RISK LEDGER

# Under Pressure:

## How Law Firms Can Meet Rising Client Cyber & Resilience Demands

A Risk Ledger Special Report

# Contents

# About this Report

The Under Pressure report focuses on the legal sector's shift from manual, "tick-box" compliance toward a proactive model of collaborative supply chain cyber defence. Risk Ledger is driving this evolution by building a dedicated community of firms through targeted webinars and thought leadership, replacing outdated processes with real-time, shared intelligence that addresses complex 4th and nth-party risks.

We are specifically supporting Mills & Reeve as they harden their supply chain security and lead the industry in client-focused resilience. By leveraging our platform to map supplier relationships and manage assessments at scale, Mills & Reeve has achieved continuous visibility and external attack surface monitoring, ensuring their digital ecosystem remains a reinforced shield rather than a hidden vulnerability.

# About Risk Ledger

Risk Ledger was founded in 2018 by Haydn Brooks and Daniel Saul with a mission to shift the way organisations approach cyber security and risk management in the supply chain by building a global network of connected organisations.

Today, Risk Ledger is the cutting-edge Third Party Risk Management (TPRM) platform, dedicated to transforming supply chain security. We empower security and procurement teams to Defend-as-One, visualising their entire supply chain in real-time and providing unmatched transparency and collaboration. Our platform offers comprehensive, continuously updated risk assessments that reduce compliance burdens and enhance your organisation's cyber defences. By visualising and managing every link in your supply chain, Risk Ledger ensures you are always one step ahead of emerging threats.

Our commitment to asking the right questions and working closely with industry experts allows us to build a more secure, resilient future for all. With our Defend-as-One approach, we strengthen your organisation's ability to detect, respond to, and prevent cyber attacks. Risk Ledger isn't just about managing risk—it's about fortifying your entire supply chain because every link matters in cyber security. We're here to help you secure today's operations and safeguard tomorrow's reputation, creating a safer digital landscape for all.

**Risk Ledger Ltd.**
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

**Company registration number (England & Wales):** 10831970

**Contact**: www.riskledger.com | marketing@riskledger.com | +44 1234 567890

# Executive Summary

In 2026, the UK legal sector sits at a high-stakes crossroads where the "currency of trust" is no longer implicit but strictly codified. As sophisticated clients in Critical National Infrastructure (CNI)—spanning finance, energy, and government—face tightening regulations like NIS2, DORA, and the Cyber Security and Resilience Bill, they are increasingly viewing their legal partners as extensions of their own attack surface.

This report, Under Pressure, explores how firms are moving beyond the administrative fatigue of legacy "tick-box" compliance to embrace a model of continuous monitoring and deep-tier supply chain mapping. At Risk Ledger, we are fostering a community of law firms—supported by forward-thinking practitioners like Mills & Reeve—to trade isolated, manual assessments for real-time risk insights and a "Defend-as-One" strategy that secures the entire legal ecosystem.

## Key Findings & Industry Shifts

- **Flow-Down of CNI Regulatory Obligations:** High-profile clients are now legally mandated to include "supply chain security" within their core risk management. Consequently, they are transferring these stringent obligations directly onto their law firms, requiring firms to harden their own supply chains as a condition of instruction.
- **The Invisible "Nth-Party" Threat:** Most firms possess almost zero visibility into the "long tail" of 4th and nth-party risks—the subcontractors and service providers that their own suppliers rely on. Without mapping these deep dependencies, firms remain exposed to hidden concentration risks and single points of failure that can disrupt client services.
- **The Decay of Traditional TPRM:** Legacy "point-in-time" assessments and annual spreadsheets have reached a breaking point. These snapshots could be out of date almost immediately, leaving firms "looking in the rearview mirror" and identifying risks only after they have potentially been exploited.
- **A Shift to Collective Defence:** The industry is moving away from a culture of historical secrecy toward one of greater collaboration. By pooling intelligence on a shared network of suppliers, a threat identified by one firm becomes a lesson learned for all, raising the "security floor" for the entire profession.
- **Efficiency Through Standardisation:** Moving toward standardised, platform-based assessments eliminates the "questionnaire loop" for both firms and suppliers. This allows security teams to redirect their talent from administrative "chasing" toward high-value strategic resilience planning.

