cyber 39

# Digital Resilience in the Legal Sector

A GUIDE

thirty nine cyber

ASSESS. ADDRESS. **SUCCESS.**

HELP WHEN YOU NEED IT, NOT WHEN YOU DON'T.

# Cyber Risk Analysis: The Legal Sector

The legal sector operates in a uniquely exposed position — handling sensitive personal, commercial, and often high-stakes regulatory data on behalf of clients. Firms increasingly rely on digital systems, cloud platforms, and third-party services, making them prime targets for a range of cyber threats. Unlike general business disruptions, a successful cyber attack on a law firm can damage client trust, halt operations, and even trigger professional negligence claims. Below is an outline of key attack vectors and the specific risks they present.

## 1. Business Email Compromise (BEC)

Vector: Fraudsters spoof or compromise email accounts (typically partners or finance leads) to redirect payments or trick staff into sending client data.

Relevance: Law firms regularly process high-value transactions, disbursements, and retainers. BEC attacks exploit the trust placed in email instructions — particularly in property, litigation, and mergers.

Implication:

- Financial loss (often six figures)
- Breach of client confidentiality
- Professional indemnity exposure
- SRA or ICO regulatory scrutiny

## 2. Ransomware & Data Theft

Vector: Malware delivered through phishing emails or compromised supplier systems encrypts files and exfiltrates client data. Ransom demands are often made in cryptocurrency.

Relevance: Many firms still lack tested backup or recovery processes, and shared drive systems create broad attack surfaces.

Implication:

- Operational shutdown (delaying court or deal timelines)
- Client data exposure (e.g. case notes, evidence, contracts)
- Mandatory breach reporting (ICO and SRA)
- Reputational harm leading to lost business

The Likely Threat

The Likely Threat

## 3. Supply Chain Compromise

**Vector:** Attackers breach IT providers, chambers, or third-party legal platforms used by the firm. Credentials or data then cascade down.

**Relevance:** Increasing dependency on document portals, legaltech, outsourced support, and hybrid working tools exposes firms to external risks beyond their direct control.

**Implication:**

- Loss of control over sensitive case files
- Breach liability despite indirect attack
- Complex recovery and client re-assurance process
- Business interruption with no clear fault line

## 4. Insider Threat & Human Error

**Vector:** A member of staff (intentionally or not) sends files to the wrong party, opens phishing attachments, or mishandles credentials.

**Relevance:** High staff workloads, remote working, and the inherent sensitivity of legal content increase the risk of accidental or disgruntled misuse.

**Implication:**

- Data breach (especially in family, criminal or corporate cases)
- ICO fines or corrective orders
- Erosion of client trust
- Case integrity issues (e.g. admissibility of disclosed info)

The Likely Threat

### 5. Credential Stuffing & Cloud Account Takeover

**Vector:** Re-used passwords or weak credentials are exploited to access document management systems (e.g. iManage, NetDocuments), email or file-sharing platforms.

**Relevance:** With remote access and cloud usage on the rise, attackers exploit poorly configured systems or shared passwords.

**Implication:**

- Silent access to confidential client records
- Evidence tampering or surveillance without detection
- Delayed discovery and complex forensic investigation
- Reputation damage if case strategy or materials leak

## Conclusion

The legal sector's exposure to cyber risk is amplified by the value of the data held, the duty of confidentiality owed to clients, and the operational impact of disruption. Attackers know that firms are often under time pressure, reliant on trust and digital communication, and bound by professional obligations, making them ideal targets.

Investment in cyber awareness, incident response planning, and resilience maturity is no longer optional. It is an operational necessity, not only to protect the firm, but to preserve client confidence and professional credibility.

Tips to Improve Resilience

## Cyber Resilience Advice for Law Firms

At ThirtyNine, we understand that law firms sit at the crossroads of confidentiality, trust, and time-critical operations. Based on the most common attack vectors in the sector — and the pressures firms face — our advice is built around one goal: keeping your digital operations confident and continuous, even in a crisis.

## Here's our practical guidance for each of the key cyber risks outlined:

### Business Email Compromise (BEC)

- Enforce multi-factor authentication (MFA) across all email accounts — no exceptions
- Implement email filtering and impersonation protection (e.g. DMARC, SPF, DKIM, anti-spoofing rules)
- Raise awareness among finance and partner-level staff with realistic simulations and scenario-based learning
- Establish dual-control protocols for financial transactions and sensitive requests
- Include BEC scenarios in your incident response plan and rehearsals

### Ransomware & Data Theft

- Ensure frequent, offline backups with routine recovery testing
- Map and segment your internal systems — especially shared drives and legacy applications
- Use least privilege access controls for documents and file systems
- Conduct endpoint detection and response (EDR) deployment and log correlation to spot unusual access
- Run tabletop exercises simulating ransomware on a case management system or during litigation deadlines

Tips to Improve Resilience

## Here’s our practical guidance for each of the key cyber risks outlined:

### Supply Chain Compromise

- Identify and categorise all suppliers — including legaltech, IT support, cloud platforms, and chambers
- Send due diligence questionnaires or review basic security documentation for Tier 1 suppliers
- Ensure your contracts include data protection, breach notification, and security responsibilities
- Have a process for revoking access to systems and document platforms if a supplier is compromised
- Include third-party dependencies in your resilience maturity assessment

### Insider Threat & Human Error

- Make cyber awareness part of your firm’s culture, not just a compliance exercise
- Provide targeted training for specific roles (e.g. partners, PAs, juniors)
- Monitor for data transfers, forwarding, and unusual logins, especially after resignation or conflict
- Implement role-based access controls — people only access what they need, no more
- Encourage an open reporting culture: mistakes must be surfaced quickly, not hidden

### Credential Stuffing & Cloud Account Takeover

- Ban password reuse — and implement MFA on all remote access tools
- Audit and securely configure all client portals, document systems, and collaboration tools
- Invest in password managers and modern identity tools to help users do the right thing easily
- Monitor cloud logs and access locations for signs of credential misuse
- Regularly review permissions and dormant accounts — particularly after staff departures

## ThirtyNine's Approach

We don't believe in tick-box exercises or off-the-shelf advice. Our Digital Resilience Maturity Assessment is framework-based but tailored to how your firm works — your systems, your people, your pressure points.

### We assess across five core areas:

- Governance & accountability
- User behaviour and awareness
- Technology controls
- Supply chain security
- Incident response capability

### The output?

A clear, prioritised roadmap showing where you are, where the risk sits, and what to do next — whether you're a small boutique or a multi-office practice.

Want to know more?
Book an appointment here

cyber

39