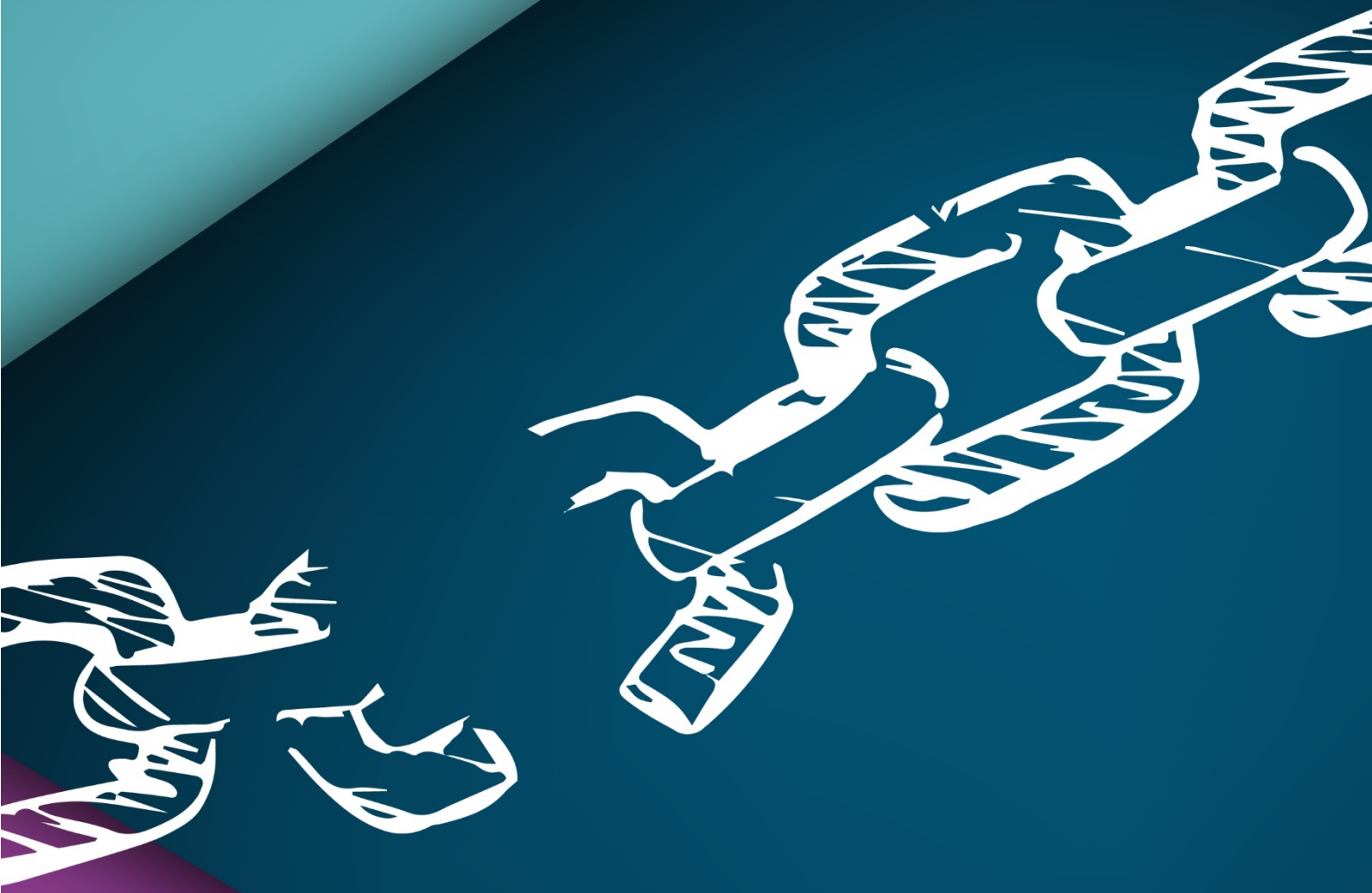
Guide to **Supply Chain Cyber Security**



evalian

Evalian Limited – Guide to Supply Chain Cyber Security

This comprehensive guide will give you an insight into supply chain cybersecurity and risk management. The table of contents at the right-hand side enables you to navigate the different sections.

Introduction

The interconnected nature of the world means we can employ external organisations to deliver beneficial services to our own in the blink of any eye. Technology allows us to share information far and wide, to our colleagues, customers and partners. It allows outsourcing, subcontracting, and sharing of the processing of information at a scale not previously seen, sometimes with organisations we've never met.

