Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# Dealing with risks in the supply chain

## Good practices in Dutch organisations

Publication date: 15 August 2023 (Dutch version), 12 September 2023 (English translation)

**Authorised distribution:**
TLP:CLEAR (Traffic Light Protocol)

This publication bears the label TLP:CLEAR and is distributed by the NCSC. The NCSC uses the Traffic Light Protocol (TLP) to define clearly and unambiguously what may be done with the information it provides. If information has a TLP designation, you will know with whom the information can be shared. This is described on the NCSC's website (https://www.ncsc.nl/onderwerpen/traffic-light-protocol)

TLP:CLEAR indicates that there are no restrictions on sharing the information more widely.

Your input is welcome at info@ncsc.nl.

# Contents

# Introduction

Monitoring and controlling cybersecurity risks in the supply chain can be described as challenging at the very least. How does one do it? Products and services are brought into the Netherlands from all over the world, after all. Such an international network comes with opportunities as well as risks.

The NCSC recently opened a dialogue with Dutch public and private organisations on the following question: 'How do you deal with cybersecurity risks from your supply chain?' This document offers concrete starting points to answer that question.

### Different perspectives and the definition used

On 11 April 2023, the NCSC conducted a workshop with representatives of public and private organisations to share good practices[1] for handling risks in the supply chain.

The supply chain can be viewed from different perspectives. Research institute TNO has mapped these various perspectives on behalf of the NCSC.[2]

In the workshop, we used the following definition*:* 'The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services.'[3]

### Lessons from Log4j

Supply chains are technically complex and it is difficult to keep a grip on dependencies. This was found when a serious vulnerability was detected in Log4j.

Log4j proved to be the digital equivalent of salt; an exceptionally large number of applications was found to contain Log4j components.[4] Cybercriminals and state actors were then quick to exploit vulnerabilities in Log4j.[5]

### Geopolitical developments

Geopolitical developments, too, may give rise to new risks in the supply chains of Dutch organisations.

An international conflict, for instance, may have an impact on supply chain security. Products may not be available due to sanctions or export restrictions, and international supply chains may be targeted by politically motivated digital attacks.[6]

## Target audience

This document is intended for CIOs, CISOs and risk managers that want to gain insight into and get a grip on risks in the supply chain.

## Background

This document was created in the course of a workshop with the chairpersons and vice-chairpersons of the ISACs[7] in which the NCSC takes part.

In this workshop, the participants shared good practices on dealing with risks in the supply chain. The NCSC enriched the outcomes and incorporated them into this publication.

# Overview

It is difficult to get a grip on your supply chain without adequate insight and understanding. This chapter discusses best practices that can help your organisation gain a thorough understanding of your suppliers and in what ways your organisation depends on them.

## GP[8] 1.1: Make sure there is an up-to-date list of your assets[9]

Insight into your supply chain begins with an up-to-date list of your assets. It is important to have a thorough understanding of your organisation's crown jewels. Crown jewels are the information and information systems that are absolutely vital to an organisation.[10]

- Your ICT department maintains an asset list. You may already have identified your crown jewels in your risk management process or business continuity plan. Use this existing information to identify the most important assets in your organisation. How are your crown jewels and assets interconnected?
- If the availability, integrity and confidentiality of important assets and crown jewels are compromised, the interests of the affected organisation may be threatened. Mapping these organisational interests that need to be protected and how they are connected to your assets creates a good starting point for risk management.
- You can also use Software Bills of Materials (SBOMs) in an asset list. An SBOM describes the components of which a piece of software consists and the relationships between these components.[11] SBOMs allow you to gain insight into the software that your organisation uses and the origin of the various software components.
- Also include shadow IT*[12]* in your list. Shadow IT generally remains under the radar and may have severe consequences for your organisation, as you do not have insight into these products and services but they enlarge your attack surface. There are technical options, such as conducting a scan, to identify present shadow IT in your organisation.

## GP 1.2: Compile a list of suppliers

In your organisation, the various departments have to deal with part of your suppliers. Checking these departments on a regular basis allows you to create an up-to-date total supplier list.

- Departments in the primary process, as well as support departments such as ICT or marketing & communications or staff departments, all use suppliers. Every department may have different suppliers.
- The accounts payable overview of your procurement department can be an important source of information. It can be compared against a mapped overview from your ICT department to check that it is comprehensive. For instance, you may run into ongoing service contracts for specific software that cannot be found anywhere else.

