Cyber supply chain risk management under the Cyber Resilience Bill

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Most organisations in this era of hyper-connectivity have vast, intricate ecosystems of suppliers, software vendors, cloud providers, and digital partners. While this interconnectivity drives efficiency, innovation, and scalability, it simultaneously introduces cyber supply chain risk.

The supply chain is often the path of least resistance for sophisticated cyber criminals. By compromising a single trusted supplier who may have lower security defences, attackers can gain access to numerous high-value targets. This dynamic has transformed supply chain security into a business resilience imperative.

The upcoming UK Cyber Security & Resilience Bill represents a significant moment in cyber security legislation. It shifts the focus toward increasing systemic accountability across the entire digital supply chain. For UK businesses, effective cyber supply chain risk management is now a legal and operational necessity.

What is cyber supply chain risk management?

Cyber supply chain risk management (C-SCRM) is the process of identifying, assessing, and mitigating risks associated with the entire lifecycle of an organisation's supply chain for information technology (IT) and operational technology (OT) products and services. It encompasses software, hardware, cloud services, outsourced functions, and any third-party interaction that touches an organisation's data or systems.

Why does it matter now?

The priority on C-SCRM has been driven by the explosion of digital reliance and the evolution of the threat landscape.

Modern businesses rely heavily on specialised, external services. A typical enterprise might use hundreds of software-as-a-service (SaaS) tools, depend on multiple cloud infrastructure providers, and contract out functions, from payroll to managed IT support. While efficient, this reliance drastically expands an organisation's digital footprint, and therefore its attack surface.

Cyber criminals are acutely aware of this. High-profile incidents like the Jaguar Land Rover (JLR) production shutdown and the widespread Snowflake credential harvesting campaign have demonstrated how one successful supply chain breach can impact thousands of downstream organisations globally.

The Jaguar Land Rover (JLR) shutdown in August 2025 is cited as one of the most economically damaging cyber attacks in UK history, highlighting the fragility of the manufacturing sector. A sophisticated group known as Scattered Lapsus$ Hunters exploited a critical vulnerability in SAP NetWeaver, a common piece of third-party software used to manage JLR's global enterprise resources. JLR was forced to shut down its IT systems and halt global manufacturing for nearly five weeks.

In 2024, the Snowflake incident shifted the conversation from software vulnerabilities to identity vulnerabilities. Attackers used credentials stolen from third-party contractors and employees via malware. These accounts were vulnerable because they lacked Multi-Factor Authentication (MFA). By compromising these credentials, the threat actor (UNC5537) gained a skeleton key to the data of over 165 major organisations, including data exfiltration from AT&T, Ticketmaster and Santander bank.

These attacks are attractive to adversaries because they offer a high return on investment; a single compromise yields access to multiple targets, often with the high levels of privilege granted to a trusted supplier. If a critical supplier suffers a ransomware attack, your operations could be crippled. If a vendor mishandles your data, your organisation faces the regulatory penalties and reputational fallout. If a software provider delivers an update containing malware, your entire network is at risk.

This reality highlights why cyber supply chain risk management is a primary pillar of the upcoming legislation.

How the Cyber Security & Resilience Bill is increasing accountability

The proposed Bill is designed to address the systemic vulnerabilities of supply chains by strengthening the resilience of digital products. Critically, the Bill broadens the scope of responsibility, emphasising that organisations must be resilient not just within their own four walls, but throughout their operational network.

A central theme of the Bill is accountability. Historically, some organisations have adopted a compartmentalised approach to third-party services. The Bill challenges this directly.

Here's how:

Focus on resilience, not just compliance

The very title of the Bill emphasises cyber resilience. This means moving beyond passive compliance and focusing on an organisation's ability to anticipate, absorb, adapt to, and rapidly recover from cyber incidents affecting their supply chain. It requires proactive identification of vulnerabilities and the implementation of robust contingency plans.

Mandated security by design for products

The Bill targets digital products (hardware and software), enforcing essential security requirements throughout their lifecycle. For purchasing organisations, this means cyber supply chain risk management must begin with procurement. Organisations will be required to exercise greater due diligence to ensure the products they integrate meet these new, rigorous standards.

Incident readiness and reporting

A key element of the proposed legislation is the requirement for covered entities to have robust incident response plans that explicitly account for supply chain failures. This includes clear internal processes for when a key supplier is breached and mechanisms to ensure third-party partners provide timely notification of incidents that affect the organisation.

The Bill essentially formalises a concept that forward-thinking organisations have already recognised: outsourcing a service does not mean outsourcing the responsibility for that service's security. The Cyber Security & Resilience Bill mandates that organisations have high confidence in, and clear visibility of, the security posture of their suppliers, partners, and the products they deliver.

