cowbell

Cyber Threats Targeting the Legal Sector

A global analysis of cyber espionage, extortion, and digital risks affecting law firms

Executive Summary

Law firms operate as centralized repositories for some of the world's most sensitive information. From corporate merger strategies and intellectual property schematics to confidential litigation files and vast trust accounts, the legal sector has become a high-value "data honey pot" for sophisticated cyber adversaries.

Cowbell's latest intelligence reveals an aggressive and escalating threat landscape driven by a dual-threat: financially motivated ransomware groups deploying double-extortion tactics, and state-sponsored espionage actors using law firms as backdoors to bypass the hardened perimeters of their government and enterprise clients. We outline the regional threat landscapes across the US, UK, and Australia, detail notable cyber incidents, and provide a sound approach to digital resilience for the global legal sector.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

The Threat Landscape: A Convergence of Adversaries

The legal sector is increasingly targeted due to the inherent leverage attackers gain when confidential information is exposed. The consequences of breaches extend beyond immediate technical disruption, often leading to a loss of attorney-client privilege, severe regulatory fines, and malpractice claims.

- **Financially Motivated Ransomware:** Ransomware groups explicitly target legal organizations because the urgent nature of court deadlines and the strict confidentiality required by clients creates immense pressure to pay.
- **State-Sponsored Espionage:** Nation-state actors (particularly from China) are infiltrating law firms to access classified or proprietary data related to national security, trade agreements, and foreign investment. These actors prioritize stealth, with some maintaining undetected access within legal networks for over a year.
- **Insider Threats & Social Engineering:** Due to the fast-paced, urgency-driven nature of legal transactions, Business Email Compromise (BEC) and sophisticated phishing campaigns remain highly effective at diverting escrow and settlement funds.

Notable Cyber Incidents: United States

For US brokers, this intelligence underscores a critical shift: law firms are no longer just collateral damage in ransomware campaigns; they are deliberate, primary targets for both cybercriminals and foreign intelligence services. We are seeing groups like the Silent Ransom Group exclusively focus their extortion efforts on US practices, while state-sponsored actors infiltrate networks to steal trade secrets. We must help our legal policyholders structure the right Cyber and Professional Liability coverage to navigate these complex breaches, fund expert digital forensics, and protect their clients' most sensitive data.

Williams & Connolly and Wiley Rein (Nation-State Espionage)

In 2025, Chinese government-affiliated cyber groups breached these prominent Washington D.C. law firms. Attackers compromised email accounts to access highly sensitive information related to US foreign investment, tariffs, and national security policy.

Brent Caldwell Law Office

In March 2026, INC Ransom breached this North Carolina-based real estate finance and litigation firm. Attackers exposed 1.1 terabytes of sensitive client data, demanding a $1 million ransom - a devastating figure for an SMB practice.

Pillsbury Winthrop Shaw Pittman LLP

In late 2025, a sophisticated AI-crafted phishing email impersonating a legitimate client bypassed security protocols. The breach compromised the personally identifiable information (PII) and financial details of nearly 40,000 Texas residents, resulting in consolidated class-action lawsuits against the firm.

Katz, Kantor, Stonestreet & Buckner (KKSB)

In February 2026, the Kairos ransomware operator breached this personal injury firm, exposing 700 GB of highly sensitive client data, including medical records and personal injury documentation.

Notable Cyber Incidents: United Kingdom

The UK legal sector is the backbone of global commercial transactions, making it an incredibly lucrative target. The intelligence demonstrates, for example, that a breach at an IT service provider can completely paralyze the conveyancing market, halting property deals nationwide. For UK brokers, this highlights the necessity of discussing third-party risk management (TPRM) with every legal client. We are here to provide the proactive guidance and robust coverage that keeps UK solicitors resilient in the face of supply chain disruptions and aggressive ICO regulatory scrutiny.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

CTS Corporation (Supply Chain Attack)

In late 2023, an anonymous ransomware collective breached CTS, a managed IT services provider widely used by UK law firms. The attack exploited a zero-day vulnerability (CVE-2023-4966), bringing down phone, email, and case management systems for over 80 legal organizations. The 38-day downtime severely disrupted the UK property market.

Thrings Solicitors and Lawyers

In December 2025, the World Leaks group claimed a ransomware attack against this prominent legal firm. The attackers published 7.3 terabytes of data (over 12 million files), exposing internal administrative data, client records, and attorney-client communications.

Gardiners Solicitors

In October 2025, the DragonForce ransomware collective breached this smaller UK firm, publishing 87GB of highly sensitive data. The exposure included criminal proceedings, witness names, and real estate contracts.

UK Legal Aid Agency

An April 2025 cyberattack forced the agency's systems offline for months, preventing aid attorneys from billing for services and exposing the personal data of hundreds of thousands of legal aid applicants.

Notable Cyber Incidents: Australia

Australian law firms are facing an unprecedented regulatory environment. With privacy legislation penalties now reaching up to AUD $50 million for security failures, the stakes have never been higher. Recent attacks against specialist family law firms and regulatory boards have forced practices to secure Supreme Court injunctions just to manage the fallout of data extortion. Our role is to ensure Australian legal practitioners have the financial resilience and expert incident response backing necessary to survive these existential threats.

Anthony Wall
Head of Underwriting (Australia)

Paterson & Dowding

In December 2025, the Anubis Ransomware group breached this specialist family law firm in Western Australia. The stolen data was highly intimate, including screenshots of personal family correspondence, superannuation forms, and financial liabilities. The firm was forced to obtain a court injunction to legally prevent the publication or transmission of the impacted data.

Legal Practice Board of Western Australia (LPBWA)

In May 2025, Dire Wolf Ransomware attacked this independent statutory authority, forcing a shutdown that disrupted the state's legal infrastructure for months. After failed negotiations, Dire Wolf allegedly sold the 300GB data cache on the dark web for $100,000.

Brydens Lawyers

In February 2025, one of New South Wales' largest litigation firms suffered a ransomware intrusion that compromised over 600 gigabytes of sensitive employee and client data, including Tax File Numbers (TFNs) and health information.

Threat Actor Profiles

- **Silent Ransom Group (SRG / UNC3753):** Emerging after the collapse of the Conti syndicate, SRG specializes in targeting US-based law firms. They use sophisticated IT-themed social engineering to steal data for extortion without deploying traditional encryption.
- **APT41 & BRICKSTORM (Nation-State Espionage):** China-sponsored advanced persistent threats (APTs) that infiltrate law firms handling sensitive political, trade, or national security matters. They prioritize stealth, maintaining prolonged, undetected access to exfiltrate legally privileged intelligence.
- **DragonForce, INC Ransom, & Akira:** Financially motivated Ransomware-as-a-Service (RaaS) collectives operating within the Russian cybercrime ecosystem. These groups aggressively utilize double-extortion techniques, weaponizing the strict confidentiality requirements of the legal sector.

The Sound Approach to Risk: Recommendations

- **Enforce Strict Identity and Access Management (IAM):** Implement phishing-resistant Multi-Factor Authentication (MFA), such as FIDO2 or WebAuthn, across all email accounts, document management systems, and remote access services to neutralize credential theft.
- **Introduce Robust Third-Party Risk Management (TPRM):** Law firms must continuously evaluate their IT service providers and cloud vendors. Ensure contracts include “right-to-audit” clauses and demand adherence to recognized frameworks like ISO 27001 or NCSC Cyber Essentials.
- **Establish DFIR Playbooks:** Develop tactical Digital Forensics and Incident Response playbooks. Law firms must know exactly how to preserve evidence for regulatory proceedings (e.g., ICO, SRA, or state bars) while maintaining attorney-client privilege during a crisis.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today’s threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0065 0626