Insight Space

cyber insights programme

nccgroup

Supply Chain Risk

A back door for hackers?

The rise of cyber security risks in company supply chains.

Market Research Report

Cyber security attacks on company supply chains have increased sharply in the past year, but there is confusion about whether companies or their suppliers are responsible for keeping supply lines secure.

Global. Transformative. Resilient.

Introduction

Supply chains around the world have been under severe strain in the past two years during the pandemic. Some experts have warned that shortages in global supply chains for things ranging from computer chips to alcohol and brown sugar could last for another two years.

For companies, the prolonged disruption to supply chains is creating cyber security problems as well as logistical ones. Last year, a security vulnerability known as Log4j in widely used open-source software vulnerability, highlighted the difficulty of keeping track of and fixing security problems in convoluted global supply chains.

Our latest research suggests that Log4j is far from an isolated incident. Cyber security attacks on company supply chains have increased by 51% in the past six months, according to our global survey of approximately 1,400 cyber-security decision makers at large companies in 11 countries including the UK, United States, China, Germany and Singapore.

Encouragingly, our respondents recognised third-party and supplier risk as one of their top three challenges for the next 6-12 months and plan to increase their security budgets this year. However, our research uncovered some glaring security issues around third-party risk, so it's crucial that organisations address these issues alongside any investment in security products and services.

Encouragingly, our respondents recognised third-party and supplier risk as one of their top three challenges for the next 6-12 months

51%

Cyber security attacks on company supply chains have increased by 51% in the past six months according to our global survey

> "Supply chains around the world have been under severe strain in the past two years during the pandemic. "

Supply chain confusion

Despite the severity of security risks to supply chains, there is confusion among companies about whether a company or its suppliers are responsible for keeping them secure.

Around one in three (36%) of respondents in our research said that they are more responsible for preventing, detecting and resolving supply chain attacks than their suppliers. Just over half (53%) said that their company and its suppliers are equally responsible for the security of supply chains.

This ambiguity could increase organisations' third-party risk if it means that they are not conducting the appropriate due diligence on their suppliers, and could expose them to regulatory penalties. The EU's Digital Operational Resilience Act (DORA) mandates that financial entities include key security requirements in their contracts with third parties, indicating that regulators across the globe are increasingly emphasising the organisation's role in supplier risk management.

Our research also highlighted room for improvement here: half (49%) of the organisations we surveyed said that they did not stipulate security standards that their suppliers must adhere to as part of their contracts. One in three (34%) said that they do not regularly monitor and risk assess their suppliers' cyber security arrangements, so there is a big opportunity for organisations to get ahead of the curve and tighten their supplier risk management now.

36%

of respondents said that they are more responsible for preventing, detecting and resolving supply chain attacks than their suppliers

A growing threat?

Supply chain attacks were one of the top three types of cyber attack to increase in the last 6 months, behind phishing and malware and attacks of operational technology. Concerningly, only one in three (32%) respondents were "very confident" that they could respond quickly and effectively to a supply chain attack.

Despite this gap between the rate of attacks and organisations' ability to deal with them, just one in four (24%) named third-party and supplier risk as a major cyber security challenge for the next six to 12 months. Many plan to invest in new third-party software, hardware and SaaS security products in 2022, which could further complicate organisations' supply chains and increase their attack surfaces.

32%

of respondents were "very confident" that they could respond quickly and effectively to a supply chain attack

Security challenges

The top challenges for organisations over the next 6–12 months are:

- Data privacy
- Understanding the threat landscape post Covid-19
- Finding a way to measure/report the effectiveness of cyber security and
- Third-party and supplier risk

When we asked decision-makers about their organisation's resilience against such threats, they presented a mixed picture. Six in ten (57%) said that they were "quite resilient" while one in three (34%) said that they were "very resilient."

34%

of decision-makers said their organisation's resilience was "very resilient."

33%

of decision-makers said that they could respond to a cyber attack within four hours.

Speed of response

Thirty-three per cent of decision-makers said that they could respond to a cyber attack within four hours, followed by 28% (one day), and one hour and one week (jointly at 14%). However, only one in three (34%) said that they were "very confident" that they could quickly identify the root cause of the breach, with the same percentage reporting that they were "very confident" they could fix the root cause to prevent it from happening again.

There is uncertainty about whether some companies would be able to meet regulatory requirements for information security and report a cyber breach to the relevant authorities, too. Forty-five per cent of respondents said they were "fairly confident" that they could report a data breach to authorities according to any local legal or regulatory obligations.

> "There is uncertainty about whether some companies would be able to meet regulatory requirements for information security and report a cyber breach to the relevant authorities."

Spending increases

After freezes and cuts to company IT security budgets during the last couple of years, budgets are set to rise again this year – by an average of 10%, according to our research.

Threat detection and response (32%), cyber security reviews and assessments (25%), security awareness and training (14%), training and testing (infrastructures and application) represent the top priority spend areas for our respondents in the next 6-12 months.

Meanwhile, managed security services (54%), off-premise cloud integrated security products (44%) and hardware-based third-party security products (42%) will see the largest proportional increases in budget.

10%

IT security budgets are set to rise again this year – by an average of 10%, according to our research.

RESEARCH SUMMARY

Cyber security attacks on company supply chains have increased by **51%** in the past six months, according to an NCC Group survey of approximately 1,400 cyber security decision makers at large companies in 11 countries, including the UK, United States, China, Germany and Singapore. The survey was conducted in December 2021 and January 2022.

Respondents said that they planned to increase their cyber security budgets by an average of **10%** in 2022.

One in three (**34%**) of companies surveyed said that they do not regularly monitor and risk assess their suppliers' cyber security arrangements.

Despite the severity of security risks to supply chains, there seems to be confusion among companies about whom – a company or its suppliers – is responsible for keeping them secure.

Priorities for cyber security investment this year include threat detection and response, cyber security reviews, security training and security testing.

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

UNI104675