## GP 1.3: Classify and prioritise your suppliers

Suppliers may offer services, goods (such as hardware), or software. In order for you to focus on the principal suppliers, it is important to classify and prioritise your suppliers. You can do this from different perspectives:

- Which suppliers are associated with your crown jewels? Some suppliers are of immediate importance to the undisturbed operation of your primary and/or critical business processes. You can pinpoint them by looking at supplier dependencies from the perspective of your crown jewels.
- Which suppliers have access to confidential systems and/or data? Some suppliers provide a non-critical service to your organisation but do have access to confidential systems and/or data.

  An example is suppliers processing the personal information of your employees, customers or relations for marketing & communication purposes. Sometimes, a supplier has direct access to a dataset or information system of your organisation.
- What suppliers are you worried about because of their bad reputation? These suppliers may require extra attention because your organisation or partners have had bad experiences with them. When a supplier is involved in an information security incident, such as a leak, this may also cause you to have another look at this supplier.
- Several methods, such as the Kraljic Matrix, are valuable in mapping and prioritising risks in the supply chain.[13]

## GP 1.4: Know and understand your principal suppliers

A safe supply chain starts with knowing your principal suppliers. Invest in a good relationship with your principal suppliers. This will create an adequate basis to talk about cybersecurity and the way in which the supplier handles their own supply chain. This yields an overview of the cyber maturity of a supplier and provides insight into critical dependencies on subcontractors that are important to your organisation.

There are several methods to assess the cybersecurity status of your suppliers:

- Dialogue: Facilitate a dialogue between the security experts of the organisations involved. Asking the right questions will allow you to gain insight into a supplier's cyber maturity.[14]
- Exchanging experiences: Where possible, exchange experiences with industry partners to gain more insight into the resilience of (industry-specific) suppliers.
- Cybersecurity ratings: Use the range of frameworks and models that aim to profile the cybersecurity rating of organisations. In practice, these use commercial rating agencies (e.g. for ISO 27001 and 28000 ratings).
- Frameworks such as CYRA may also present a solution.[15] An instrument such as CYRA is an easily accessible tool for organisations in all industries to map cyber resilience. CYRA also uses a self-assessment and/or certification to provide insight into an organisation's level of cyber resilience.

# Geopolitics

How do geopolitical developments impact your supply chain? This chapter discusses risks arising from geopolitical developments in greater detail.

## GP 2.1: Map the risks arising from geopolitical developments

Global events may have an impact on your supply chain. Risks arising from such events may be of a geopolitical, economic, sociological, technological or ecological nature.[16]

Where do the products and services on which you depend come from? And via what logistical lines do they reach you?

- Include sabotage and espionage-related risks in your periodical risk analysis, too. In 2023, for instance, the Dutch government decreed that all applications originating in countries with an offensive cyberprogramme targeting Dutch interests would be discouraged on mobile work devices. This decision was made on the basis of a risk assessment.[17]

- Rising geopolitical tension may have an impact on insider risks[18], which refers to threats from employees of your suppliers that may also do work for you.[19]

## GP 2.2: Map potential targets from the attacker's perspective

Insight into your threat landscape and attack surface are vital in order to assess whether your organisation and supply chain are of interest to state actors. Suppliers can be used as intermediary to access your systems or those of other customers. Such an analysis is even more interesting if you depend on services and/or products from a country with an offensive cyberprogramme that affects the interests of the Netherlands.[20]

- For this analysis, it may make sense to take the perspective of an attacker and determine, from this angle, what information and processes may present interesting targets.

- Include your suppliers in this threat landscape and attack surface. In many cases, suppliers are exploited as an intermediary to gain access to your information and processes. If your confidential information is stored in a supplier's systems, attackers do not need to gain direct access to your systems to breach the confidentiality of your information.

- Avoid tunnel vision by involving external experts in performing a threat analysis. This will help you make sure you do not overlook any important threats.[21]

# Resilience

After you have mapped risks in the supply chain, you can implement measures to mitigate identified risks. This chapter discusses available measures and how they relate to the risks you have identified.

## GP 3.1: Digital resilience starts with yourself

If your supply chain is compromised, this may have a direct effect on your own organisation. Make sure to implement a number of measures to ensure that the risks to your organisation are limited if an organisation in your supply chain is compromised.

### GP 3.1.1: Perform a periodical risk analysis

Make sure that your organisation is widely committed to the risk analysis, perhaps as part of an annual risk management cycle. Include risks relating to (logistical) processes, support services, persons (e.g. hired, maintenance crew, employees), and products (e.g. hardware and software).

- Make sure that it is clear how the procured service or devices are linked to the rest of your network. Determine the risks involved and mitigate them by implementing appropriate measures, for instance based on the basic cybersecurity measures[22].

