Supply chain cyber security

Assessing and gaining confidence in your suppliers

National Cyber Security Centre
a part of GCHQ

'**How to assess and gain confidence in your supply chain cyber security**' is aimed at procurement specialists, risk managers and cyber security professionals wanting to establish (or improve) an approach for assessing the cyber security of their organisation's supply chain.

It's particularly suitable for medium to large organisations who need to gain assurance that mitigations are in place for vulnerabilities associated with working with suppliers. It can be applied 'from scratch', or can build upon any existing risk management techniques and approaches currently in use.

The guidance is broken into 5 stages, which are summarised in the following diagram. Note that some of the steps in stages 3 and 4 can be carried out in parallel. You can download the guidance in full from ncsc.gov.uk/supplychain.

1 Before you start

- **Understand why your organisation should care about supply chain cyber security**
- **Identify the key players in your organisation**
  Having the right people in place to support supply chain cyber security will help drive the changes required.
- **Understand how your organisation evaluates risk**

2 Develop an approach to assess supply chain cyber security

- **Prioritise your organisation's 'crown jewels'**
  Determine the critical aspects in your organisation that you need to protect the most.
- **Create key components for the approach, which include:**
  - security profiles to be assigned to each supplier
  - questions to determine the security profile of each supplier
  - cyber security requirements for each profile
  - management plans to track suppliers' compliance with security requirements
  - clauses relating to cyber security to insert into supplier contracts

3 Apply the approach to new supplier relationships

- **Educate the team**
  Ensure that the people who will be involved in assessing suppliers are trained in cyber security.
- **Embed cyber security controls throughout the contract's duration**
  Consider cyber security throughout the contract lifecycle: from decision to outsource, supplier selection, contract award, supplier delivery to termination. Think what practices can be introduced to make sure this happens for every acquisition.
- **Monitor supplier security performance**
- **Report progress to the board**

4 Integrate the approach into existing supplier contracts

- **Identify existing contracts**
- **Risk assess your contracts**
- **Support your suppliers**
- **Review contractual clauses**

5 Continuously improve

- **Evaluate the approach and its components regularly**
- **Maintain awareness of evolving threats and update practices accordingly**
  Maintain awareness of emerging threats and use the knowledge acquired to update your supply chain cyber security accordingly.
- **Collaborate with your suppliers**

1

Before you start

Gain knowledge about your own organisation's approach to cyber security risk management.

National Cyber Security Centre
a part of GCHQ

Key steps

Understand why your organisation should care about supply chain cyber security

Unless you understand what needs to be protected and why, it can be very hard to establish any meaningful control over your supply chain. In this step you will determine:

- Why might someone be interested in attacking your supply chain?
- Who are behind supply chain attacks, and what are their motives?
- What are the potential cyber threats that could cause harm to your organisation?
- What vulnerabilities could be exploited within your supply chain via a cyber attack
- What is the impact on your organisation if these vulnerabilities are exploited?

Once this is understood in the context of your organisation, it becomes a lot easier to talk about and build a case for senior buy-in and investment to promote change around supply chain cyber security within the organisation.

Identify the key players in your organisation

Having the right people in place to support supply chain cyber security will help drive the changes required. Think of people within your organisation and consider:

- Who do you need to convince to establish or improve assessment of supply chain cyber security?
- Who is responsible for developing a new approach to assessing supply chain cyber security?
- Who should be consulted during the development of this new approach?
- Who should be kept informed about the activity?

Once you have identified the above:

- Pitch to your influencers and decision makers on why they should invest in securing the supply chain.
- Create terms of reference that you can use to initiate the change effort.
- Set up a governance process where security leadership meets with the board on a regular basis.
- Define a process with clear roles & responsibilities and criteria.

Understand how your organisation evaluates risk

Effective cyber security should be appropriate to your systems, your processes, your staff, your culture, and the level of risk you are willing to take.

Therefore the way you assess cyber security in your supply chain will depend upon understanding how you organisation works, its function, and what its risk appetite is. There is not one approach to this activity, and businesses will usually have their own methods of dealing with risks.

