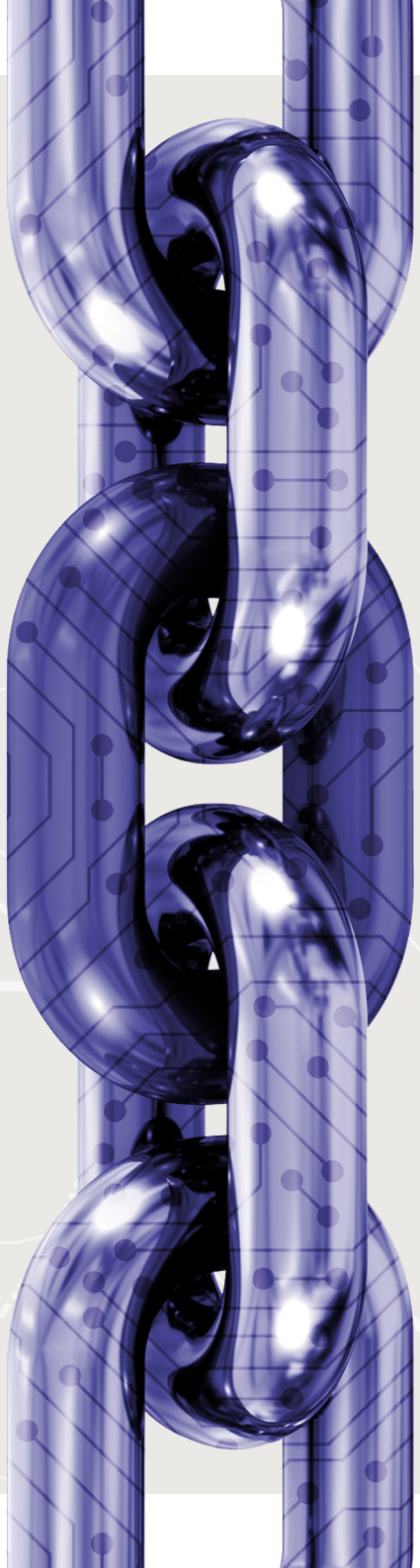
SUPPLY CHAIN CYBER SECURITY.

IN SAFE HANDS.



NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

Contents

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

INTRODUCTION

Cyber security threats seek to target an organisation's most vulnerable points. As organisations focus on strengthening their own cyber security, their exposure to cyber threats in the supply chain is increasingly becoming the weakest point in their defences. Recent history has demonstrated many instances in which organisations were attacked through less-secure points in their supply chains, resulting in significant financial and reputational damage.

This guidance outlines three key phases in establishing an effective capability to manage supply chain cyber risk and improve organisational cyber resilience. Taking these steps will help you to **identify** supply chain entities and supplier management processes, **assess** the cyber threat landscape and determine which suppliers are most critical, and establish processes to effectively **manage** supply chain risk and continuously improve your organisation's cyber resilience.

Addressing supply chain cyber security risks requires coordination across the whole organisation.

Who is this guide for?

New Zealand's National Cyber Security Centre (NCSC) has produced this guidance for business leaders and cyber security professionals to better understand and manage the cyber risks in supply chains.

This guidance is designed for both government and non-government organisations of varying sizes and capabilities. It is not a complete framework, but provides an introduction to understanding and managing supply chain cyber risk. This guide accompanies the NCSC's *Charting Your Course* series of publications on **Cyber Security Governance**[1] and **Incident Management**.[2]

Terminology

- Supply Chain Risk Management (SCRM): A set of activities and practices undertaken by organisations to identify, assess and manage risk in their supply chains.
- ICT Supply Chain Risk Management (ICT-SCRM): An integral part of an organisation's SCRM strategy that addresses risks presented by ICT assets and services, and their producers, distributors, service providers, and other associated entities in the supply chain.
- Supply Chain Cyber Security: The practice of identifying, assessing and managing cyber security risks in the supply chain, encompassing technological and human risk factors.

1 https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance/

2 https://www.ncsc.govt.nz/guidance/incident-management/

Cyber security risks in supply chains

The range of supply chain entities that may present cyber security risks is not limited to those who provide information and communications technology (ICT) services or infrastructure: digital interaction with supply chain entities may occur from any part of an organisation. Supply chain cyber threats are therefore an organisation-wide challenge that requires a business-led response to manage the very real risks they pose.

To demonstrate this concept, suppose Company A decides to undertake a digital transformation project. Their marketing department engages a third-party service provider (a tier 1 supplier) to assist with the transformation. This service provider leverages a cloud-based customer platform (a tier 2 supplier) that is delivered as a service. As part of the transformation, all Company A's customer details are migrated into this cloud service. Unfortunately, the service provider (tier 1) fails to secure the administrative accounts they are using to configure the cloud platform (tier 2), and a malicious actor gains access using their accounts and extracts files containing Company A's customer details.