This means enterprises no longer sit within a digital walled castle. Now, they are part of a network of networks, where their suppliers provision their payroll, process expenses, order hire cars (conveniently to home addresses), process their sensitive data and deliver physical goods and services on their behalf. This means most organisations now have a complex supply chain, where their supplier subcontracts to another supplier and they subcontract and so on, to such an extent that information is crossing multiple organisational and political boundaries in an electronic heartbeat.

These supplier relationships reduce costs and increase business efficiency, but they also give rise to new risks. The increased sharing of information or connectivity to our systems increases our vulnerability to security breaches.

Evalian Limited – Guide to Supply Chain Cyber Security

Management and mitigation of supply chain vulnerabilities are therefore critical for organisations who wish to protect their revenue, reputation and remain compliant with sector, regulatory and national legislative bodies.

Setting the Scene

In 2013, a scandal rocked household brands as they discovered it wasn't beef they were selling, it was horse meat. Burgers on sale at two UK supermarkets and three Irish supermarkets were found to contain traces of it: a total of 27 supermarket beef products were tested, with ten of them containing horse DNA and the vast majority, 23, containing pig DNA. One of the issues the scandal highlighted was how vulnerable to food crime the supply chain is.

The Horsegate scandal is a great analogy for cybercrime in the supply chain. Before the scandal, traders trusted their suppliers to deliver goods of a certain standard without any form of due diligence. In the wake of Horsegate, there has been a considerable increase in audit activity to ensure product authenticity.

Defining the Cyber Supply Chain

Clearly, the cyber supply chain is different to the food supply chain and poses different threats. Suppliers with access to your information are not always easy to identify, compared to tangible products, and, as such, the starting point is to identify which organisations are in your cyber supply chain. To help with this we have to define what the cyber supply chain is.

The United States' National Institute of Standards and Technology (**NIST**)'s guidance Supply Chain Risk Management Practices for Federal Information Systems and Organizations 800-161 ("NIST 800-161") defines it as the linked set of resources subject to cyber supply chain risks from suppliers, their supply chains, and their products or services. Cyber supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to it.

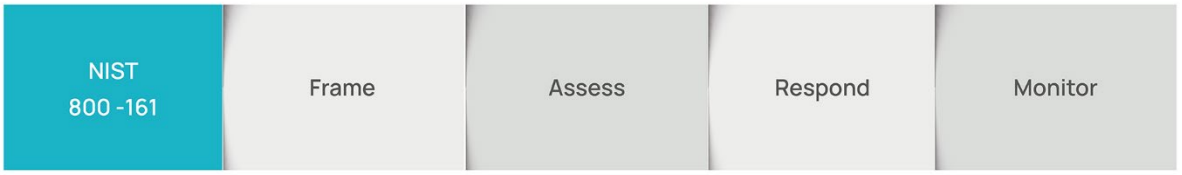
Trust, But Verify

"Trust, but verify" is a Russian proverb and now a cybersecurity maxim. Whereas supplier relationships have historically been built on trust, organisations now need to move beyond trust and seek assurance from their cyber supply chain. They need to question the authenticity of the suppliers and partners they are sharing information with or have access to their digital estate.

Sources of Best Practice

Supply chain cybersecurity is a nascent field. It's like the elephant outside the room, which no one really wants to talk about, even less do anything about. Nonetheless, there are best practice guides available which we recommend to clients.