Outputs

- Better understanding of the threats to your supply chain based on the nature of the relationship you have with your suppliers (and the accesses they have to your systems and services).

- Team established to develop a new approach for assessing supply chain cyber security.
- Senior buy-in to implement change to establish or improve supply chain cyber security.

- Increased understanding of existing risk appetite and processes within your own organisation.

2 Develop an approach to assess supply chain cyber security

Once you've determined the critical aspects in your organisation that you need to protect the most, create a repeatable, consistent approach for assessing the cyber security of your suppliers.

National Cyber Security Centre
a part of GCHQ

Key steps

Prioritise your organisation's 'crown jewels'

Determine the critical aspects in your organisation that you need to protect the most (your 'crown jewels'), taking into consideration potential threats, vulnerabilities, impact and your organisation's risk appetite.

Create a set of security profiles

Using your organisation's 'crown jewels', create a number of tiered supplier security profiles. Each profile should represent an increasing scale of impact, which can be assigned to each of your suppliers.

Determine the security profile for each supplier

You can use a series of questions to triage each supplier, and determine which of the security profiles they be should assigned.

Define the minimum cyber security requirements for each security profile

For each security profile, determine the minimum cyber security requirements that each supplier must adhere to. Map out the necessary requirements with increasing levels of stringency as the risk level increases, ensuring that they are proportionate to the risk posed.

Decide how to assess your suppliers

A combination of techniques should be considered to allow the cross section of suppliers to be assessed, which can include question-based surveys, interviews, site visits, or independent assessment / certification.

Plan for non-compliance

Suppliers may not always fully comply with your requirements. However, you may still wish to work with them, whilst they rectify any shortfalls. Planning for this is useful as you can articulate the expected frequency and nature of continued assessments, to ensure an accurate and up-to-date picture.

Create contractual clauses

Create a standard set of clauses to include within your contract agreements to cover a variety of likely scenarios for your organisation. These can then be easily inserted into the process as part of an acquisition.

Outputs

- A clear understanding of the most critical aspects of your organisation, with criteria for determining what assurances you need from suppliers to be able to protect them.
- A set of 'security profiles', with the minimum cyber security requirements each profile is expected to meet.
- Questions to determine the security profile of each supplier.
- Artefacts required to assess each supplier's requirements.
- A supplier security management plan to track compliance to cyber security requirements.
- Standard contractual clauses (relating specifically to cyber security) to insert into contracts.

3 Apply the approach to new supplier relationships

Embed new security practices throughout the contract lifecycle of new suppliers, from procurement and supplier selection through to contract closure.
(Some of steps in stages 3 and 4 can be carried out in parallel)

National Cyber Security Centre
a part of GCHQ

Key steps

Educate the team

Ensure that the people who will be involved in assessing suppliers:

- are aware of the threats posed by supplier cyber security
- understand their role in reducing the risk
- understand the process that you have defined for your organisation

Embed cyber security controls throughout the contract's duration

Consider cyber security through every step of the contract lifecycle:

- If a decision has been made to outsource to an external supplier, determine whether a cyber security risk assessment is needed and to what level, based on the risk criteria you have set.
- During supplier selection, conduct due diligence, assess each supplier's ability to meet your cyber security controls and ensure this is a part of the decision-making process for selection.

- When awarding a contract, stipulate compliance with necessary cyber security controls in the supplier contract and agree this with the supplier.
- Whilst in contract with the supplier, ensure supplier security provisions are effective and meeting expectations, incidents are managed appropriately and there is an up-to-date awareness of evolving threats and vulnerabilities.
- When terminating a contract, make sure you regain control of your assets and shut down any unauthorised or unintended access to your information and systems.

Monitor supplier security performance

A one-off assessment will not be sufficient to ensure your cyber security standards are being met. Monitoring vulnerabilities in your supplier's cyber resilience on a regular basis will help you to identify where there are shortfalls and to work with your suppliers to address them (before they are exploited and become an issue).

Report progress to the board

It is important to uphold governance to ensure that cyber security practices introduced remain relevant and are ultimately meeting the objective to help secure the supply chain.