The service provider (tier 1) remains unaware that their administrative accounts have been compromised until Company A's marketing department is approached by a malicious cyber actor who demands a ransom to delete the customer data, or they will release it publicly.

In recent years, an increasing business reliance on supplier-managed cloud services in place of traditional on-premises enterprise software has highlighted the need for organisations to gain visibility of the direct and indirect suppliers present in their supply chains. Some suppliers require privileged systems access in order to manage services or equipment. Cloud services often necessitate extra applications and services to deploy, manage and secure them, which introduce additional supply chain providers.

Sophisticated and geographically interconnected manufacturing processes and services have also created hardware supply chains of rising complexity: for example, the production of a single hardware item may involve dozens of component manufacturers and subcontractors, some of which have several degrees of separation from the primary manufacturer.

> **"***Cyber security is never just a technology problem, it's a people, processes and knowledge problem.***" NIST**

Supply chain visibility barriers

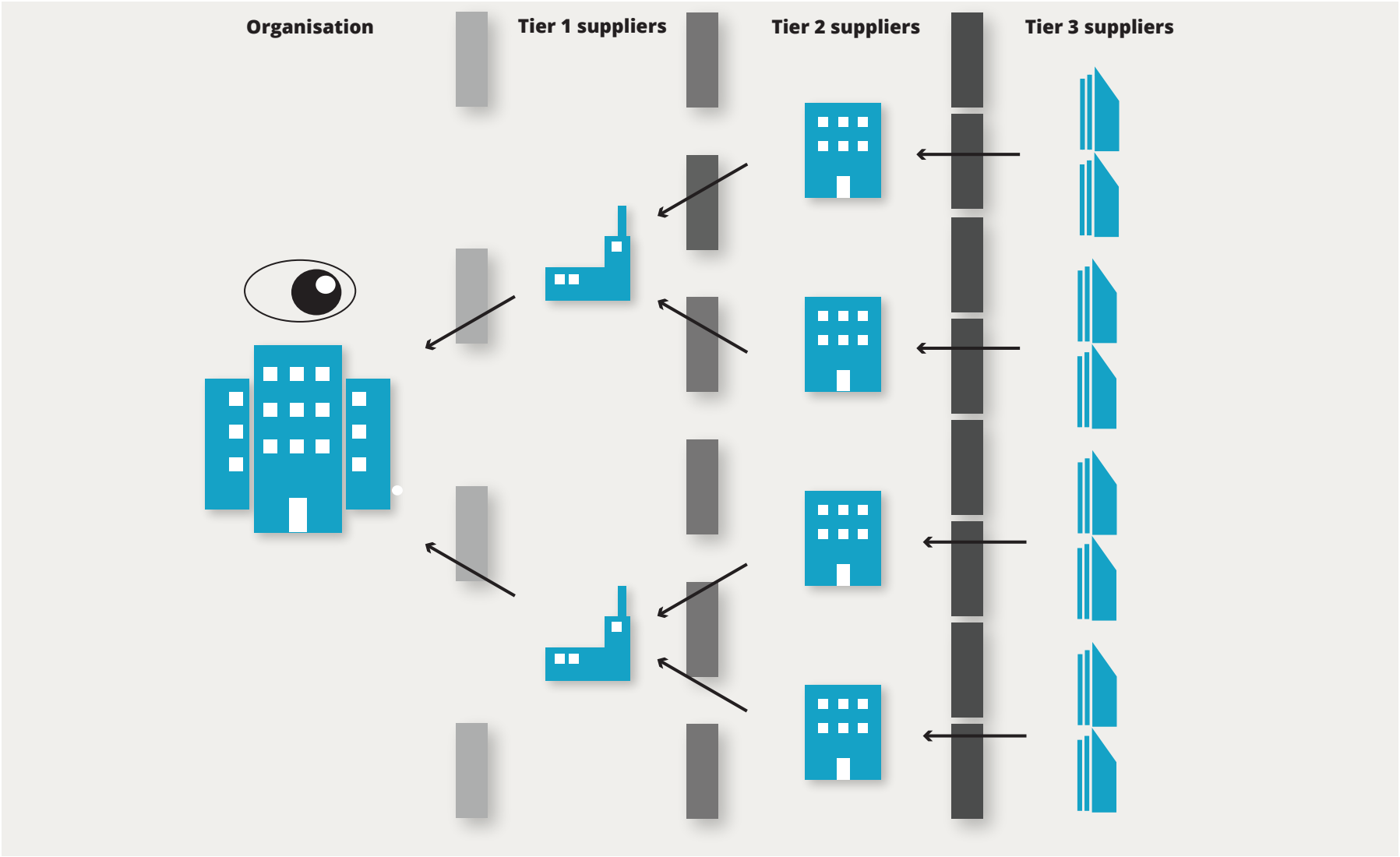


Figure 1: A typical organisation's visibility of its suppliers at successive degrees of separation.