### GP 3.1.2: Ensure that your employees are aware of third-party risks

Not everyone in your organisation can be an expert in the field of cybersecurity. Procurement officers are not always aware of the cybersecurity requirements you wish to implement for suppliers.

- Include your procurement department in the various cybersecurity measures for suppliers and cybersecurity standards.
- Sometimes employees create their own networks or systems without you being able to exert centralised control (Shadow IT).[23] Ensure that employees are aware of the risks associated with the use of third-party services and devices in order to avoid such situations where possible.

### GP 3.1.3: Run through a worst-case scenario

The worst-case scenario is your supplier being the victim of a serious cybersecurity incident that has a high impact on your organisation's operations.

- A table-top exercise allows you to run through a scenario in which an important supplier is hit by a cybersecurity incident.[24] This can help you prepare for a worst-case scenario.

## GP 3.2: Adequate arrangements with suppliers prevent trouble

Even when you have an excellent cybersecurity basis, you will want additional guarantees that your suppliers comply with your expectations where it concerns resilience. Knowing how your supplier handles cybersecurity and reaching an agreement on this subject means that you will know the extent to which you really are on top of risks.

If you want to work with a supplier, it is wise to reach an agreement on this and put it on paper, for instance about conducting (announced or unannounced) security audits or security tests, or reporting and solving security incidents. Use a Service Level Agreement (SLA) and ensure that these arrangements can be enforced contractually.

- Know what you are asking and what you are allowed to ask. Is service availability most important to you instead of, for instance, data confidentiality? To what extent are matters such as digital independence vital to your organisation? And are you asking for a custom package (where you can impose additional requirements) or a standard service and agreement? Be critical of your own organisation on these points as well and consider whether your organisation has adequately organised its own resilience in this regard.

- Finally, make sure that aligning wishes in the field of security is implemented as a standard part of your own procurement procedure and that procurement officers can find the right information and/or expertise to enter into a suitable agreement.

## GP 3.3: Exchange of knowledge and experiences

Cybersecurity risks are generally not exclusive to individual organisations. Sometimes, collaborating with 'competitors' in an industry or chain partnership can be valuable to exchange knowledge and expertise.

### GP 3.3.1: Know how to find each other and build trust

Trust is the main prerequisite for stakeholders to share knowledge with each other. Make sure that people know each other and know how to find each other. An ISAC is an example of a place where people meet and can learn to trust each other because the same people come together every time, so they can get to know and trust each other.[25]

- Make sure that information can be shared easily and confidentially. An ISAC is a form of collaboration in which information can be shared confidentially and periodically. A platform or portal where information/files can also be shared confidentially in electronic format, can contribute to this, for instance to ensure that not everything has to be done by e-mail.
- It is not always easy to build trust. In 2020, the NCSC asked The Hague University of Applied Sciences to map success factors for cybersecurity information sharing between organisations.[26] This document offers more information on how to collaborate with other organisations in your industry or chain.

### GP 3.3.2: Offer tips on supplier lists, procurement requirements, and security standards

Gain insight into each other's procurement and contracting policies. Share knowledge on the requirements and what components have been tested. This can serve to make the entire chain stronger. Learning from others enhances one's own procurement and contracting policies.

- You can offer each other access to supplier lists for specific products, for instance. If the same products must be sourced, it is practical to know what suppliers have already been approved by others. This may accelerate the process.

### GP 3.3.3: Jointly influencing international suppliers

It may be difficult to influence international suppliers. By collaborating in procurement processes, you can develop a joint list of wishes and requirements.

- For instance, you can ask for transparency with regard to the products you want to source. A group can exert more pressure on suppliers to comply with quality requirements. Test these quality requirements on a regular basis.

## GP 3.4: Prepare an exit plan

You may wish to part ways with a supplier after you develop concerns about the security of your supply chain. A step-by-step plan that you can follow will help, especially if it also features the required legal steps. This allows you to part ways with a supplier before being subjected to unnecessary risks.

It will help if you have reached a clear agreement with the supplier at an earlier stage (cf. GP 3.2), because you will be able to refer to the contract in case of non-compliance.

- Determine your threshold values to pursue the exit strategy legally and terminate a contract. Seek legal assistance in wrapping up an agreement whilst keeping the continuity of your day-to-day (business) processes in mind. The organisation must continue to operate correctly when you switch suppliers. Another thing to consider is transfer of knowledge and information in case of a personnel change.
- Create an exit plan before entering into a contract: this will help avoid becoming overly dependent on one specific supplier.
- Do not give away data or intellectual property. If you implement the exit plan, you must also safeguard the information the supplier has about your organisation. They must return that information to you. The information must also be handed over to a new party and includes intellectual property rights, administration rights, logs, source code, software licences, and the availability of relevant data.

## GP 3.5: Consider geopolitical risks in your procurement strategy

### GP 3.5.1: Ensure that you establish well-considered procurement and contracting policies

Draw up a well-considered contracting policy and/or establish a procurement strategy for the organisation, taking account of geopolitical risks such as geopolitical tensions and digital espionage, and share it within the organisation.

- The lowest-cost product or service is not always the best choice for your organisation. Test the safety and quality of products and review any related documentation before proceeding to a purchase decision.

### GP 3.5.2: Avoid becoming too dependent on specific suppliers

Make sure that your organisation does not become dependent on any specific supplier or vendor, especially if such suppliers are located in an area that may be affected by political tensions and resulting instability. This may lead to supply issues.

- Know what other suppliers operate in your market and where they are based. Also consider what parent companies or stockholders are involved. Here, too, geopolitical developments and sanctions may have a serious impact on your supply chain.

# Want to know more?

SBOM Startersgids [SBOM starter guide]

TNO published the SBOM starter guide in collaboration with the NCSC in 2023. The two partners looked at how organisations can set up Software Bills of Materials (SBOMs) processing.

*Starter guide: Software Bill of Materials: Hoe, wat en waarom* [Starter guide Software Bill of Materials: How, what and why], TNO & NCSC, June 2023

*Good Practices for Supply Chain Cybersecurity*, ENISA

In June 2023, ENISA mapped good practices for supply chain cybersecurity from the perspective of European organisations, surveying 1,081 organisations from the 27 EU member states.

*Good Practices for Supply Chain Cybersecurity*, ENISA, June 2023

*Supply chain security guidance*, NCSC-UK

NCSC-UK has mapped 12 principles to enable businesses to get on top and in control of their supply chain.

*Supply chain security guidance*, NCSC-UK, visited on 5 July 2023

Threat Assessment State-sponsored Actors (TASA), AIVD, MIVD and NCTV

Some countries run an offensive cyberprogramme targeting Dutch national security interests, including China, Russia, Iran, and North Korea. The AIVD, MIVD and NCTV discuss this threat in greater detail in the Threat Assessment State-sponsored Actors (TASA). This document provides insight into any risks you may incur when having dependencies in these countries.

Report: *Threat Assessment State-sponsored Actors 2*, AIVD, MIVD and NCTV, November 2022

Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning, TNO

In 2021, TNO published a document on supply chain management in the digital domain on behalf of the NCSC, taking a deep dive into supply chain risk management (SCRM) and several perspectives on this topic.

Report: *Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning* [Issues and perspectives for ICT SCRM – an initial exploration], TNO, April 2021

*Using the Software Bill of Materials for Enhancing Cybersecurity*, Capgemini

In 2021, Capgemini was commissioned by the NCSC to publish a document on SBOM and how it can be leveraged to improve cybersecurity.

Publication: *Using the Software Bill of Materials for Enhancing Cybersecurity*, Capgemini, February 2021

*5 adviezen voor veilige inkoop van clouddiensten*, NCSC

Many organisations are either considering or in the process of purchasing cloud services. Cloud services can serve as a major functional supplement for organisations, although this does require balanced measures to be taken during their purchase. In this document, the NCSC takes a closer look at how organisations can source cloud services with greater security.

Factsheet: *5 adviezen voor veilige inkoop van clouddiensten* [5 recommendations for sourcing cloud services in a secure manner], NCSC, October 2020

### *Start een ketensamenwerking*, NCSC

In 2018, the NCSC published a guide on starting a chain partnership. The NCSC discusses in detail how organisations can collaborate in a chain and jointly detect and mitigate risks.

Guide: *Start een ketensamenwerking* [Starting a chain partnership], NCSC, November 2018

### *Ketenweerbaarheid tegen cyberdreigingen*, TNO

In 2017, TNO published a whitepaper with background information, good practices and a step-by-step plan to enhance cyber resilience in a chain.

Whitepaper: *Ketenweerbaarheid tegen cyberdreigingen* [Chain resilience in the face of cyberthreats], TNO, February 2017

### CYRA

Cyber Weerbaarheidscentrum Brainport, FERM Rotterdam, MKB Cyber Campus and TŰV NORD Nederland have established CYRA. CYRA stands for CYberRAting and is a method to provide smaller businesses with a perspective and starting points in realising digital resilience. CYRA also contributes to transparency of chain partners.