Define success criteria and metrics for reporting to the board, with a consistent method and frequency so the board have visibility of the risk levels.

Outputs

- Cyber security practices embedded throughout the acquisition process, supported by a multi-disciplinary team of cyber security trained professionals.
- Increased awareness of supply chain threats amongst staff.
- Performance is being regularly measured against defined metrics, visible to board members.

4 Integrate the framework into existing contracts

With a new approach in place, review your existing contracts either upon renewal, or sooner where critical suppliers are concerned.
(Some of steps in stages 3 and 4 can be carried out in parallel)

National Cyber Security Centre
a part of GCHQ

Key steps

Identify existing contracts

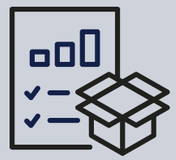
Build a register of all suppliers that your organisation is working with. This may not be straightforward if suppliers have been contracted in via various sources, so consider asking the finance department to provide information on any suppliers that have been paid over a particular timeframe. At a minimum your key suppliers should be identified.

Support your suppliers

If you find a shortfall in how existing suppliers are managing cyber security risks, you should discuss the steps required to rectify this. It can be recorded in the security management plan.

Risk assess and prioritise contracts

Risk assess and prioritise existing contracts, with focus on critical business functions and areas of high cyber risk. Conduct an assessment of those contracts in priority order until you are confident that the core contingent of suppliers have been assessed.



Review contractual clauses

If the contract with your supplier does not address the ability to assess during the contract term (or to understand the cyber security position of the sub-contractors), you need to understand what can be achieved on a 'best endeavours' basis until this can be contractually binding.

Monitor supplier security performance

A one-off assessment will not be sufficient to ensure your cyber security standards are being met. Monitoring vulnerabilities in your supplier's cyber resilience on a regular basis will help you to identify where there are shortfalls and to work with your suppliers to address them (before they are exploited and become an issue).

Report progress to the board

It is important to uphold governance to ensure that cyber security practices introduced remain relevant and are ultimately meeting the objective to help secure the supply chain.

Define success criteria and metrics for reporting to the board, with a consistent method and frequency so the board have visibility of the risk levels.

Outputs

- A register recording all your suppliers.
- 'High priority' suppliers are risk assessed against defined security controls
- Suppliers with security shortfalls are identified, and a plan to improve their security is agreed.
- Improved approach based on lessons learned from the activity.

5 Continuous improvement

Periodically refining your approach as new issues emerge will reduce the likelihood of risks being introduced into your organisation via the supply chain.

National Cyber Security Centre
a part of GCHQ

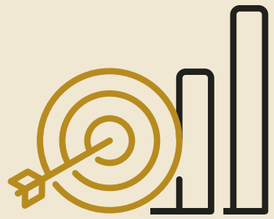
Key steps

Evaluate the framework and its components regularly

Evaluate how well the process is working, what can be learned from the evaluations that have previously occurred, and adjust the process accordingly so that it provides the right level of risk/reward for your organisation.

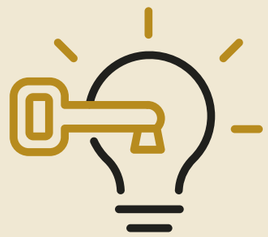
Maintain awareness of evolving threats and update practices accordingly

Once the initial assurance of your supply chain is complete, it is important to recognise that the threat landscape, procurement and supply chains are continuously evolving. An assessment made a long time ago may no longer be sufficient. Maintain awareness of emerging threats and use the knowledge acquired to update your supply chain cyber security accordingly.



Collaborate with your suppliers

Use your awareness of evolving threats and your suppliers' cyber resilience to raise concerns regarding any identified vulnerabilities. Depending on the resources available to you, the frequency of this may be fluid or may be done periodically. A supplier security management plan can be used to articulate how frequently this is done, and what method of assessment is required. If there are outstanding issues that need to be resolved with your supplier, you may look to do this more regularly.



Outputs

- Foundation established to continuously improve.

For more supply chain security guidance, please visit ncsc.gov.uk/supplychain.