Targeted and opportunistic attacks

Complex supply chains can create broad attack surfaces which present opportunities for malicious cyber actors. If an attacker's primary target is a large organisation with strong cyber defences, they may look for an alternative access path. This could be through a weakly defended service provider with access to the target's systems. Successfully infiltrating the weaker defences of the service provider could allow the attacker to circumvent the strong defences of their main target and cause extensive damage.

Targeted attacks often require significant preparation, but many other attacks are opportunistic and result from attackers undertaking broad sweeps of numerous organisations to identify vulnerabilities: for example, a malicious actor might conduct automated internet scanning that identifies a poorly defended supplier, then successfully attack that supplier and leverage their accesses into other organisations.

In this environment, it is important that organisations maintain a strong understanding of the cyber security risks in their supply chain and develop an effective programme to identify, assess and manage these risks.

> "Your investment in cyber security may not protect you if attackers can break in through a weak link in your supply chain."

Real-world examples of supply chain attacks

The cyber risks to supply chains can be readily demonstrated using real-world incidents. For example:

In **2019**, researchers discovered that malicious cyber actors had created a Trojanised alternate version of update utility software created by ASUS, a large multinational consumer electronics company. The alternate version contained malware but was signed with legitimate certificates and distributed to users on ASUS' own update platform. The goal of this attack was to target a small and specific set of ASUS customers, while ignoring all other users. The malware remained undetected for a significant period of time because it appeared to be genuine software hosted by ASUS.

A Trojan horse, or simply a Trojan, is a malicious programme designed to conceal its true intention. When users install a Trojan, it may perform harmful functions such as allowing backdoor access to their systems.

In **2020,** a novel form of malware called Octopus Scanner was discovered to have been targeting open source software repositories in the hosting platform Github. Octopus Scanner was programmed to seek out specific software projects and embed malicious code which, when executed, gave malicious cyber actors access to sensitive information in compromised machines. Most applications now include open source code, and the Octopus Scanner incident serves as an example of an increasing attack focus on open source code in the supply chain.

Also in **2020**, malicious cyber actors conducted a highly sophisticated supply chain attack that breached the systems of the software company SolarWinds and inserted malicious code that was distributed in software updates to SolarWinds' customers. The malicious code allowed the cyber actors to gain access to victims' systems and extract sensitive data. It was estimated that about 18,000 customers downloaded the compromised software, with follow-on activity by the cyber actors only occurring on a small number of networks. The attack caused significant financial and reputational damage.

PHASE ONE:

IDENTIFY

Identify your suppliers

Traditionally, suppliers that potentially carried cyber security risks would likely be evaluated by an organisation's IT department. However, many services now have information systems components that can introduce cyber security risks, and these services extend beyond the IT team's domain. The rapid global uptake of internet of things (IoT) devices and connected systems means that plant machinery, equipment, building systems, and physical security systems are often internet-connected and may even provide remote access as part of maintenance and servicing schedules. In addition, the consumption of cloud-based services has become simpler with free versions and credit card-based billing.

This makes it possible for any part of the organisation to use new cloud services without needing to seek technical or financial approval. These services can quickly become embedded in operational processes before they are discovered by the wider organisation. A process of fully identifying your suppliers therefore needs to systematically consider the entire organisation and should extend beyond ICT services and office-based systems.

The Centre for Internet Security, a non-profit organisation, maintains a recommended list of controls (the CIS 20)[3] designed to improve cyber security defences.

CIS Control 1 (Inventory and Control of Hardware Assets) states that organisations must identify hardware devices connected to their networks using an active discovery tool, and maintain an updated register of every asset that may have the capability to store or process information.

CIS Control 2 (Inventory and Control of Software Assets) states that organisations must use software inventory tools to automate the documentation of all software running on business systems, and utilise application allow-listing to permit only authorised software to run.

Applying these controls will assist you to gather information about what is running on your networks - an essential cyber hygiene practice that underpins all other cyber resilience efforts.

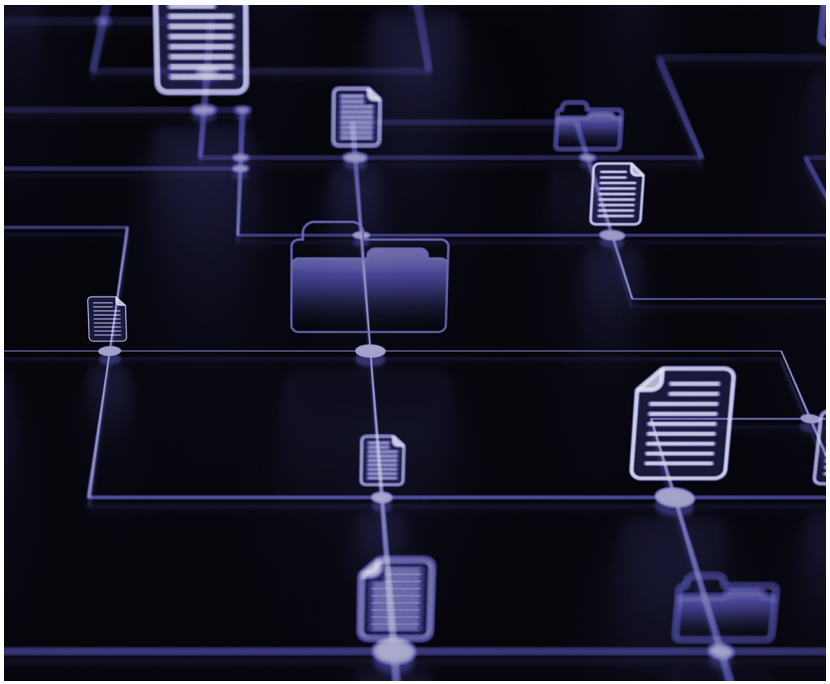
3 https://www.cisecurity.org/controls/cis-controls-list/

Understand your supplier management processes

Supplier management may be handled by different parts of the organisation including procurement, the legal and finance departments, specialist supplier relationship teams, or a combination of these. Organisations generally have business processes in place to establish new suppliers, manage relationships with existing suppliers, and provide visibility of purchasing decisions within the organisation. It is important to make these processes visible and incorporate cyber security teams in order for them to effectively assess new suppliers or consider significant changes in existing suppliers.

Additionally, there may be formal certification and accreditation processes within the organisation, or project management offices that conduct supplier engagement. In some cases, it may be necessary to engage with each of these business departments or units and establish an ongoing relationship.

The information gathered from the discovery process needs to be structured in a governance model that clearly identifies the roles and responsibilities for supplier management. This includes identifying the financial and technical authority for engaging new suppliers, as well as establishing ownership for ongoing supplier management. It is very important that every supplier has a clearly identified owner within the organisation. A RASCI[4] chart (this sets out who is Responsible, Accountable, Supporting, Consulted, and Informed in each activity) is a good mechanism to capture the key accountabilities and responsibilities, and this should include the role that cyber security teams play in supporting supplier management and being informed of any additions or changes in suppliers.



"Every supplier must have a clearly identified owner within the organisation."

4 https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf

Understand your suppliers' security measures

Maintaining visibility of your suppliers' security postures and clearly communicating your requirements to them are both important considerations, particularly for suppliers who are critical to your business. If you have certain expectations about the ways your information and assets should be managed and protected by external parties, or about the levels of protection and assurance required of products and services to be delivered, these should be clearly articulated and written into your contracts.

The New Zealand Protective Security Requirements (PSR[5]) includes 12 principles of supply chain security which describe the following measures in further detail. The PSR is suitable for both public and private sector organisations.

- Understand who your suppliers' own suppliers and contractors are. It may be necessary for you to have some visibility into multiple levels of the supply chain in order to have confidence in its security and integrity.
- Understand your suppliers' current security arrangements, including how long they have been in effect. Decide if you are willing to let your suppliers use their own subcontractors to fulfil your contractual obligations. Be aware of what access your suppliers grant to their own subcontractors, where it impacts your information and assets.
- Establish and clearly communicate the minimum security requirements you have for your suppliers. These requirements may extend beyond information security and into personnel and physical security. For example, you may require suppliers to conduct pre-employment checks to a certain standard in order to ensure that their staff are trustworthy and to reduce the risk of compromise by an insider.
- Consider the security implications for your organisation if a critical supplier experiences a change of ownership or major shareholding, or undergoes a merger. If this could impact their suitability, it may necessitate a security review of that supplier.
- Ensure your contracting processes include security considerations. This means supply chain and contract managers should work closely with senior information security staff to outline your security requirements at the tender development stage, and ask prospective suppliers to provide evidence that they can meet those requirements. Think about the consequences if a supplier becomes unable to continue meeting your requirements, or the contract must be terminated: do you have contract cancellation provisions? Do you have requirements for the return or disposal of your assets and information from that supplier?

5 https://www.protectivesecurity.govt.nz/governance/supply-chain-security/principles-of-supply-chain-security/

Identify your critical services and assets

To effectively manage the cyber risks in your supply chain, you must develop a clear understanding as to which of the assets and services (including third-party services) your organisation uses are most vital to your mission. When you know what is most in need of protection, you can begin to prioritise and allocate your limited resources accordingly. One way this can be achieved is by applying a process called a criticality analysis, which evaluates the potential harm to your organisation caused by failures, outages, or other disruptions to each of the assets and services you use. Evaluating criticality should be a continuous process, not a one-off event that occurs in the procurement phase. As a system ages, for example, it may become less essential to the mission, changing its criticality status.

A thorough criticality analysis model is described in NIST document 8179[6], however, organisations lacking the resources to apply this process may still be able to perform a less demanding analysis by creating a simple scorecard system or grid model to rank the criticality of assets and services. The output of this process should be a list of your organisation's significant ICT assets and services, who their suppliers are, and the relative importance to the organisation of each of them from an availability, confidentiality and integrity perspective. It's important that this process is undertaken in consultation with subject-matter experts and specialists from relevant parts of the business. Workshops are an efficient way to facilitate discussion.

During the course of this process, consider the following questions:

- Which services and assets (S&A) are most essential to the ongoing operations of your business?
- How serious would the consequences be if these S&A were taken offline or otherwise disabled?
- Which external parties would be impacted if these S&A were taken offline?
- Are any of these S&A a vital element of a broader system – a single point of failure?
- To what extent are primary S&A reliant on other secondary S&A for their continued operation?
- Do these S&A store any sensitive data, such as personally identifiable information? What would happen if this data were exposed by a third party?
- What is the estimated lifespan of your critical S&A? Does their security risk increase as their end-of-life approaches?
- Who has access to your most critical S&A? This could include permanent staff, contractors, and even suppliers. What level of access control do you have over these systems?

6 https://csrc.nist.gov/publications/detail/nistir/8179/final

PHASE TWO:

ASSESS

Determine which suppliers are the most critical

Suppliers present varying levels of risk to your organisation. Some have minimal access to your systems or an otherwise low risk potential and could be substituted without significant impact, while others provide mission-critical products or services that pose a high level of risk if compromised or interrupted. For example, Organisation A may be storing significant amounts of personal information on customers in a cloud service, while Organisation B uses the same service but does not keep any sensitive information in it, so the criticality and confidentiality requirements for the same service are quite different between the two organisations.

By reviewing your supplier lists and categorising them into levels of risk, you can formulate business continuity plans and arrange for contingencies in the event that a critical supplier is disrupted.

The level of analysis you choose to undertake in determining supplier criticality will be dependent on your resources. Organisations that are unable to perform detailed analyses should at the very least develop a consistent rating system they can use to assess suppliers based on their criticality. As a starting point, the following criteria can be used in this assessment:

- The level of access the supplier has to your organisation's systems, and the frequency of that access;
- The access the supplier has to your intellectual property, customer information, or other sensitive data;
- Whether the supplier could likely be used by a third party as a vector to attack or disrupt your business or customers;
- Your level of financial dependence on the supplier;
- The impact to your business and customers if the supplier experienced a major disruption;
- The time and cost in restoring or maintaining your business if you suddenly lost access to the supplier's products or services.

Collaborate with suppliers on cyber security

Developing strong, collaborative security relationships with your key suppliers can improve the flow of information and assist with coordination during a security incident. This approach can also improve your visibility into suppliers' organisations, giving you a better understanding of their security posture and helping to anticipate potential security problems before they become serious.

Supply chain risk should be viewed as a mutual concern between you and your suppliers. It's important that you listen to your suppliers' feedback, seek to address concerns they may have about your own security arrangements, and endeavour to provide support or information they require, where possible. Just as you may require security audits from your suppliers, you should equally be willing to submit to their audit requests and be as open as possible with providing information about any potentially impacting security issues you may currently be working through. If you have experienced a security incident, providing details of this to your suppliers may help them to prevent attacks on their own systems.

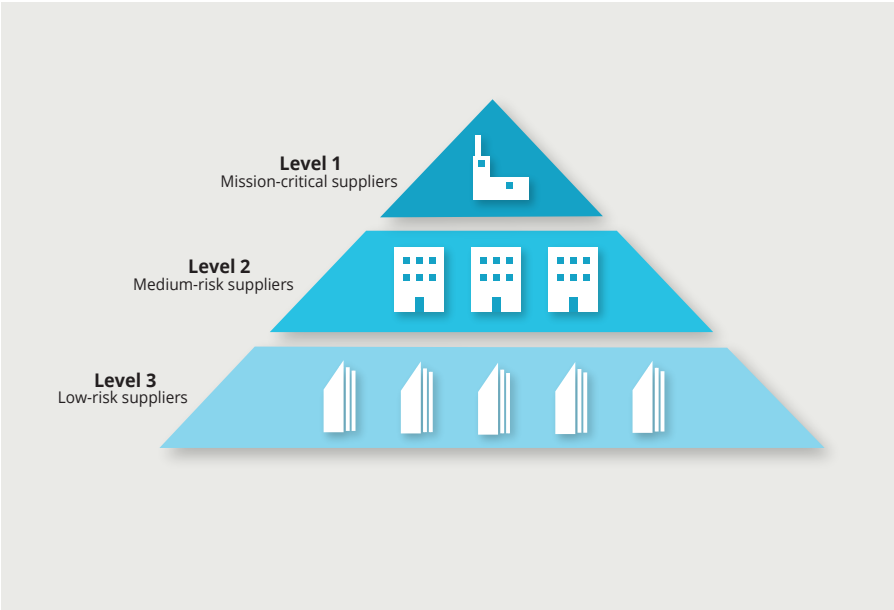


Figure 2: A typical organisation's suppliers sorted by criticality levels.

