Insight Space

cyber insights
programme

How to reduce supply chain risk

Executive Viewpoint

- Applying a risk-based approach
- Asking the right questions
- Five actions to reduce supply chain risk

Sam Thornton
Associate Director,
NCC Group

Global. Transformative. Resilient.

How to reduce supply chain risk

Working with suppliers is business-as-usual for most large organisations around the world.

According to our recent global survey of 1,400 cyber security decision makers, many plan to invest in new third-party software, hardware and SaaS products this year. These solutions can strengthen operations and increase efficiencies, but they can also increase organisations' cyber risk by providing new avenues for hackers to infiltrate their networks and systems.

Left unchecked, this risk can result in data loss, regulatory fines and reputational damage. Attacks on supply chains have increased by 51% in the last six months, so it's vital that organisations act to reduce their third-party risk now. In this article, we explain how businesses can combat these threats by adopting a risk-based approach to supplier management, and outline the questions that decision makers should ask of their suppliers to reduce third-party risk.

Sam Thornton
Associate Director,
NCC Group

51%

increase of attacks on supply chains in the last six months

Applying a risk-based approach

A risk-based approach requires organisations to understand the assets that are critical to their goals and objectives, where those assets are located across their people, process and technology, and the risks to the business if they were compromised.

As a result, decision makers can identify, manage and monitor the suppliers that support critical assets more effectively, and understand the potential threats and impacts on the business in the event of a supply chain attack.

For example, organisations can identify early warning signs for potential contractual failures by continually monitoring key suppliers and the levels of access they have to the network and applications. By doing so, they can identify any unusual behaviour that could indicate an attack on the supply chain, such as misconfiguration of access credentials, and respond accordingly.

Ultimately, a risk-based approach to supplier management forces organisations to pay attention to the data involved in supplier contracts and services. Armed with this knowledge, decision makers can develop a comprehensive supplier assurance program to protect that data as part of a wider risk management program.

Identify

Manage

Monitor

Asking the right questions

Taking responsibility for third-party cyber security is a key aspect of any supplier assurance program.

However, 53% of cyber security decision makers believe that they and their suppliers are equally responsible for the security of supply chains according to our research. Regulators are increasingly emphasizing the organisation's responsibility for supplier risk management, making it impossible for decision makers to outsource responsibility for a cyber attack.

> 53%
> of cyber security decision makers believe they and their suppliers are equally responsible for the security of supply chains

Do we know who our suppliers are?

This should include any sub-contractors involved, their approach to risk management and their commitment to following the organization's cyber security controls.

Do we know what our suppliers are doing?

Ask whether your organisation knows which assets are supported by third-party suppliers, how critical they are to the business, and the impacts if exploited.

How are we assessing and monitoring our suppliers?

One in three respondents told us that they do not regularly monitor and risk assess their suppliers' cyber security arrangements, putting them at increased risk of a third-party cyber attack. Ensure that you know when a supplier isn't compliant with a contract or service agreement, or isn't following defined security controls. Ask how often you assess and monitor suppliers, and confirm that contracts and service agreements include key performance indicators.

If an incident does occur, can we detect it and recover from it?

Are your incident response and business resiliency plans up to date? Have they been tested, are they looking at the right things (people, process, technology) and are they fit for purpose? If not, these should be addressed as priorities to mitigate supply chain risk.

Modern supply chains are complex and wide-reaching, so managing third-party risk can feel like a difficult task. In fact, only 32% of respondents to our survey were 'very confident' that they could respond quickly and effectively to a supply chain attack. However, by adopting a risk-based approach to supply chains, organisations can begin to reduce their third-party risk and work with suppliers in confidence.

Five actions to reduce supply chain risk

1. Understand what your business objectives and critical assets are, and which assets are supported by third parties.

2. Fully understand the services provided by suppliers and the value of any data, infrastructure, or platforms that they have access to.

3. Apply a risk-based approach to selecting and assessing suppliers, and ensure contracts include confidentiality clauses, appliable security and regulatory controls and key performance indicators.

4. Continually monitor supplier performance and adherence to contractual obligations, including their handling of any associated data.

5. Ensure business incident identity, response and resiliency plans are fit for purpose and regularly tested.

About NCC Group

NCC Group exists to make the world safer and more secure. As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 3,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how we can help you address legacy security issues to build your organisation's cyber resilience, speak to our team today.

www.nccgroup.com