NET-DEFENCE

Understanding Your Legal Supply Chain: Why It Matters Now More Than Ever

Managed Service Offerings

- IT Support
- Business Resilience as a Service
- Cyber Certifications and Resilience
- Telephony and Communication

net-defence.com

Agenda

- What is supply chain risk?
- What does the Legal Sector SC include?
- Why does it matter?
- Real world examples

What is supply chain risk?

Supply chain risk refers to the potential for disruptions anywhere along the supply chain that can negatively affect the flow of goods, services, information, or finances.

It is anything that can go wrong in the process of getting a product or service from the supplier to the customer.

What is supply chain risk?

Common Sources of Supply Chain Risk
Supplier risks: bankruptcy, poor quality, delays, or single-source dependency
Operational risks: equipment failures, labour shortages, production errors
Logistics risks: transportation delays, port congestion, accidents
Demand risks: sudden changes in customer demand or inaccurate forecasting
Environmental risks: natural disasters, pandemics, extreme weather
Geopolitical risks: war, trade restrictions, tariffs, political instability
Cybersecurity risks: attacks on your systems that manage operations

Legal Sector SC – What does it include?

Core Professional Services Partners

These are partners directly involved in delivering legal services.

- Barristers / Chambers
- Expert witnesses
- Forensic specialists
- Legal process outsourcing (LPO) providers
- Document review and e-discovery teams
- Consultants providing specialist expertise (e.g., regulatory, financial, technical)

Legal Sector SC – What does it include?

<u>Technology Providers</u>

Technology is now one of the *largest* areas of the legal supply chain.

Software & Platforms

- Case and practice management systems
- Document management (DMS) & Knowledge management (KMS)
- e-Disclosure / e-Discovery tools
- Legal research platforms
- Contract lifecycle management systems
- HR & payroll software
- Finance, billing, and time-recording systems

Legal Sector SC – What does it include?

Technology Providers Continued

Infrastructure & Cloud

- Public cloud providers (Azure, AWS, Google Cloud)
- Private cloud & hosted desktop solutions
- Data centres and colocation providers
- VoIP, telephony and unified communications

Security & Protection

Security monitoring (SOC)

- Antivirus / EDR
- Email security / anti-phishing
- Multi-factor authentication providers
- Backup, DR and business continuity services

Legal Sector SC – What does it include?

Data & Information Providers

Handling data is central to legal work.

- Identity verification providers
- Credit, AML and sanctions check providers
- Client onboarding / KYC platforms
- Data enrichment and legal research data sources

Office, Facilities & Physical Services

Even with hybrid working, firms still rely on physical supply chains.

- Printers, scanning, and reprographics
- Postal, couriers, secure document transport
- Archiving and offsite record storage
- Shredding and destruction services
- Office furniture, stationery, consumables
- Facilities management and building maintenance

Legal Sector SC – What does it include?

Outsourced Operations

These operate in the background but are essential for day-to-day business.

- IT managed service providers (MSPs)
- Outsourced finance / cashiering
- HR and recruitment services
- Training and CPD providers
- Marketing and print design agencies

Client-Facing Support Services

Anything that forms part of the client delivery chain.

- Transcription and dictation services
- Translation companies
- Mediation or ADR services
- Court bundling and litigation support

Legal Sector SC – What does it include?

Risk, Governance & Compliance Providers

Given the regulatory environment (SRA, ICO, etc.), firms depend heavily on compliance suppliers.

- Cybersecurity consultants
- ISO auditors (27001, 9001, etc.)
- Cyber Essentials certification bodies
- GDPR, data protection advisers
- Legal practice auditors
- Professional indemnity insurance providers

Finance & Payments

Banks and financial service providers

- Merchant service providers
- Escrow services
- Pension providers

Why Supply Chain Risk Has Become Critical

- Regulatory Pressure (SRA Standards & Regulations)
- Professional Indemnity Insurance (PII) Expectations
- Data Protection & GDPR Accountability
- Spike in Vendor-Related Cyber Breaches
- Reputational & Client Trust Risk
- Operational Dependency (Hybrid & Digital Legal Practice)
- Emerging Additions (UK-Specific)

Why It Matters

Supply chain risks can lead to:

- increased costs
- stockouts or shortages
- missed deadlines
- reputational damage
- reduced customer satisfaction

Types of Risk

Inherent risk
An inherent risk is a type of vulnerability that will always exist within your supply chain, regardless of any actions you take.

Introduced risk
As the name suggests, this risk is introduced into your supply chain through various factors, such as human error, negligence, or malicious actions. These threats can originate from both internal and external sources.

Exploited risk
Exploited risk occurs when a vulnerability within your supply chain is actively leveraged by cybercriminals to launch an attack, compromising the confidentiality, integrity, or availability of critical systems and data.

Top 5 risks for Cyber originating in your supply chain

1. Third-party/vendor system breaches
Suppliers often have access to a company's networks, data, or systems. If a vendor is compromised, attackers can use that access as a back door into the main organisation.

2. Malware or compromised software updates
Cyber attackers can insert malicious code into software or firmware at any point in the supply chain. When companies install the update, they unknowingly introduce the threat (e.g., trojanized software builds).

3. Weak security practices at lower-tier suppliers
Smaller or distant suppliers may lack strong cybersecurity controls. Because supply chains have many tiers, a single weak link can expose the entire ecosystem.

4. Data leakage across interconnected systems
Supply chain partners often share sensitive data (designs, forecasts, credentials). Poor encryption, misconfigurations, or insecure file-sharing can lead to unauthorized access or leaks.

5. Ransomware disrupting operations
If a supplier or logistics provider is hit by ransomware, it can halt production, delay shipments, or shut down critical services—impacting the entire supply chain.

Real World Examples

CTS (Converge Technology Specialists) – 2023
A major supply-chain cyber-attack on CTS, an IT services provider serving 80–200 UK law firms, caused week-long outages and blocked access to critical PMS and case files for conveyancing and other legal practices.
Firms were unable to complete property transactions or access documents.

This is considered as the largest modern UK legal sector supply chain breach.

Allen & Overy – Ransomware Attack (2023)
Although not exclusively supply-chain, the ransomware incident highlighted dependency on third-party digital infrastructure and the risks from external IT support and cloud-based systems.

The LockBit group claimed responsibility.

Real World Examples

Sector-Wide Vendor Compromise Trends
According to multiple industry reports:
77% surge in cyber-attacks on UK law firms (2023-2024)
(Up from 538 to 954 breaches. A significant share were vendor-linked incidents where the attacker used a third-party system as the entry point)

62% of legal sector breaches involve third parties
(Referenced in supply-chain risk assessments)

SME Supplier Vulnerabilities (structural risk, not single incident)
Research shows that the majority of legal supply chain providers-IT, scanning, document management, outsourced support-are SMEs with weaker cyber controls, making them attractive supply-chain targets.

Though not a single attack, this identifies a systemic supply-chain threat vector for the sector.

Not all suppliers are created equally!

All suppliers are not equal. Focus on:

- What data they access
- How critical they are to operations
- Their own supply chain dependencies
- Their cyber maturity and ability to defend themselves
- Proportional due diligence based on risk

Not all suppliers are created equally!

Want to understand:

- How to perform a basic supplier risk assessment?
- Understand scoring, risk categories, and prioritisation?

Join us for webinar 2 –

“Assessing Supplier Risk : A practical workshop session”

Questions?

Secure your data.
Protect your business.
Defend against cyber threats.
Business resilience starts with us.

net-defence.com