# Introduction: The New Frontier of Legal Resilience

For the modern UK law firm, the traditional boundaries of the office and the private network have dissolved. In their place is a complex, high-stakes digital ecosystem where a firm's security is only as strong as the most obscure subcontractor in its supply chain. As we move through 2026, the legal sector finds itself at a critical juncture: client expectations for cyber security assurance are no longer focused solely on the firm itself, but are escalating to include 4th and nth party risks—the suppliers of your own suppliers.

This shift is particularly pronounced for legal firms due to the sensitive nature of the data they manage on behalf of their clients. Regulators and sophisticated clients in finance, energy, and government now view legal partners as an extension of their own attack surface, transferring their own stringent regulatory obligations—such as NIS2 and DORA—directly onto their law firms.

The "tick-box" compliance of the past is failing. Traditional Third-Party Risk Management (TPRM) models are no longer fit for purpose because they rely on manual, point-in-time assessments that cannot keep pace with an evolving threat landscape. These legacy processes often result in "supplier sprawl," where thousands of vendors must be managed with limited visibility across their own external dependencies.

This report explores how the legal sector can move away from isolated, resource-heavy processes toward a model of collaborative cyber defence. By leveraging shared intelligence and community-based risk management, enabled by new tools and approaches to TPRM like Risk Ledger's, firms can replace static questionnaires with real-time visibility. This shift transforms third-party risk from a duplicated administrative burden into a proactive, scalable, and mutually reinforced shield for the entire profession.

# 1. Rising Cyber Expectations in Legal Services

The legal industry has long operated on a foundation of implicit trust, but in 2026, that trust is being codified into rigorous technical and regulatory demands. Clients no longer view their law firms as isolated silos; they see them as critical, and often vulnerable, nodes within their own digital supply chains.

## Client-Driven Compliance Escalation

The most significant pressure is coming from clients in highly regulated sectors—finance, energy, and government—who are actively transferring their own regulatory burdens onto their legal counsel. This "flow-down" of obligation is primarily driven by:

- **NIS2 & DORA:** These mandates require essential and important entities to include "supply chain security" within their core risk-management processes.
- **Operational Resilience:** Clients are now obligated to map their "important business services," which frequently include the legal advice and data handling provided by their law firms.
- **Audit Rights:** Firms are increasingly facing demands for "right to audit" clauses that extend beyond the firm itself to include 4th-party suppliers, such as cloud storage providers or AI-driven transcription services.

## From Assurance to Partnership: The Maturity Shift

The era of the annual security questionnaire is ending. Clients now expect law firms to demonstrate continuous security maturity rather than providing a single, static snapshot of their defences. This means moving from a reactive "tick-box" exercise to a proactive partnership where firms provide:

- **Real-Time Evidence:** Proving that security controls like MFA and endpoint protection are active and effective 24/7.
- **Supply Chain Transparency:** Disclosing not just the firm's own posture, but the security standards of the subcontractors they rely on to deliver client services.

# Transformation of "Good": Defining the 2026 Posture

In 2026, a "good" cyber posture is defined by resilience and transparency rather than just the absence of a breach. Leading firms are now measured against several key pillars:

- **Continuous Monitoring:** The ability to detect and contain threats within hours, supported by auditable reporting that proves regulatory hygiene.
- **Integrated Resilience Planning:** Moving beyond basic backups to rehearsed incident response plans that minimise client disruption.
- **Zero Trust Architecture:** A shift away from broad network access toward identity-verified, matter-level encryption and segmented access.

Ultimately, for the UK legal sector, cyber security is no longer just an IT overhead, but is turning into a competitive differentiator and a fundamental requirement for maintaining the "currency of trust" in a hyper-connected market.

# 2. The Legal Industry's Internal Challenges

While the external pressure from regulators and clients is clear, the UK legal sector faces a unique set of internal "friction points" that make modernising risk management particularly difficult. In 2026, many firms are discovering that their greatest vulnerabilities are not just technical, but structural and cultural.

## The Evolution of Partner-Led Governance

The partner-led governance model is a defining strength of the legal profession, ensuring that client interests and risk management remain at the heart of the firm's operations. While this decentralised structure has historically focused on practice-specific excellence, it also offers a powerful foundation for a more nuanced approach to cyber security. By leveraging the deep involvement of partners, firms can move away from a "one-size-fits-all" IT policy and toward a sophisticated, risk-aware culture where security is championed at the highest level of every practice group.