Understand the cyber security risks in your supply chain

When you have determined which of your assets and services are the most critical, you can begin to evaluate the risks your supply chain may present to each of them. For example, the use of cloud services could increase your potential exposure to denial-of-service attacks against an online system, or the use of a remote management service could increase the threat of compromised systems. Staff involved in supply chain management should have a strong awareness of cyber risks and keep up-to-date with recent security developments.

The NZISM states: Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately. (CID:3638)

Attacks on ICT infrastructure in supply chains have been increasing steadily in recent years. According to a 2020 report by Accenture, 40% of all security breaches now occur via weak links in the supply chain. As organisations increasingly move their systems into cloud environments and more staff work from remote locations, the threat is only likely to continue growing. It's therefore vitally important for organisations to develop a sound understanding of the potential risks from vendors, service providers, and end users present in their supply chains.

Supply chain risk comes in a variety of forms, including non-adversarial threats that can arise from an organisational weakness. Examples of supply chain cyber security concerns include the following:

- Malware is inserted into your systems via compromised software or code provided by a third party;
- A service provider is compromised, giving an attacker unauthorised access to your systems and data;
- An insider employed by a supply chain entity is able to access your systems to conduct malicious activity;
- Counterfeit or compromised hardware components are inserted into the supply chain;
- Poor quality-control in a software development or production process is exploited by a malicious actor;
- Systemic vulnerabilities are discovered (such as the discovery of the Spectre and Meltdown vulnerabilities in 2018);
- Virtual infrastructure is disrupted (for example during a DDoS attack).

Systematically evaluate and review supplier security

While procurement timelines may traditionally have involved considerations of a suppliers' cyber security practices towards the end of the sourcing process, in the contemporary business environment it's important that cyber security aspects are addressed at an early stage by the involved teams across the organisation. Cyber security should be a fundamental element of supplier selection, in the same way as pricing or delivery timeframes. The following practices, while not an exhaustive list, provide a useful set of guidelines for supplier selection and risk management:

- Collaborate internally on your security requirements. Produce your security requirements in consultation with impacted teams from across your business, including engineering and operations, as well as IT security. Ensure all relevant stakeholders have the opportunity to provide input.

- Ensure your security requirements are in writing. Clearly state your minimum security requirements for suppliers when drafting RFPs or contracts. Your requirements should be proportionate to the associated risk level of the contract. Where it's necessary, include provisions for exercising the right to audit the supplier's security, and for regular reports on security performance to be provided to you. Consider the security implications of allowing suppliers to use their own subcontractors.

- Develop a framework for prospective supplier cyber risk assessment. Performing diligence on suppliers will help to identify areas of concern at an early stage. Every organisation has a unique set of security requirements and a specific tolerance for risk, but a set of general cyber security risk indicators can be used to evaluate any supplier.

  These include their:
  - ◊ information security standards, controls and procedures;
  - ◊ malware protection and threat management systems;
  - ◊ identity and access management procedures;
  - ◊ audit and compliance procedures;
  - ◊ documentation standards;
  - ◊ data access controls;
  - ◊ data lifecycle management;
  - ◊ physical security procedures;
  - ◊ quality assurance procedures;
  - ◊ distribution channel security.
  - ◊ commitment to security assurance throughout a product's life cycle.

Determine the existing controls landscape

With an understanding of your organisation's key assets, the threats you face, and the impact that supplier relationships can have on threat levels, it is possible to determine the controls in place to help identify, protect, detect, respond, and recover from these threats. It is particularly important to consider how existing internal controls could be impacted by using a new supplier.

This should also include maintaining a clear understanding of any compliance requirements. In particular for international suppliers, it is important that New Zealand regulatory and compliance requirements are clearly identified and included in the controls framework.

PHASE THREE:

MANAGE

Establish a programme

Organisations should establish a programme for managing cyber risks in their supply chains that is appropriate to their size, staffing and other resources. Supply chain risk management (SCRM) programmes were once considered feasible only for the largest enterprises, but increasing cyber risks now require that all organisations should have a plan in place. While large enterprises may be capable of standing up a dedicated team for this purpose, smaller-scale organisations can still assign staff to perform supply chain cyber risk management duties as a part of their role.

