Supply chain management – practical considerations

Authors: Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

In the last couple of year, there has been significant emphasis on supply chain management, as there has been a growing number of successful attacks that started by targeting a service provider in order to reach its clients (e.g. for exfiltration of data, for affecting the integrity of the data, for deploying ransomware within that client organization).

Thus, recently, there have been a series of best practice guides for handling third parties providing services to an organization or holding (or processing) the data of an organization. This includes NIST[1] with best practices and SP 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations and CISA, with best practices on this topic.[2] These best practices and guidance working papers focus on technical and organizational aspects of handling supply chain management. In this article, we are focusing on practical aspects in order to put in place appropriate processes in relation to the supply chain.

Further, from a legal perspective, the requirements in terms of third parties and sub-contractor have also increased in the past decade. In certain cases, this impact is clearly detailed, as is the case of outsourcing in the financial services sector or in data protection legislation (e.g. the obligations undertaken by the co-contractor of the organization have to be replicated throughout the supply chain to all of its sub-contractors and so on). In other cases, the impact is less clearly detailed, as is the case of the NIS Directive (including national implementation legislation), which expressly emphasize the obligations undertaken by the co-contractor of the organization.

In this article we are focusing on a couple of first steps that can be taken in this direction and which can be implemented by organizations having a low or medium level of maturity in terms of third party management.

It is important to use resources efficiently within an organization. To this end, a prioritization should be performed on the approach to be taken to ensure security throughout

[1] NIST, Cyber Supply Chain Best Practices, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf , last accessed on 21 July 2021. NIST, SP 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft , last accessed on 21 July 2021.
[2] CISA, ICT Supply Chain Risk Management Toolkit, https://www.cisa.gov/ict-supply-chain-toolkit , last accessed on 21 July 2021. CISA and NIST, Defending Against Software Supply Chain Attacks, https://www.cisa.gov/publication/software-supply-chain-attacks , last accessed on 21 July 2021.

the supply chain. Below we have included a couple of preliminary characteristics of co-contractors or services/products provided by them that can be used for establishing a risk based third party framework. Such an approach is aimed at using in an efficient manner existing resources and at addressing the risks with the highest impact or probability, depending on the risk appetite of the organization.

Based on the impact on data (and personal data), co-contractors/sub-contractors can be classified as follows:

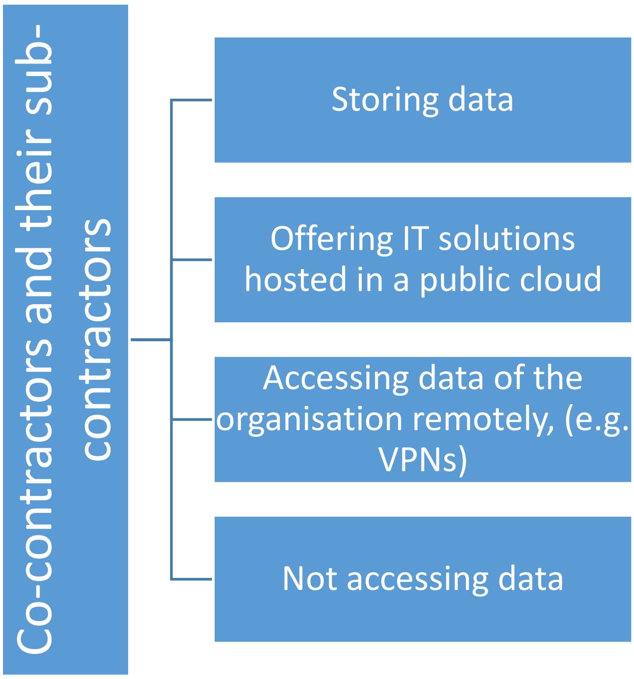

Co-contractors and their sub-contractors
Storing data
Offering IT solutions hosted in a public cloud
Accessing data of the organisation remotely, (e.g. VPNs)
Not accessing data

Figure 1 – Third parties classified based on their access to data (and personal data)