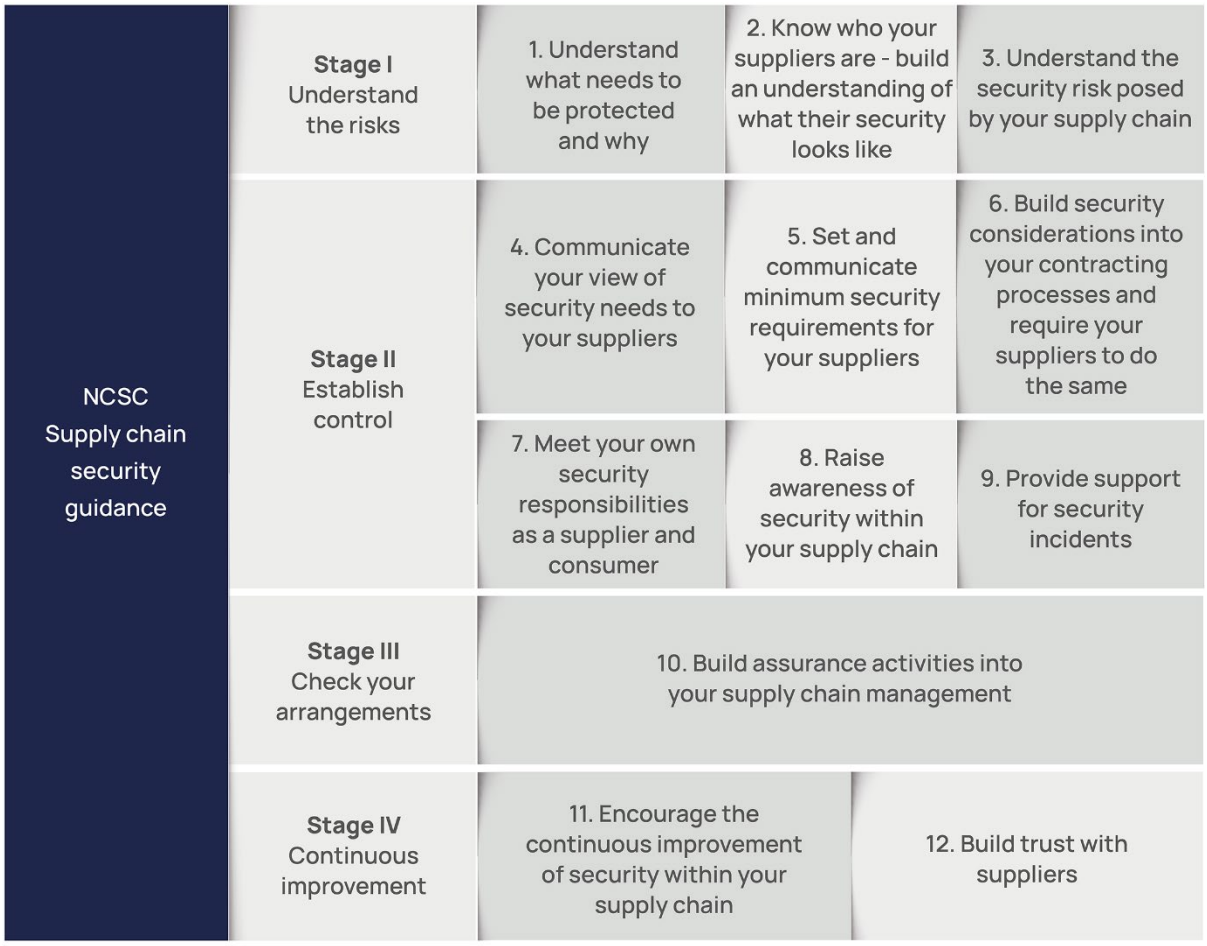
We have already mentioned NIST 800-161. This proposes an approach to supply chain cybersecurity that covers 4 stages across 3 tiers. The 4 stages sit above Organisation (executive leadership), Mission (business management) and Information Systems (systems managers), as shown in the following image:



NIST has also published an Interagency Report (NISTIR) 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. NISTIR 8267 is a more digestible document than 800-161 and suggests the following 8 key practices for supply chain cybersecurity risk management:

Evalian Limited – Guide to Supply Chain Cyber Security

The UK's National Cyber Security Centre (**NCSC**) proposes 12 principles designed to enable effective control of the supply chain. While this may seem more complex compared to NIST's four stages, the NCSC's guidance is easy to digest and a great starting point for anyone with a non-technical background. These stages are shown in the following image:



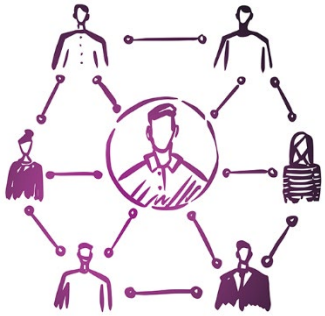
Another helpful source of guidance is ISO 28000, which provides a specification for a security management system for the supply chain. Organisations can be certified to ISO 28000 to demonstrate best practice in supply chain risk management – but be aware the standard covers more than supply chain cybersecurity.

For an example of how supply chain cybersecurity management can operate in practice, you can also take a look at the pragmatic approach followed by the UK Ministry of Defence, details of which are available here.

Establishing a Supply Chain Cyber Security Programme

When establishing a supply chain cybersecurity programme, it is important to create a justifiable reason for doing so and to communicate this across the whole organisation (not just within IT or technical teams). Understanding and addressing risks in your supply chain normally starts by working with the procurement / commercial element of your organisation to identify who your suppliers are and to prioritise the suppliers who are assessed as high risk.

Evalian Limited – Guide to Supply Chain Cyber Security



It is common for organisations not to know how many suppliers they have or what information they are sharing. This discovery work enables them, often for the first time, to go from what Donald Rumsfeld famously referred to as the 'unknown unknowns' to 'known knowns'. Furthermore, mitigating cyber risk in the supply chain allows you to build alliances within your organisation (commercial, legal and IT as a minimum) to ensure risks are addressed effectively.