Key supply chain risk areas organisations must address

Successfully implementing cyber supply chain risk management requires practical application. The Bill, while providing the legal framework, requires organisations to deploy specific, effective controls.

Organisations should prioritise these five key areas:

1. Supplier risk assessments

Effective C-SCRM begins before a contract is signed. Suppliers should be tiered based on the criticality of the service they provide and the sensitivity of the data they access.

For high-risk suppliers, assessments must be thorough. Organisations should review vendor security policies, incident response plans, results of recent penetration tests, and compliance with industry standards, for example, Cyber Essentials Plus. The new Bill increases the need for organisations to verify that suppliers have integrated security throughout their product development lifecycle.

2. Access controls for third-party users

All external access to an organisation's network must be governed by the Principle of Least Privilege (PoLP).

If a contractor needs access to one specific database to perform their function, they must only have access to that database, and nothing else. Crucially, multi-factor authentication (MFA) must be mandated for all third-party access. Organisations must enforce their own, stringent access control protocols for everyone interacting with their systems.

3. Secure data sharing & system integration

The point where an organisation interacts with a supplier's system is often the weakest link. Risks arise when data flows through APIs, when systems are integrated without proper segmentation, or when data is shared without adequate encryption.

Cyber supply chain risk management requires that all data exchange is governed by clear security protocols. This means using strong encryption for data in transit and at rest, validating the security configuration of all integration points, and clearly defining where the organisation's data security responsibility ends and the supplier's begins.

4. Ongoing monitoring

Cyber risk is not static. A supplier that was secure during the procurement process may have been acquired or changed their technology months later.

Annual reviews are insufficient for true cyber supply chain risk management. Organisations must transition to ongoing monitoring. This can involve using security rating tools, tracking vendor security certifications, and regularly reviewing audit reports (like SOC 2 Type II). The goal is to detect a degradation in a supplier's security posture before it results in a breach that impacts your organisation.

5. Incident reporting and response coordination

When a supplier gets hit by a breach, the clock starts ticking for your organisation. Waiting 72 hours for notification from a supplier is often too long if your operations are interconnected.

Effective C-SCRM requires clear incident reporting requirements to be embedded in all supplier contracts. These provisions should mandate immediate notification of any security event that could impact the organisation's data or systems. Furthermore, incident response processes must be regularly tested and updated to include scenarios involving key third parties, ensuring both organisations know who to contact and how to coordinate when a crisis occurs.

Building a resilient supply chain

Achieving resilience in the supply chain is not a project with a defined endpoint; it is a fundamental shift in how an organisation operates. The dynamic nature of technology, partnerships, and the evolving threat landscape means that cyber supply chain risk management must be an ongoing, cyclical process.

To build a genuinely resilient supply chain that is compliant, organisations must:

- Manage supply chain risk throughout the entire relationship, from procurement, through contract negotiation and onboarding, to ongoing management and, crucially, termination and offboarding. (Ensuring data is removed and access is revoked when a contract ends is a critical and often overlooked part of the cycle).
- Make your security expectations legally binding. Standard clauses should cover data protection, access controls,

vulnerability disclosure, and incident reporting. The ability to audit vendors should be explicitly included for high-risk partners.
- Regularly conduct cyber security testing exercises that simulate a breach at a critical supplier. This tests not just technical controls but also communication channels, decision-making processes, and operational workarounds.

How Net-Defence supports cyber supply chain compliance

Navigating the complexities of cyber supply chain risk management while preparing for the strict accountability of the Cyber Security & Resilience Bill is a challenge for any organisation. Identifying every third-party vulnerability, implementing proportionate controls, and monitoring threats across a vast ecosystem requires specialised expertise, sophisticated tools, and strategic planning.

As specialists in cyber security and an experienced IT MSP, we help organisations manage their digital supply chain risks effectively. We guide businesses through the process of building resilient frameworks that secure their entire operational network.

We support organisations by:

- Gaining visibility into an organisation's digital supply chain, tiering suppliers by risk level and identifying hidden vulnerabilities in both legacy partners and new vendors.
- Designing and deploying robust, risk-based controls including clear access management policies, secure integration protocols, and data protection strategies.
- Helping organisations move towards a proactive security posture to allow for real-time threat detection.

Ensuring all cyber supply chain risk management frameworks are in line with evolving cyber security legislation.

The first step is ensuring organisations confront the reality of their interconnectedness. By treating cyber supply chain risk management as a priority, businesses build the fundamental resilience required to thrive in the complex, volatile digital landscape.

Contact Net-Defence today to learn how our comprehensive cyber security services can help you secure your supply chain and prepare for upcoming regulatory changes.