This model provides a unique opportunity to turn traditional challenges into strategic advantages:

- **From Siloed Budgets to Targeted Investment:** Rather than seeing disparate practice systems as a hurdle, firms are beginning to use the partner's influence to ensure that security investments are precisely tailored to the specific risk profiles of their most sensitive matters.
- **Decisive Leadership in Remediation:** The direct involvement of the partnership means that once a security mandate is unified at the board level, the path to implementation can be swift and comprehensive. When partners view cyber resilience as a core component of client service, the speed of policy adoption moves from a process of "approval" to a mission of "shared protection."
- **Cultivating a Culture of Vigilance:** The historical culture of discretion and meticulousness inherent in the partnership is the ideal breeding ground for a modern security mindset. By evolving this "historical secrecy" into a proactive "shared defence," partners can lead the charge in establishing the UK legal sector as the global gold standard for digital trust.

## The Scale of Supplier Sprawl

The modern law firm sits at the centre of a massive web of external dependencies. From case management platforms and document repositories to niche transcription services and AI-driven legal tech, the average firm now has to manage hundreds, if not thousands, of third-party relationships.

- **The Visibility Gap:** Most firms only have a surface-level understanding of their direct (3rd party) suppliers but possess almost zero visibility into the "long tail" of 4th and nth party risks, the subcontractors and suppliers that those suppliers rely on themselves.
- **Concentration Risk:** Without a clear map of these dependencies, firms are often unaware that many of their "different" suppliers may all rely on the same underlying cloud infrastructure or software library, creating potential hidden single points of failure.

## Skills, Budget, and Cultural Barriers

Compounding these structural issues is a persistent shortage of specialised cyber talent within the legal operations space.

- **The Talent War:** Law firms are competing with the financial and tech sectors for a limited pool of security experts, often resulting in small, overstretched internal teams.
- **The "Secrecy Trap":** Historically, the legal profession has thrived on a culture of confidentiality and competition. However, this same culture can hinder the open information sharing and collaboration required for modern, community-based defence.
- **The Compliance Paradox:** Many firms still treat cyber security as a "tick-box" compliance exercise rather than a dynamic operational risk, leading to an over-reliance on static, annual audits that are outdated the moment they are completed.

In 2026, the firms that manage to successfully navigate these challenges are those that recognise security is not an IT problem to be "solved," but a core business discipline that requires leadership, transparency, and a shift toward collective resilience.

# 3. Why Traditional TPRM Fails

The legal sector's reliance on traditional Third-Party Risk Management (TPRM) has reached a breaking point. While these methods were designed to provide a baseline of trust, they have become an exercise in managing paperwork rather than managing risk. In the fast-moving threat landscape of 2026, the flaws in the legacy "due diligence" model are now systemic risks in their own right.

## The Point-in-Time Fallacy

The most glaring weakness of traditional TPRM is its static nature. Due diligence questionnaires and annual audits offer only a "snapshot" of a supplier's security posture at a single moment in time.

- **Decay of Data:** A security assessment completed in January is often obsolete by March as new vulnerabilities emerge and supplier environments change.
- **Reactive Stance:** Because these assessments are periodic, firms are essentially "looking in the rearview mirror," identifying risks only after they have potentially been exploited.

> Firms are "looking in the rearview mirror,"

## Manual Overload and Resource Inefficiency

Traditional TPRM is a labour-intensive process that scales poorly. Security and compliance teams often find themselves trapped in a cycle of administrative "chasing".

- **Chasing Paperwork:** Significant man-hours are spent emailing spreadsheets, following up on incomplete answers, and manually verifying evidence.
- **The "Compliance Ceiling":** As a firm's supplier list grows, the team's ability to perform deep-dive analysis shrinks. Quality is often sacrificed for quantity just to meet audit quotas.

## The Duplication of Effort

The current model is equally burdensome for suppliers. A single software provider serving fifty different law firms will likely have to answer fifty near-identical security questionnaires.

- **Questionnaire Fatigue:** Suppliers, overwhelmed by repetitive requests, may provide generic or "copy-paste" answers that lack the depth required for genuine risk assessment.
- **Wasted Intelligence:** Each law firm conducts its assessment in a silo. If five firms identify a critical vulnerability in a shared supplier, there is currently no mechanism to pool that intelligence, leaving the rest of the sector blind to the threat.