Further, regardless if data access/data management/data storing is involved, third parties can be classified based on the impact of their services/products on the security landscape of the organization, as follows:

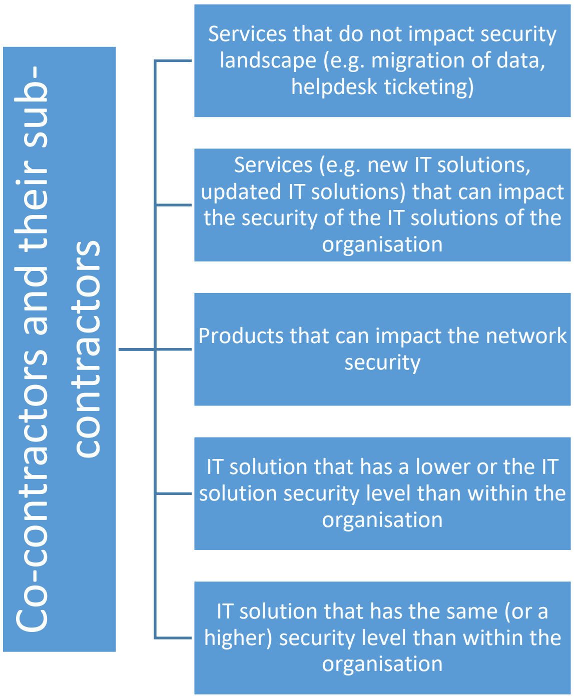
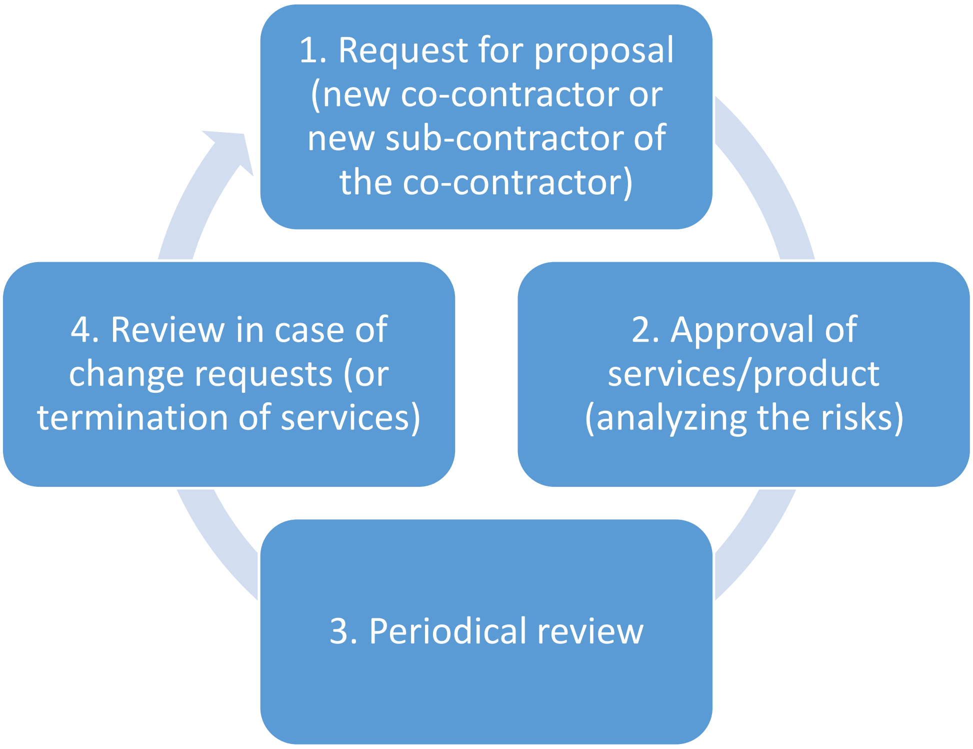

Co-contractors and their sub-contractors
Services that do not impact security landscape (e.g. migration of data, helpdesk ticketing)
Services (e.g. new IT solutions, updated IT solutions) that can impact the security of the IT solutions of the organisation
Products that can impact the network security
IT solution that has a lower or the IT solution security level than within the organisation
IT solution that has the same (or a higher) security level than within the organisation

Figure 2 – Third parties classified based on their impact on the security landscape

Regardless of the classification above, there are certain steps that should be taken in relation to third parties. These can be considered the supply chain life-cycle. The specific actions for each step can be established by each organization based on specific guidelines (such as the ones above) and applicable thereto.



