Guide

Top 10 Questions about Supply Chain Cyber Risk for Executives & Directors

Quantifying the risk of third party provider breaches and downtime

Huntsman®
Defence-Grade Cyber Security

10 Questions about Supply Chain Cyber Risk

Understanding the business implications of a cyber breach or ransomware attack on a supply chain partner is increasingly important for senior executives and directors, and their organisations, and sits squarely within risk governance and business continuity responsibilities.

Supply chains are in the news right now demonstrating that any disruption to their delivery of goods and services for any reason, cyber or otherwise, is of concern. Current supply chain shortages are testament to the global "knock-on" nature of these risks.

In a world of digital interdependence, shared data, products and services and their supporting systems, an organisation's cyber security posture is only as good as that of its least secure supplier.

"Supply chains are in the news right now demonstrating that any disruption to their delivery of goods and services for any reason, cyber or otherwise, is of concern."

Managing the supply chain risk

Assessing the level of cyber security protection, control maturity and ransomware readiness within a number of independent third parties is a complex task. Organisations or departments might have many suppliers but typically only limited resources with which to assess the assurance of those suppliers.

> "A quick cyber security risk assessment is a practical way to gather some valuable insights into your current cyber maturity level."

As highlighted in the recent **Critical Technology Supply Chain Principles** published by the Australian Government, as reliance on technology has grown, organisations of all sizes need to shift from traditional habits and decision-making frameworks when considering supply chains, in order to grow resilience.

Cyber security has become a normal part of the board risk agenda, and in 2021 the sheer volume of attacks that have infiltrated organisations via their supply chains, has heightened their importance.

The vulnerability of many suppliers was highlighted during the pandemic when the disruption to goods and services was so critical that a number of business categories were re-classified to become part of the broader Critical Infrastructure sector.

Measuring to manage

Just as Boards and senior executives need ongoing visibility of their own cyber security posture, they also need an understanding of their supply chain cyber risks. The key to successful risk management within your supply chain is to be able to effectively assess and quantify the presence and extent of security controls and their level of effectiveness, with as little disruption to operations as possible.

Of course, there are various approaches to risk assessment, ranging from questionnaires through to full programmes of on-site audits. But the value of these, and the risks from suppliers in terms of the sensitivity of data they access and the criticality of the services or products they supply, often means making decisions that balance the fidelity of risk information and the effort used to derive it.

The more visible the measure of effectiveness of the security controls across the range of its suppliers, the greater the reliability of any overall security assessment for the organisation. Ransomware and its potentially damaging implications amplify the risks posed by suppliers.

Any assessment of the potential risks presented by a third-party supplier should consider the significance of the goods and services provided, the criticality of those components to operations, the nature of any data shared and the vulnerability of your organisation to a malicious attack emanating from that supplier.

Use these Questions to help better understand your organisation's supply chain risks of data theft, supply interruption, business disruption or reputational damage that could be caused by infection to or from a third party.

1	**Do you have an inventory of suppliers, subcontractors or even customers that includes those:** I. who share data, or you allow to access your data; and/or II. whose contribution of goods and services is critical to your ongoing operation?
2	**How reliant are you on your external providers for the security of your data?**
3	**Do you have digital or physical suppliers whose services to you could be disrupted by a ransomware attack affecting their systems?**
4	**Do you have alternate suppliers/contingency arrangements, if a cyber-attack caused a prolonged outage at a key/critical supplier or customer?**

The questions above will support security-by-design thinking, and form a starting point for identifying and understanding your supply chain and its participants and whether cyber security is in-built in your products or services and the supporting systems, or whether it has been retro-fitted and needs stronger integration.

5	**How do you validate a supplier's level of cyber resilience – do you have an agreed and effective mechanism to reliably assess the security of key/critical suppliers?**
6	**How transparent is your IT assurance process and how reliant is it on information provided by suppliers themselves?**

Questions 5 and 6 aim to prompt further consideration of supplier Transparency. Leadership needs to be aware of any cyber risks associated with the reliability of information from suppliers, in order to support staff to adjust or create processes that are more accurate and evident, at any point in time.

7	**With the known limitations of a number of well-known risk assessment methodologies, how do you assess and report the level of internal security, cyber hygiene and ransomware readiness of your suppliers relative to the services/products they provide to you?**
8	**Do you have a tested incident management plan, points of contact and experts available to assist in the event of a key supplier's security incident?**
9	**Is the security posture of your suppliers part of your continuous improvement and cyber risk management process?**
10	**How do you prioritise the level of risk of your suppliers – in terms of data involved, criticality of services, size, complexity – and what impact does this have on how you obtain assurance on cyber security safeguards?**

This last group of questions aims to support you to identify the true autonomy and integrity of your cyber security with third parties.

These questions are a starting point for Executives, Directors, Risk Sub-Committees and key team members needing to identify the true position of your organisation's supply chain risk, and how visible the controls and risk mitigation steps are for leadership.

Validating your cyber security controls and those of your key supply chain partners against an agreed and recognised cyber governance framework may be an important next step to formalising your procedures, as well as gathering significant intelligence about the maturity of your security, and ensure you take a systematic approach to including supply-chain thinking into your cyber risk frameworks.

Further information:
https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management

https://www.homeaffairs.gov.au/cyber-security-subsite/files/critical-technology-supply-chain-principles.pdf

Want to find out more?

Contact Us

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

About Huntsman Security

Huntsman Security's technology heritage lies in delivering cornerstone cyber security risk management, monitoring and response technology to some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman