Cyberfort
Expert-led. Security Driven.

Supply Chain Cyber Exposure Review

Rapid assessment of third-party cyber risk exposure

Introduction

Your organisation's security is only as strong as the weakest link in your supply chain, and right now, that chain has never been longer, more complex, or more exposed. The shift to outsourced services, cloud platforms, and specialist third-party providers has created a sprawling network of digital dependencies that most organisations cannot see clearly, let alone manage effectively.

Cyberfort's Supply Chain Cyber Exposure Review cuts through that complexity. In days, not months, we give you a clear, prioritised picture of where your third-party relationships are creating cyber risk, which suppliers represent your highest exposure, and exactly what to do about it. Because in a world where attackers routinely use your suppliers as the path of least resistance into your organisation, not knowing is not a defensible position.

What is the Supply Chain Security Situation organisations are facing?

You can't manage what you can't see. Most organisations have no consolidated view of which suppliers have access to their systems, what data they hold, or what security standards they actually operate to.

Supplier questionnaires are completed once, filed, and forgotten. The risk picture is static while the threat environment is not.

The volume of third-party relationships makes assessment feel impossible. A typical mid-sized organisation has dozens, sometimes hundreds of suppliers with some form of digital access or data-sharing relationship. Assessing them all with the same rigour applied to direct infrastructure is not feasible without a structured, risk-prioritised approach.

Contractual assurances are not the same as security assurances. A supplier's ISO 27001 certificate or GDPR data processing agreement tells you about their intent, not their actual security posture. Certification can be out of date, narrowly scoped, or simply not reflective of the controls that protect your specific data and systems.

Incident response plans rarely account for supplier failure. When a supplier is compromised, most organisations discover it from the supplier or from the news. They have no independent detection capability, no pre-agreed response playbook, and no clear picture of what data or access was at risk. By the time the full impact is understood, the window for containment has long passed.

Supply Chain Security in Focus

14%

The estimated number of organisations who have undertaken a formal security review of their supply chain in the last 12 months

UK Gov Cyber Security Breaches Survey 2025

30%

The number of data breaches related to third party security incidents

Verizon DBIR 2025

More than **75%**

of software supply chains were exposed to cyber attacks in the last twelve months.

Blackberry IT decision makers and cybersecurity leaders survey 2024

These numbers converge on a single reality: most organisations are significantly exposed through their suppliers, most are unaware of the specific nature of that exposure, and attackers know it. The risk has not crept up quietly; it has been exploited at scale while third-party risk management programmes have failed to keep pace.

What are the types of situations where a supply chain security review is needed?

Certain situations significantly elevate an organisation's supply chain cyber risk exposure or bring that risk into sharp focus for boards and insurers these generally include:

You are onboarding new suppliers or outsourcing functions for the first time; each new relationship is a potential entry point that needs to be assessed before it becomes embedded.

You are preparing for a regulatory audit or compliance review, whether that is NIS2, DORA, ISO 27001, or sector-specific regulation, demonstrating documented supply chain due diligence is now a baseline expectation.

You are going through a merger, acquisition, or divestiture, M&A activity brings inherited supplier relationships and unknown cyber exposure into scope overnight. Acquirers are increasingly held responsible for a target's supply chain posture.

You have recently experienced a security incident, whether or not a supplier was involved, a recent incident almost always prompts boards to ask hard questions about third-party exposure.

You are renewing cyber insurance or facing an insurance audit, insurers are tightening their requirements around third-party risk. Organisations that cannot demonstrate active supplier risk management face higher premiums or coverage gaps.

You are bidding for public sector or enterprise contracts; many procurement frameworks now require evidence of supply chain risk management as a condition of contract award.

Who is this service for?

This service is designed for senior leaders - **CEOs, CFOs, COOs, CISOs, and Risk Directors** in mid-market and enterprise organisations who rely on third-party suppliers, managed service providers, or outsourced functions that connect to their systems or handle their data.

It is particularly relevant for organisations operating in regulated sectors, bidding for public sector contracts, or facing scrutiny from insurers and enterprise customers over their supply chain risk posture.

If you have suppliers and you cannot clearly answer "which ones could take us down, and how would we know?" this review is for you.

What does a typical engagement for this service look like?

Our Supply Chain Cyber Exposure Review is designed to be fast, low-friction, and immediately actionable. A typical engagement runs as follows:

1

Step 1 - Scoping and Supplier Mapping

We work with your team to build a clear picture of your supplier landscape: who has access to your systems, what data they hold, and what existing governance is in place. This is a structured workshop and document review, not a lengthy audit.

2

Step 2 - Risk-Prioritised Assessment

Using a combination of technical analysis, open-source intelligence, and structured supplier evaluation, we assess your highest-risk supplier relationships against a consistent security framework. We focus effort where exposure is greatest.

3

Step 3 - Findings, Heatmap, and Roadmap

We present the full findings in an executive-ready format. Your Third-Party Risk Heatmap, Critical Supplier Review, Exposure Prioritisation Report, and 90-Day Roadmap, ready to go straight to your board, your insurer, or your auditor.

Business Value of this service

- Identify high-risk suppliers quickly
- Reduce exposure to third-party compromise
- Improve board visibility of supplier risk
- Support compliance and cyber insurance obligations

Key Deliverables of the Cyberfort Supply Chain Exposure Review Service

- Third-Party Risk Heatmap
- Critical Supplier Review
- Exposure Prioritisation Report
- Supplier Assessment Templates
- 90-Day Risk Reduction Roadmap

Key Outcomes from this service

Organisations that complete Cyberfort's Supply Chain Cyber Exposure Review leave with:

A Third-Party Risk Heatmap - A visual, board-ready view of your supplier landscape ranked by cyber risk exposure, so leadership can see at a glance where the concentration of risk sits and make informed prioritisation decisions.

A Critical Supplier Review - A deep-dive assessment of your highest-risk suppliers, examining their actual security posture, access privileges, data handling practices, and incident history - not just their paperwork.

An Exposure Prioritisation Report - A clear, risk-rated output that tells you which supplier relationships require immediate action, which require monitoring, and which are adequately managed, so your team is working on what matters most.

Supplier Assessment Templates - Practical, reusable tools that embed supply chain risk assessment into your procurement and vendor management processes going forward, so this becomes a durable capability, not a one-off exercise.

A 90-Day Risk Reduction Roadmap - A structured, actionable plan that takes you from current exposure to measurably improved supply chain security posture within a defined timeframe, with clear ownership and milestones.

The result is an organisation that has moved from blind trust in its supply chain to evidence-based assurance, with the board visibility and documented due diligence that regulators, insurers, and enterprise customers increasingly require.

How Cyberfort can help your organisation improve its supply chain security posture

Supply chain risk is not a procurement problem with a cyber dimension; it is a cyber problem that requires specialist expertise to assess and address.

Cyberfort brings the technical depth to evaluate supplier security posture beyond the surface level of certifications and questionnaires, combined with the commercial and regulatory awareness to frame findings in terms that resonate with boards, insurers, and auditors.

We work with organisations across financial services, professional services, engineering, government, and critical infrastructure, sectors where the consequences of a supply chain compromise extend well beyond the immediate incident into regulatory sanction, reputational damage, and loss of customer confidence.

We understand what good looks like in these environments, and we know how to close the gap between where our customers are and where they need to be.

Our delivery model is fast, structured, and designed to produce executive-ready outputs without consuming months of internal resource. This is not a theoretical risk framework exercise, it is a practical, expert-led assessment that gives you the intelligence to act, the tools to sustain improvement, and the evidence to demonstrate due diligence.

Your suppliers are part of your attack surface. We help you own it.

What our customers say about this service

"The heatmap alone was worth it. For the first time, our board could see the supply chain risk picture in a format they could actually engage with and make decisions from."

COO, Professional Services Firm

Next Steps

Book a 30-minute call with one of our supply chain security specialists to understand your current exposure and whether this review is right for you. There is no commitment, just a clear, honest conversation about where your risk sits and what it would take to address it.

Contact us at info@cyberfortgroup.com or call +44 (0)1304 814800 to arrange your call.

To find out more about our full range of cyber security services, visit cyberfortgroup.com

Cyberfort
Expert-led. Security Driven.

DATA SHEET