation. Secure-by-design requires that manufacturers consider cyber threats from the outset to enable mitigations through thoughtful design, development, architecture, and security measures. Its core value is to protect user privacy and data through designing, building and delivering digital products and services with fewer vulnerabilities.

By investing in secure digital products and services, organisations can reduce operating costs, enhancing organisational reputation and profitability, to deliver long-term, sustainable corporate value and cyber resilience.

Supporting resources

Choosing secure and verifiable technologies

Choosing Secure and Verifiable Technologies is a co-sealed publication led by ASD's ACSC. It provides organisations advice and guidance on procuring digital products and services following secure-by-design practices and principles. For more information, please visit Choosing Secure and Verifiable Technologies | Cyber.gov.au.

Secure-by-Design Foundations

ASD's ACSC Secure-by-Design Foundations (the Foundations) have been designed for both technology manufacturers and consumers, to assist in the adoption of secure-by-design. Each Foundation identifies key areas of focus and associated mitigated risks. For more information, please visit Secure-by-Design Foundations | Cyber.gov.au.

IoT Secure-by-Design Guidance for Manufacturers

The ASD's ACSC *IoT Secure-by-Design Guidance for Manufacturers* has been developed to help manufacturers implement 13 secure-by-design principles from the *AS ETSI EN 303 645* cyber security standard for consumer IoT devices. For more information, please visit IoT Secure-by-Design Guidance for Manufacturers | Cyber.gov.au.

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default

The *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default* whitepaper is a co-sealed publication led by the Cybersecurity and Infrastructure Security Agency (CISA). It provides technology manufacturers advice on developing products with secure-by-design and secure-by-default strategies. It is underpinned by three founding principles for technology manufacturing leaders: take ownership of customer security outcomes; embrace radical transparency and accountability; and lead from the top. For more information, please visit Shifting the Balance of Cybersecurity Risk | Cyber.gov.au.

Minimum Viable Secure Product

Minimum Viable Secure Product is a list of essential application security controls that should be implemented in enterprise-ready products and services. The controls are designed to be simple to implement and provide a good foundation for building secure and resilient systems and services. For more information, please visit Minimum Viable Secure Product | Mvsp.dev.