1. Request for proposal (new co-contractor or new sub-contractor of the co-contractor)
2. Approval of services/product (analyzing the risks)
3. Periodical review
4. Review in case of change requests (or termination of services)

Figure 3 – Supply chain life-cycle

Below, we are detailing specific aspects to consider for each of the above steps. Throughout the below sections, we refer to the co-contractor of the organization as the vendor.

1. Request for proposal

When an organization wishes to obtain a specific service or product, the first step is to prepare a request for proposal procedure, whether there is a single potential vendor or there are multiple potential vendors.

In this phase, the organization can request a baseline of security measures (and data protection requirements) to be confirmed by the entities submitting the proposals. Generally, lack of full compliance with such baseline entails the exclusion of the respective vendor from the request for proposal process. This assessment should be performed by individuals within the organization that have expertise in the security, respectively, data protection field.

The baseline requirements can be tailored based on the types of services provided by the vendor, focusing on the aspects outlined below.

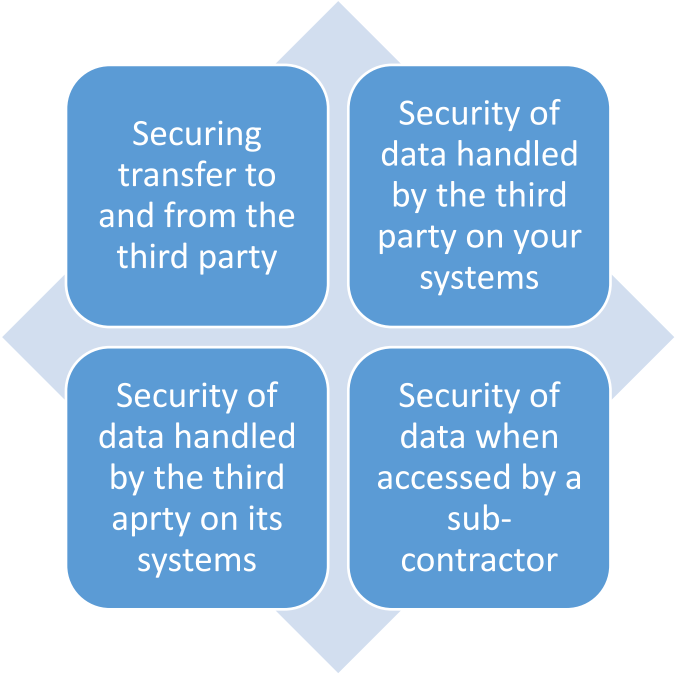

Securing transfer to and from the third party
Security of data handled by the third party on your systems
Security of data handled by the third aprty on its systems
Security of data when accessed by a sub-contractor

Figure 4 – Security approaches based on services provided by third parties

The same process is applicable in case of sub-contractors. Generally, for custom types of services and products (e.g. not for cloud services, off-the-shelf software), the organization can request to be notified of any sub-contractors being contemplated before these are contracted by the vendor.

2. Risk analysis

The selected vendor, aside from the brief baseline confirmation/analysis during the request for proposal phase, should be subject to a more detailed analysis in terms of security (and data protection), correlated with the matters detailed in the contract being negotiated with this vendor.

From a legal and privacy perspective the following main aspects have to be taken into account at the outset and during the use of third parties for various services:

- **Know your IT (and third party) landscape** – it is important to understand the impact of the services/products on the organization and on the data/information held by the organization.
- **Understand the risk** – once the IT landscape is clear, the risk assessment can commence, taking into account the services/product stand-alone and within the IT ecosystem of the organization. In this respect, there a series of risk assessment frameworks that can be used or adapted, such as Octave, NIST RMF, etc.
- **Manage the risk** – for the identified risks, proper measures (controls) can be put in place as a response to the risk (e.g. to reduce the risk level). Such measures can be implemented by the organization or by the vendor. They can be organizational (e.g. procedure, obligation undertaken in a contract) or technical (e.g. changes to the It solution, changes to the infrastructure).
- **Establish workflows with the vendor** – the organization will require assistance in certain situations from the vendor and its sub-contractors. These should be discussed and established from the outset, periodically refreshed in order for all parties to know their role in the process. The organization may consider establishing workflows for:
  - security incident identification and investigation,
  - assistance in case of investigations from authorities or complaints from clients of the organization,
  - reporting obligations of the organization to relevant authorities,
  - auditing of vendor by an independent auditor or by the organization itself

From a technical and operational perspective, the security (and data protection) baseline can be analyzed taking into account the below:

- Relying on third party’s external auditors – an organization should generally prefer to have an analysis performed by external auditors chosen by it, as this entails knowing exactly the scope, the documents provided by the third party, etc.
- Using auditors chosen by the organization – this is the preferred approach. It may be used as a periodical review and not necessarily at the outset of the involvement with the vendor.
- Relying on third party’s internal auditors or assessment – this should generally be avoided, as this does not present a level of independence needed.

- Automating the process – for certain reporting that the organization may want to monitor throughout the relationship with the vendor, the organization may set-up indicators (e.g. KRI, KPI) in an automated manner in order to efficiently gather and analyze the data.

- Allocating proper resources – these actions of analysis, monitoring, etc. require in the organization employees with proper experience.

- Sharing threat intelligence and having in place proper notification and investigation processes – for prevention of incidents, swift response in case of a security incident or identification of a vulnerability is essential.

  Less experienced vendors may require training and guidance in terms of incident identification and incident handling. More experienced ones may establish a process for sharing of information about threats.

  Often, a software or infrastructure component used by the vendor (or its sub-contractors) may include a vulnerability that is used by attackers. In this case, proactive analysis of potential vulnerabilities by each entity in the supply chain, the constant communication throughout the supply chain and swift reaction in case such vulnerability is essential.

- Controls within the organization – following the analysis, certain measures may need to be implemented within the organization. Proper monitoring thereof should be in place.

- Controls within the co-contractor's IT infrastructure (or its sub-contractors) – in addition, the analysis may reveal the need for certain measures to be implemented by the vendor (or its sub-contractors). This is the reason why it is essential to have an analysis before signing the agreement with the vendor and before deploying the solution of the vendor. Certain changes may need to be made to the vendor's solution and certain obligations may need to be included in the contract with the vendor. Proper monitoring of the implementation of such measures should be made by the organization.

- Verify security within the IT infrastructure the IT solution is placed after deployment – it is essential not view the services/product offered by the vendor in context, respectively, in the IT ecosystem it is going to be deployed in. Thus, during this risk analysis phase, this should be the angles from which the assessment is performed.

3. Periodical review

The above analysis should be performed periodically. The option for analysis can range, as detailed above, from independent auditors, internal auditors of the organization, and auditors of the vendor or independent certifications of the vendor, depending on the classifications mentioned at the beginning of the article, the previously identified risks and the resources of the organization. These should be also had in mind in terms of frequency of analysis. For higher risk vendors, more frequent reviews should be considered, whereas, for less high risk vendors, less frequent reviews can be chosen.

4. Review in case of change requests

Throughout the lifetime of service provision, various changes may occur, such as new modules, changes in functionality of existing modules, exclusion of certain modules. These situations should be identified within the organization and serve as triggers for a re-analysis similar to the ones in step 2. Changes, either new elements or exclusion of new elements, can both bring additional risks and the need for additional measures.