Cybersecurity and Legal Tech: Are UK Law Firms Prepared?

Written by Sarah Kelly

Two-thirds of UK lawyers say they're worried about cybersecurity, and only about a third feel prepared. That 29-point gap, captured in Clio's *The State of Legal Tech 2026* report, gets to the crux of cybersecurity in UK law right now: most lawyers know the threat is serious, but far fewer are sure their infrastructure can hold up.

The uncertainty surfaces in everyday scenarios: board meetings where the question goes unanswered, rising premiums on professional indemnity renewals, and clients' security questions nobody at the firm is fully sure how to address.

Why law firms are prime targets

Attackers target law firms for a specific reason: the matter file. A single matter pulls together financial information, personal data, commercial intelligence, and privileged advice in one place, and that combination is valuable to attackers long after the breach.

A leak rarely stops at one document, either. The way firms organise matter files means a single intrusion typically hands over the client, the case they're partway through, and adjacent files all at the same time.

Firms with the most concentrated client data often have the smallest IT teams and the least capacity to recover when something goes wrong. Phishing, ransomware, and data breaches now reach firms of every size. Automation has compressed the window between vulnerability discovery and exploitation to a speed traditional in-house patching can't match.

The cost of a serious incident lands hardest on the firms least equipped to recover, which is why cybersecurity is moving out of the IT budget and into the strategic conversation. Recovery from a breach goes well beyond the technical problem, drawing in regulators, professional negligence claims, and the slow work of rebuilding client trust afterwards. That trust now runs through the technology underneath your firm, and protecting client data has become part of legal practice itself.

What the data says about UK law firms

Most of that 29-point gap sits in the supporting infrastructure. UK firms have spent the past decade adding tools, often one at a time, each with its own login, update schedule, and security model. The accumulation stays invisible until something goes wrong, when it becomes the explanation for the breach.

Manual patching, on-premises servers, and ad hoc access controls weren't built for the threats firms face today. Most of those tools were built for a world where data sat on the office network, and attacks came in through the front door, a setup most UK firms left behind years ago.

A written policy can't patch a server, and induction training can't close the gaps the system itself creates. Strong day-to-day security relies on three things working together: modern infrastructure, regular updates, and platform-level controls running in the background. When a firm is missing any of those, even careful staff can only do so much to compensate. Closing the gap usually starts with secure, cloud-based legal technology that handles today's threats by design.

Building a secure legal tech foundation for UK law firms

Most legal IT teams already know what a secure platform should include:

- Encryption for data in transit and at rest
- Granular user permissions
- Automatic updates that close vulnerabilities quickly
- Independent security audits and compliance certifications
- Protection against device loss or local server failure

Even careful staff click links in a hurry or reuse passwords across systems they didn't realise were connected. But the strongest platform on the market won't fix either of those. Training has to do that work, and it only helps when it shifts daily behaviour: how your team treats unexpected attachments, how they handle credentials, how they think about the AI tools they use every day.

Clio Manage covers the technical side of that checklist. The platform protects your data with 256-bit encryption, sets user permissions at a granular level by default, undergoes regular independent security audits, and maintains SOC 2 Type 2 compliance to demonstrate the controls hold up against recognised industry standards.

Cloud infrastructure has an advantage that doesn't get much airtime in the security conversation. Leading cloud providers invest more in monitoring, response, and resilience than any individual firm could afford on its own. Moving to the cloud swaps your in-house security team for a much larger one, run by people whose entire business depends on getting security right.

AI and the future of legal cybersecurity

AI is the new variable most firms are still working out. The exposure it introduces is concrete enough already. The same tools that help your lawyers draft, summarise, and research can leak privileged information to systems outside your firm's control if your staff doesn't configure them carefully.

The cases are already out there: privacy leaks at large practices, client questionnaires that now ask explicitly about AI use, and AI-assisted drafts surfacing details from a different matter inside an LLM's response. The pressure to adopt AI is real, and firms gain ground by building clear AI guardrails into the workflow alongside the rollout.

Defensive capabilities are catching up, and firms that fold security into everyday work see the benefits:

- Reviewing your systems and access permissions on a fixed schedule
- Choosing technology partners who treat continuous security improvement as part of the product
- Building security checks into your everyday workflows from the start
- Refreshing staff training regularly, not only at induction

Do all of this even when nothing has gone wrong, and you'll be glad you did when a phishing email lands in your inbox at 4:47 p.m. on a Friday.

Closing the cybersecurity gap

The gap won't close itself. The firms moving past it run on platforms that prioritise security from the start, and that decision is mostly about which technology partner you pick. Clio gives UK firms a secure cloud foundation that scales as the threats change.

See how Clio helps your firmstay secureas the threats evolve.

Frequently asked questions

Why is cybersecurity important for UK law firms?

Law firms hold sensitive client data, which makes them prime targets for cyberattacks and regulatory action.

What are the most common cybersecurity risks for law firms?

The most common cybersecurity risks for UK law firms are data breaches, ransomware, phishing, and intrusions that exploit ageing systems. Insider threats and supply-chain attacks via third-party vendors are increasing concerns.

Does running legal software in the cloud improve security?

Yes. Platforms like Clio provide 256-bit encryption, continuous monitoring, and regular updates that most firms can't realistically replicate in-house.

How can Clio help UK law firms stay secure?

Clio combines strong security controls, recognised compliance certifications, and transparent data management to help your firm protect clients and keep their trust.

About Clio

Clio is the global leader in legal AI, powering legal work across the profession, from law firms of every size to corporate legal teams, government agencies, and courts. Its Intelligent Legal Work Platform unites the business and practice of law, connecting the people, information, and processes behind legal work. Clio's AI brings the context together with legal sources drawn from Clio Library, a growing collection of more than one billion legal documents. Over 400,000 legal professionals in more than 130 countries rely on Clio to run their legal world. Learn more at www.clio.com.