Roles and responsibilities within a cyber risk management programme should be clearly defined: a simple way to accomplish this is by creating a RASCI chart.[7] The programme should not be run in isolation within a specific team or unit, but integrated within a broader organisational supply chain risk management programme.

The organisational supply chain cyber risk management programme should be supported by a framework that, depending on resources, may be either developed internally or based on an established set of standards and best practices. In some cases, it may be more efficient to integrate with existing risk management frameworks within the organisation rather than establishing separate processes which then need to also be maintained.

This could consist of aligning with the organisational processes using a common framework such as ISO 31000. Use of a standardised framework helps different teams across the organisation to identify, monitor and mitigate risks using a policy-based approach. The framework should also specify a standard set of security requirements for suppliers to meet before a business relationship can be established with them. For a list of government-recommended standards, refer to the New Zealand Information Security Manual (NZISM).[8]

> The NZISM states: Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process. (CID:3634)

7 https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf

8 https://www.nzism.gcsb.govt.nz/

Initiating the programme

The following first steps should be taken in establishing a formal supply chain cyber risk management programme:

- Gain approval at board level and involve senior leadership in setting up the programme. Ensure the leadership team is engaged with the programme by providing regular status updates, insights and recommendations.
- Establish a governance group to oversee supply chain cyber risk management functions, including representation from all relevant parts of the business.
- Ensure the programme's responsibilities are distributed throughout the organisation and extend beyond technology and procurement-focused units into all affected areas. Cross-functional teams can be used where necessary to address specific risks.
- Understand your organisation's cyber security posture. Examine your current procedures and determine which areas present the most immediate risks.
- Identify a senior staff member to take on the role of supply chain cyber risk manager. This person should have overall responsibility for managing the cyber risk component of the organisation's SCRM programme.
- Develop a standard set of policies and procedures that provide clear guidance to all parts of the business in how to undertake supply chain cyber risk management activities.

Your supply chain cyber risk management programme should include well-documented procedures for evaluating and periodically reviewing the security status and procedures of your supplier network. The level of detail you can achieve depends on the quantity of suppliers you are managing: where the number is very high, you may need to focus the most time and attention on a selection of suppliers you have judged to be most critical to your business.

Test and validate supplier performance

Effective supply chain risk management requires a combination of embedded processes and detection mechanisms. Any new suppliers, or any significant changes in the use of existing suppliers, should trigger assessment processes. Many suppliers offer additional services or capabilities that may not have been utilised at the outset of a contract. Gradual changes or extensions to services can introduce significant risks. These changes may include additional datasets being managed, or additional systems being accessed.

Mechanisms should also be put in place to detect potential performance problems with suppliers (such as a lack of timely reporting) or supplier security issues (such as data breaches). Given that some elements of supplier-provided services are not visible to customers, it is important to pay attention to any early warning signs of potentially more serious underlying issues.

All organisations should establish an ongoing cyber security programme as described in the NCSC publication *Charting Your Course: Cyber Security Governance*.[9] This programme should also take as inputs the identification and assessment of supply chain risks to ensure that controls are established, maintained, or improved in order to reduce the overall risk to the organisation.

9 https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance/

Define key reporting metrics

Supplier performance should be consistent from a cyber security perspective. To support this, key reporting metrics should be established, along with regular validation. Metrics should include measures that are appropriate to the supplier, such as incident response times, patching cycles, and maintenance schedules. Regular validation should be defined using an agreed schedule and based on the criticality of the supplier and the services they provide.

This could include a combination of regular testing, internal or external audits, self-assessment using questionnaires, or even participation in cyber security simulation events. For key suppliers, the validation must include testing the effectiveness of their operational processes to support the organisation, should there be a cyber security incident. The results of testing and validation should input into the supplier performance plan as well as guiding further investment in the organisation's cyber security programme.

Embed a culture of supply chain cyber risk awareness

Organisations should ensure that supply chain cyber risk awareness becomes embedded in their culture. This means setting an objective for all employees, not just those directly involved in SCRM, to have a good level of understanding about cyber security and managing cyber risk. Successful cyber attacks may be involuntarily enabled by non-technical staff in departments such as sales or finance, so it's important that cyber security is viewed as an organisation-wide responsibility and not one managed in isolation by the IT department.

As part of your organisation's efforts to embed supply chain risk awareness, consider taking the following steps:

- Make basic cyber security awareness training programmes compulsory for all staff. Security awareness must be raised before accountability can occur. Hold regular internal education sessions.
- Place an emphasis on positive recognition for staff who exemplify best practice: for example, by providing rewards and acknowledgement in internal communications.
- Make specialist training, such as professional certifications, available to staff with a supply chain risk focus and those in leadership positions.
- Involve key staff in industry-wide information-sharing events, including conferences, online forums, and special interest groups. Consider establishing such events if they are not already in place. Enable your staff to make external connections and build a security community.
- Ensure the organisation's risk tolerances are defined and accessible to relevant key staff. Mechanisms for reporting risk should also be well-understood.