Your supply chain cybersecurity programme should set out a logical plan of work. The goal is to create specific outcomes to ensure what, for many organisations, is a behemoth, can be addressed pragmatically, in a risk-based manner and progressed against an agreed plan. After all, the way to eat that elephant, which in this case is not in the room, is by taking one bite at a time.

You should initially use a simple, three-stage process to profile cyber risk in your supply chain:

Cyber risk profiling

First, working with procurement, conduct a risk assessment on each contract. This assesses cyber risk and creates a unique identifier, which can be used to reference each specific cyber risk profile. Establishing one for each contract allows organisations to easily identify where risk is and calculate if mitigation is required.

Supplier assurance

Second, work with your suppliers to find more information about their cybersecurity standards. This identifies which suppliers have adequate controls in place and which require an improvement in their information security and data governance. Good supplier relationships are crucial and you will need to consider the acceptability of risks, whilst your suppliers enforce appropriate remediation work.

Buyer's assessment

Third and finally, assess the responses to the supplier assurance questionnaires, examine each risk in detail and look at the whole risk picture.

Know and Understand Critical Suppliers

Once the three-stage process is complete, you can move focus to your critical suppliers – critical both in terms of your business need and exposure to cyber risk. We recommend you keep the technical stuff streamlined and employ common cybersecurity standards to ensure mitigations are appropriate to the risk and the value of the contract. You should

follow a process that allows you to present evidence for supplier selection or targeted action. Your end-state is a vendor approval process that is business as usual, which you and your suppliers find easy to use and does not need a technical advisor to complete.

Take a risk-based approach

As an example, a low-risk contract may require a supplier to meet the NCSC's standard of Cyber Essentials. This requires the supplier to go through a self-certification process to meet a standard that mitigates against the most common of Internet-borne threats. If the contract is higher risk, then you may want the supplier to meet the Cyber Essentials Plus standard, which involves third-party assurance and a vulnerability assessment of their digital estate.

Your highest risk suppliers will likely have access to, or be interconnected with, your systems or will process your most sensitive information on their systems. Where this applies, you may require them to certify against ISO 27001 or to evidence that they follow a specific set of guidelines such as the NIST Cyber Security Framework or the NCSC's 10 Steps.

If you have a particular concern, wish to mitigate a specific threat or protect a specific supplier, you may choose an approach the UK's MOD has done in its Defence Cyber Protection Partnership, which is a collaboration between the Ministry of Defence, industry, and other Government departments.

Its aim is to build cybersecurity into the Defence Supply Chain. Its approach to suppliers is to mandate specific controls depending on the level of risk. The methodology also incorporates Cyber Essentials as a minimum standard, and the implementation of controls was only done after a great deal of consultation with the MOD's suppliers.

For those suppliers who declare they are already at a standard, we recommend you reserve the right to audit their controls and for these audit rights to be detailed in the updated contracts.

Implementing the Supplier Assurance Process

Practically, supply chain assurance should be implemented in three stages. First, all new contracts should go through the assurance process. Once proven, this becomes embedded as business as usual. This doesn't mean every new supplier must meet the new standard you apply but, instead, only those suppliers who need to invest in information security are asked to.

Then, you can apply the new model to existing contracts, either mid-contract if the specific situation requires it, or on re-contract submission. Your organisation will become aware of where risks lie, how they may affect your company and whether your decision is to avoid, accept, share or mitigate each risk. This activity puts you in a position from which you can make informed decisions concerning business risk and you are aware of the cost of mitigation.

The third stage is consideration of, and the potential inclusion of, suppliers beyond the first tier, whereby you flow-down the requirements through the supply chain until risks are addressed appropriately. This can illuminate the supply chain beyond the first tier, and you can continue this activity down the supply chain as far as you wish.

A good guide to how far down the supply chain you wish to go is to consider who is accountable in the eyes of the law, your customers, and the regulators. This activity can expose where in the supply chain critical activities are taking place and where the most sensitive information is shared or created.

Once a suitable governance body is established, such as a supply chain council or working group, you can create a watchlist of suppliers who had past issues and who you should be cautious of for future use (kind of like a 'naughty list'). Such suppliers could be used only after approval from this governing body, reinforcing the principle of informed risk-taking.