## Scalability Limits and the Visibility Gap

As law firms embrace digital transformation, the number of third and fourth-party relationships grows exponentially.

- **Loss of Control:** Traditional methods cannot track the "nth party" chain. If a firm's primary supplier outsources its data processing, the firm rarely has a mechanism to audit that sub-processor with any degree of rigour.
- **Automation Deficit:** Without a unified platform, automation remains fragmented. Firms are unable to trigger real-time alerts or institute automated remediation workflows across their entire ecosystem.

Ultimately, traditional TPRM has become a "tick-box" exercise that provides a false sense of security while consuming vast amounts of professional time. To meet the standards of 2026, the legal sector must move beyond the spreadsheet and toward a model defined by real-time, collective intelligence.

# 4. Rethinking TPRM as Collaborative Cyber Defence

The limitations of the legacy model necessitate a fundamental shift in how the legal sector approaches security. Instead of treating risk as a private burden to be managed in isolation, firms are moving toward a model of collaborative cyber defence. This approach recognises that in a hyper-connected digital economy, the security of the individual firm is inextricably linked to the security of the collective legal ecosystem.

## The Network Effect: Intelligence at Scale

When law firms and their suppliers operate on a shared platform, the traditional "one-to-one" assessment model is replaced by a "many-to-many" network. This creates a network effect where risk intelligence is pooled and mutually reinforced.

- **Mutual Assurance:** When a supplier updates their security profile or remediates a vulnerability, that information is instantly available to every firm they serve.
- **Collective Visibility:** The network provides a "bird's-eye view" of the supply chain, allowing firms to see beyond their direct 3rd parties and into the 4th and nth party dependencies that were previously invisible.

> "Risk intelligence is pooled and mutually reinforced."

## Real-Time Visibility Over Static Snapshots

The shift from "point-in-time" to "continuous monitoring" is the hallmark of collaborative defence. Rather than waiting for an annual audit, firms benefit from:

- **Live Data Streams:** Continuous data-sharing replaces the static questionnaire, providing a real-time pulse of a supplier's security maturity.
- **Automated Alerts:** If a supplier's posture changes—or if a breach is detected within the network—alerts are triggered instantly across all connected firms, enabling rapid, coordinated responses.

## Efficiency and the End of Duplication

Collaborative defence solves the problem of resource drain by eliminating the "questionnaire loop."

- **The "Assess Once, Share Many" Principle:** A supplier completes a single, comprehensive assessment on the Risk Ledger platform, which is then shared with all their legal clients.
- **Redirecting Talent:** By automating the administrative "chase," security teams can shift their focus from chasing spreadsheets to high-value risk mitigation and strategic resilience planning.

## From "Tick-Box" to Shared Defence

Perhaps the most significant change is cultural. Collaboration replaces the historical secrecy of the legal profession, turning isolated efforts into a proactive community security posture.

- **Sectoral Resilience:** Shared intelligence allows the UK legal sector to defend as a bloc. A threat identified by one firm becomes a lesson learned for all, raising the "security floor" for the entire industry.
- **Transparency as a Standard:** Moving away from "tick-box compliance" toward "shared defence" aligns law firms with the transparency expectations of their most sophisticated clients and regulators.

> Shared intelligence allows… to defend as a bloc."

By adopting this collaborative framework, law firms do more than just meet regulatory mandates; they build a scalable, future-proof defence that turns the supply chain from a source of anxiety into a source of collective strength.

# 5. Case Study: Defending as One in the Legal Sector

The transition from a siloed "tick-box" approach to a collaborative model is not just a theoretical ambition; it is already delivering measurable outcomes for UK legal and public sector organisations. By moving away from manual spreadsheets and embracing a networked ecosystem, firms are transforming their security posture from a reactive burden into a strategic advantage.

## Identifying Systemic Risk Through the Network

"Uncover over 1,000 hidden supplier dependencies"

Consider the scenario faced by a community of organisations, including legal departments and public sector bodies, during a widespread software vulnerability. In a traditional model, each entity would have to manually contact every supplier to ask, "Are you affected?".

