GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

Supply chain security

Collaborate with your suppliers and partners.

Most organisations rely upon suppliers to deliver products, systems, and services. An attack on your suppliers can be just as damaging to you as one that directly targets your own organisation. Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it. The first step is to understand your supply chain, including commodity suppliers such cloud service providers and those suppliers you hold a bespoke

contract with. Exercising influence where you can, and encouraging continuous improvement, will help improve security across your supply chain.

What are the benefits?

- **You can manage risk to your business that manifests in the supply chain**
- **More effective relationships with your suppliers and partners and better understanding of each other's needs**
- **Clear understanding of what parts of security you are responsible for, and what you are relying on your suppliers to do**
- **Better visibility and early warning signs of incidents that might affect your organisation**
- **Identifying any over-reliance on single suppliers**
- **Demonstrating good cyber security can help you win supplier contracts, particularly those from government where it is already required**

What should you do?

Understand your supply chain

Until you have a clear picture of your existing supply chain, it will be very hard to establish where you can have any meaningful control over it. Ensure you have a list of all your suppliers, and partners, and identify which ones are highest priority (in terms of risk) to concentrate your efforts on. Where possible include subcontractors beginning with your highest priority direct suppliers.

Look for information published by your existing commodity suppliers that help you understand the security of their service. Ensure you understand the terms and conditions in your contract or licensing agreement and what parts of security each are responsible for.

Work with the suppliers you have a bespoke contract with to understand their current security posture. How does that compare with what you've asked of them (if anything), and what they've asked of their subcontractors (focusing on the parts of their organisation that handle your contract)? Understanding your supply chain and the risks posed to it will help identify any suppliers who consistently fail to meet expectations.

Develop a common understanding with your suppliers of each party's security responsibilities, and what subcontracting decisions you are happy to delegate to them.

Embed security within your contracting process

Build security considerations into your contracting decisions, and where appropriate require your suppliers do the same. Establish supply chain security awareness and education for appropriate staff, and work with them to ensure the process is fit for purpose.

When making decisions about commodity suppliers like cloud service providers, look for published information on their website that might help you understand whether they adequately meet your security requirements. You are likely to have standard terms and conditions in your contract or licensing agreement so ensure you are aware of what parts of security you are responsible for and what they will do for you. Refer to the NCSC's Cloud security guidance for more information on how to determine how confident you can be that a cloud service is secure enough to handle your data.

Prospective suppliers should provide evidence of their approach to security, and their ability to meet the minimum security requirements you have set at different stages of the contract competition. Minimum security requirements (like Cyber Essentials for mitigating commodity attacks against enterprise technology) should be proportionate to the risk for each supplier. Ensure standards are justified and achievable and won't unnecessarily put off suppliers looking to compete for contracts with you.

Avoid creating unnecessary barriers and acknowledge and be prepared to recognise any existing security practices or certifications they might have that could demonstrate how they meet your minimum security requirements.

Ensure you provide supporting guidance, tools and processes to suppliers to enable them to effectively manage supply chain risk to your requirements. If you are a supplier, make sure you meet the security requirements of your customers, including challenging customers and partners for guidance when it's not provided.

Consider what support you will need from suppliers to maintain their products and services, likewise use vendor or community supported software where available.

Ensure that contracts clearly set out specific requirements for the return and deletion of your information and assets by a supplier on termination or transfer of that contract.

Support organisations in your supply chain to improve

Be prepared to provide assistance when necessary where security incidents in your supply chain have the potential to affect your business or the wider supply chain. Your contract should include requirements for managing and reporting security incidents.

Listen to and act on any concerns highlighted through performance monitoring, incidents, or upward reporting from suppliers that may suggest that current approaches are not working as effectively as planned.

Seek to build trust and strategic partnerships with key suppliers, sharing issues with them, and encourage and use their input to improve your collective security.

Include important partners in your cyber incident response exercising where appropriate.

Learn more

Supply chain security guidance
Principles designed to help you establish effective control and oversight of your supply chain.

Supplier assurance questions
Questions to ask your suppliers that will help you gain confidence in their cyber security.

Cloud security guidance
Guidance on how to configure, deploy and use cloud services securely.

← Incident management

Topics

Operational security

Risk management

Supply chain

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

Also see

Weekly Threat Report 23rd July 2021

The NCSC's weekly threat report is drawn from recent open source...

Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021