Identify & Collaborate with Key Suppliers

As covered above, your starting point is to develop an understanding of key suppliers, the value of your contract to them and the state of their cybersecurity. Looking beyond the first tier allows you to identify where your information is being processed and how your data are being managed and protected (or not) as they travel the world wide web. This activity enables your organisation to identify risks to its information and to take action to address that risk, no matter where it lies in the supply chain.

Your engagement should rise the tide of cybersecurity rather than dictate an immediate step change, which could lead to friction and disenfranchisement with an otherwise effective supplier. This is an opportunity to strengthen relationships with suppliers, where you can advise and help them improve their cybersecurity practices too.

Resiliency planning is essential, even for the most mature organisations. In addition to knowing how your suppliers will maintain business continuity in the event of uncertainty, you will want to know how they will respond to a cybersecurity incident affecting your data. In some cases, you might need input from your key suppliers if your organisation suffers a security breach.

Our Guide to Incident Response is a good starting point when planning for these occasions. If you want a deep dive into the topic we'd also recommend NIST 800-61 and ISO 27035. For the purposes of this guide, it is important to state organisations should develop and approve plans with key stakeholders, including key suppliers, to ensure the robustness of the supply chain and the continuation of business as usual. This activity is critical to ensure procedures are embedded in organisations and ready to leap into action in the event of an incident.

Assess and Monitor Throughout the Supplier Relationship

The supply chain cybersecurity risk assessment process should not be a one-off activity and we recommend maintaining a constant watch on your supply chain. You should also plan for unexpected interruptions to the supply chain, enabling you to ensure business continuity.

This is not possible if you overburden your commercial team and suppliers with questionnaires and unfocused follow-up responses, or if they constantly badger you for clarification of your questions. Spreadsheet-based tools serve a purpose, provided they are not too complex with unnecessary questions. Online tools which allow for quick and easy follow-up questions and conditional formatting can help speed up the process and focus attention on the key risks.

Managing supply chain risk can include considering what to do if suppliers stop support of outdated hardware and software, discontinue production of hardware components, or adopt a significant change of business direction caused by acquisition, as well as the consequences of a change in ownership or regulatory or legal changes in their sovereign state.

How Important is Supply Chain Security, Really?

Should you address supply chain risk? Well yes, and here's why.

The Identity Theft Resource Centre stated in a recent report that "Supply chain attacks are increasingly popular with attackers since they can access the information of larger organisations or multiple organisations through a single, third-party vendor". Frequently that supplier is smaller than their customer(s), has fewer resources and poorer cybersecurity controls (if any). These types of attacks are often referred to as 'island hopping' attacks.

The NCSC has provided examples of real-world supply chain compromises in their supply chain security guidance here. We have also seen some of the fallout from supply chain breaches in the UK, with BA fined £20M by the ICO after their website payment section was exploited in 2018 through a vulnerability in third-party Java script. Similarly, Ticketmaster was fined £1.25M after a chat-bot, hosted by a third party on its online payment page, allowed an attacker access to customers' financial details.

Most recently, Russia's Foreign Intelligence Service compromised the global software vendor SolarWinds. They were able to access systems using SolarWinds' software, which included other global and government bodies including the US government, Microsoft, and security vendors FireEye and Crowdstrike.

Perhaps the most famous supply chain breach was suffered by the US retail giant, Target (2014). The attackers secured access to Target's systems by compromising Fazio Mechanical Services, a small provider of heating, ventilation and air conditioning systems ("HVAC"). Fazio had access to Target's systems for the purposes of HVAC maintenance.

A Fazio employee was duped into downloading malware to their computer by a simple phishing email. Once the Fazio device was compromised, the attackers waited until the malware found login credentials for Target's systems. This provided access to a Target system from which Fazio had access to billing, contracting and project management. This was sufficient for the attackers to get a foothold. From there, they exploited other vulnerabilities to access the wider Target network and eventually access the point-of-sale systems used in its stores.

40 million debit and credit records were stolen from Target, they suffered a 46% drop in profits in the following quarter (compared to the previous year) and the company later reported that the total cost of the data breach to the company had been over $200 million.

Securing the supply chain closes the backdoor to your business and enables you to mitigate known risks. A strong programme allows your business to thrive, without dealing with unwanted data breaches, cyber-attacks and fines.

Contact us

Telephone

03330 500 111

Email

hello@evalian.co.uk

Head Office

West Lodge, Leylands Business Park, Colden Common, Hampshire, SO21 1TH

London Office

10 Fitzroy Square, London W1T 5HP

Manchester Office

Jactin House, 24 Hood Street, Ancoats, Manchester, M4 6WX

Dublin Office

69 Main Street, Blackrock, Dublin, Ireland, A94 N6D0

Visit

www.evalian.co.uk