On a collaborative platform like Risk Ledger, the "Defend-as-One" doctrine changes the response dynamic:

- **Rapid Discovery:** When a critical vulnerability (such as a 10.0 CVSS score threat in a common JavaScript library) is identified, Risk Ledger ask all suppliers on its platform whether they are using the tool, are investigating, remediating, have resolved any issues or aren't affected, which is then communicated across all their connected clients.
- **4th Party Visibility:** In one landmark instance, the collaborative network allowed a community to uncover over 1,000 hidden supplier dependencies and critical concentration risks that were previously invisible to individual assessments.
- **Real-Time Remediation:** Instead of chasing emails, security leads use integrated chat functions to discuss remediation directly with suppliers.

## Tangible Efficiency Gains

The efficiency of this model is best demonstrated by the reduction in duplicated effort for both the firm and its vendors.

- **Scaling Coverage:** Organisations have seen their supplier coverage jump from a mere 5% to 95% without a proportional increase in headcount.
- **Reducing Assessment Time:** By leveraging the "assess once, share with many" principle, security teams can now access completed security profiles of their newly connected suppliers in an instance, significantly reducing the time needed to review their suppliers security postures compared to having to wait for new assessments to be completed from scratch.
- **Sectoral Strength:** For the supplier, the ability to maintain a single, high-quality security profile shared with multiple legal clients eliminates "questionnaire fatigue," ensuring the data provided is more accurate and frequently updated.

## The Outcome: Confidence and Resilience

The ultimate "proof point" for a senior security leader is the ability to evidence a robust posture to the board and to clients. By participating in a shared intelligence network, firms can prove to their sophisticated clients in finance and government that they are not just managing their own risk, but are part of a proactive community that identifies and remediates threats before they can cause a breach.

As one Risk Ledger user in a highly regulated sector noted, this transition provides a "more holistic, real-time view of a complex supply chain," enabling firms to achieve a significantly better security posture with less demand on their internal resources.

> "More holistic, real-time view of a complex supply chain."

# 6. The Road Ahead: Building the Legal Sector's Collective Defence

The evolution of the legal sector's cyber security is no longer a matter of individual effort, but of collective resilience. As we navigate the complexities of 2026, the firms that thrive will be those that transition from reactive, siloed compliance to a proactive, network-driven defence. Meeting the escalating expectations of clients and regulators requires a fundamental shift in how we perceive and manage our digital supply chains.

## Steps to Begin the Transformation

Building a collective defence does not happen overnight, but it begins with a few strategic shifts in operational philosophy:

- **Connecting with Peers:** Firms must actively participate in shared intelligence communities to exchange insights on emerging threats and supplier vulnerabilities.
- **Standardising Assessments:** By moving away from bespoke, fragmented questionnaires toward standardised, platform-based assessments, the industry can reduce friction for both firms and suppliers.
- **Promoting Radical Transparency:** Shifting the culture from one of historical secrecy to one of open transparency regarding supply chain hygiene ensures that "good" security becomes a sector-wide baseline.

## Risk Ledger: The Enabler of Collective Defence

Risk Ledger sits at the heart of this transition, acting as the technological and community engine for the legal sector's shift toward shared defence. By providing the infrastructure for real-time visibility and collaborative risk management, Risk Ledger empowers firms to:

- **Automate the Burden:** Remove the administrative heavy lifting of traditional TPRM, allowing security professionals to focus on high-impact risk reduction.
- **Master the Nth-Party:** Gain unprecedented visibility into the deep supply chain, identifying hidden 4th-party risks before they manifest as crises.
- **Deliver Client Assurance:** Provide sophisticated clients with the continuous, evidence-based assurance they now demand as a condition of instruction.

## Conclusion

The legal industry stands at a crossroads. The traditional models of assurance are failing to keep pace with the realities of 2026, leaving firms exposed to risks they cannot see and burdens they can no longer sustain. However, by embracing a collaborative approach, the UK legal sector can turn its collective scale into its greatest strength.

The road ahead is one of shared intelligence, operational transparency, and mutual defence. By leveraging the power of the Risk Ledger network, law firms can meet the future not as isolated targets, but as a resilient community, secure in the knowledge that their supply chain is a reinforced shield rather than a hidden vulnerability.

RISK LEDGER

**Risk Ledger Ltd.**
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

**Company registration number (England & Wales):** 10831970

**Contact**: www.riskledger.com | marketing@riskledger.com | +44 1234 567890