Education programmes should be continuous: the cyber threat environment is constantly evolving, and staff must keep up-to-date with new developments.

An organisation with a strong culture of cyber security awareness will be less likely to experience serious incidents resulting from attacks that rely on poor security practices, such as data breaches caused by email phishing. This culture is also likely to assist key supply chain staff in making effective assessments of suppliers and improving their ability to identify potential risks in the supply chain.

Ensure ongoing monitoring and continuous improvement

The security of your supply chain must be monitored to identify, communicate and mitigate any status changes that could affect your organisation's exposure to risk. Your suppliers must be monitored for any changes that could affect the level of risk they present. Risk evaluations should not simply be one-off processes that are conducted only during the procurement phase; supplier risk must be regularly reviewed.

For example, transfer of a supplier's ownership may lead to significant changes in their internal systems and processes, or a disruption such as a natural disaster could also change the risk they present.

Suggested actions to ensure ongoing improvement in your supply chain security include:

- Schedule periodic reviews of your own critical systems and assets. Update your registers of systems and assets whenever there is a status change.
- Keep a current register of your suppliers and procurement decisions. Ensure the register is updated when changes occur.
- Regularly review the criticality status of each supplier.
- Require security information about your major suppliers' sub-contractors where this is possible.
- Keep a schedule for conducting regular security performance reviews of your suppliers, and record any status changes or deviations from their contractual obligations. These reviews should ideally be overseen by a group of stakeholders within your organisation.
- Encourage a flow of security information between you and your suppliers, and view supply chain security as a mutual concern.
- Communicate regularly with your suppliers on security issues, such as emerging cyber risks. Consider utilising technology solutions that streamline collaboration without elevating risk.
- Be open to receiving feedback from suppliers about your own security. Be willing to address any legitimate concerns they have about your security procedures.

SUMMARY

Addressing the cyber security risks in supply chains may appear to be a complex and daunting challenge, but organisations that take a systematic and collaborative approach will find themselves well-placed to mitigate threats, adapt quickly to changes in the business environment, and respond swiftly if an incident occurs.

Assessing the criticality of your organisation's information systems and assets will help you to understand which of these require the most resources allocated to their protection against supply chain threats. Identifying which suppliers provide your most vital assets and services will illuminate the areas of your supply chain that demand the most attention.

Evaluating the security posture of prospective suppliers during the procurement phase will provide you with vital information to support your decisions. Your security requirements and ongoing expectations should be agreed in writing. Maintaining open, collaborative relationships with suppliers will help to ensure security information flows both ways.

By actively monitoring the cyber threat landscape, evaluating threats against your own systems, assets and processes, and adjusting controls as necessary, your organisation is placed in a strong position to mitigate risks and direct your cyber security resources into the most vital areas.

Establishing a programme for managing supply chain cyber security risk and gaining buy-in from senior executives and board members will formalise and embed the process in a structured way. The programme should be integrated into the organisation's wider risk assessment procedures, with all affected areas involved in the risk management process.

Recognise that human factors, rather than technology alone, can often be the enablers of cyber incidents. Provide high-quality training and guidance to your staff, especially those in key positions, and reinforce a positive culture of cyber security awareness. Ensure that your organisational risk tolerances are well-defined and accessible.

Finally, maintaining a programme of continuous supply chain monitoring will help to ensure your records are not outdated 'snapshots in time' but living documents which can be relied on to provide current risk information and inform future procurement decisions. Constant, incremental improvements will efficiently strengthen your security procedures.

Useful resources

ACSC: Cyber Supply Chain Guidance

https://www.cyber.gov.au/acsc/government/cyber-supply-chain-guidance

Center for Internet Security: 20 Controls & Resources

https://www.cisecurity.org/controls/cis-controls-list/

CISA: ICT Supply Chain Risk Management

https://www.cisa.gov/supply-chain

CISA: Supply Chain Risk Management Fact Sheet

https://www.cisa.gov/publication/ict-scrm-fact-sheet

Centre for the Protection of National Infrastructure: Supply Chain Guidance

https://www.cpni.gov.uk/supply-chain

ISO 31000 – Risk Management

https://www.iso.org/iso-31000-risk-management.html

NCSC (UK): Supply Chain Security Guidance

https://www.ncsc.gov.uk/collection/supply-chain-security

NZISM: Supply Chain Security

https://www.nzism.gcsb.govt.nz/ism-document#3574

NIST: Best Practices in Cyber Supply Chain Risk Management

https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

PSR Governance: Supply Chain Security

https://www.protectivesecurity.govt.nz/governance/supply-chain-security/

For futher information visit: **www.ncsc.govt.nz**
or email: **info@ncsc.govt.nz**