Website: *Jouw  route naar digitaal weerbaar ondernemen* [Your itinerary to digitally resilient business], CYRA Cyber Rating, visited on 10 August 2023

# References

[1] Good practices in this document are operating methods, habits and practices that have been shown in actual practice to be effective in tackling an issue.

[2] *Issues and Perspectives for ICT SCRM – An Initial Exploration*, TNO, February 2021

[3] This definition of *supply chain risk* is the one used by the NIST, see *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5, September 2020

[4] Which was demonstrated by the Github overview of vulnerable applications with Log4j components. The NCSC updated this overview with national and international partners.

*Log4j*, NCSC, visited on 28 June 2023

[5] *Log4Shell Initial Exploitation and Mitigation Recommendations*, Mandiant, 15 December 2021

[6] *Vier cybersecuritylessen uit een jaar oorlog in Oekraïne* [Four cybersecurity lessons from a year of war in Ukraine], NCSC, DTC and CSIRT-DSP, February 2023

[7] ISAC is the acronym for Information Sharing and Analysis Centre, a consultation body focusing on cybersecurity in which organisations from a single industry exchange sensitive and confidential information about incidents, threats, vulnerabilities and mitigation measures.

*Samenwerking in een ISAC* [Collaboration in an ISAC], NCSC, visited on 8 August 2023

[8] In this document, we have marked the best practices identified by participants with 'GP'.

[9] In terms of cybersecurity, assets are information or digital systems that are of value to an organisation, such as intellectual property, customer database, personnel information, etc. Unless stated otherwise, these and other definitions have been taken from the *Cybersecurity Woordenboek* (Cybersecurity dictionary).

*Cybersecurity Woordenboek 2021*, Cyberveilig Nederland, December 2021

[10]Crown jewels are the information and information systems that are absolutely vital to an organisation. Not being able to access this information will have dramatic consequences for the organisation. This is also true if the information is no longer correct or is unwittingly divulged to others.

[11] *Startersgids Software Bill of Materials: Hoe, wat en waarom* [Starter guide Software Bill of Materials: How, what and why], TNO & NCSC, June 2023

[12] Shadow IT is hardware or software in an organisation that is not supported and configured by the IT department but does play a part in your business operations.

[13] *What is the Kraljic Matrix?*, Forbes, 28 February 2017

[14]

[15] *Jouw route naar digitaal weerbaar ondernemen* [Your itinerary to digitally resilient business], CYRA Cyber Rating, visited on 23 June 2023

[16] *The Global Risks Report 2023*, World Economic Forum, January 2023

[17] *Apps uit landen met een offensief cyberprogramma tegen Nederlandse belangen* [Apps from countries with an offensive cyberprogramme targeting Dutch interests], NCSC, visited in June 2023

[18] An insider threat is a threat originating from within the organisation, for instance because employees, former employees and suppliers can access information. Or because they know what kind of security is in place. An insider threat occurs when such (former) employees or suppliers exploit their position for malicious activities.

[19] See, for instance, CISA's publications on managing insider threat risks: *Insider Threat Mitigation*, CISA, visited on 7 July 2023

[20] Some countries run an offensive cyberprogramme targeting Dutch national security interests, including China, Russia, Iran, and North Korea. The AIVD, MIVD and NCTV discuss this threat in greater detail in *Dreigingsbeeld Statelijke Actoren* (DBSA).

Dreigingsbeeld Statelijke Actoren 2 [Threat Assessment State-sponsored Actors 2], AIVD, MIVD and NCTV, November 2022

[21] The NCSC executes MASKeR with prioritised industries. MASKeR is a risk management method that uses scenarios to map threats, interests that must be protected, and resilience. Please contact your relationship manager if you are interested in MASKeR.

[22] *Basismaatregelen cybersecurity* [Basic cybersecurity measures], NCSC, visited on 23 June 2023

[23] Shadow IT also means the use of cloud solutions such as DropBox, WeTransfer and GoogleDrive. These solutions are popular among employees to facilitate file transfer for private purposes. Using such solutions for business purposes out of your organisation's control represents an additional risk. For more information on Shadow IT, please refer to: *Shadow IT: Hoe voorkomen we het?* [Shadow IT: how can we prevent it?], KPN, December 2018

[24] *CISA Tabletop Exercise Package*, CISA, 17 December 2020

[25] *Samenwerking in een ISAC* [Collaborating in an ISAC], NCSC, visited on 23 June 2023

[26] *Succesfactoren voor het delen van cybersecurity informatie* [Success factors for sharing cybersecurity information], The Hague University of Applied Sciences, August 2020

**Publication**
National Cyber Security Centre (NCSC-NL)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

**More information**
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

15 augustus 2023

**TLP:CLEAR**