ALM | LAW.COM
LAW JOURNAL NEWSLETTERS

CYBERSECURITY LAW & STRATEGY

Top 7 Ways Law Firms Can Fortify Their Security and Protect Client Trust

In the minds of your clients, trust and security are intertwined. As stewards of confidential client information, law firms must go beyond minimum compliance, setting a gold standard that safeguards data, builds confidence and differentiates forward-looking practices from the rest. The following seven strategies, drawn from real-world experience in legal technology, outline actionable ways law firms can fortify their defenses while making security a pillar of client trust and firm reputation.

By Jacob Mathai
September 30, 2025

With law firms entrusted with some of the world's most sensitive information — including corporate secrets, intellectual property, financial records and medical data — cybersecurity is now essential. In 2025, the legal sector faces a daunting challenge: surveys consistently show that one in three law firms are at risk of a data breach in a given year, with the average costs per incident exceeding $5 million. Perhaps even more concerning, cross-industry research from organizations such as SecurityScorecard and Verizon indicates that approximately one-third of breaches originate from third-party service providers and vendors.

In the minds of your clients, trust and security are intertwined. As stewards of confidential client information, law firms must go beyond minimum compliance, setting a gold standard that safeguards data, builds confidence and differentiates forward-looking practices from the rest. The following seven strategies, drawn from real-world experience in legal technology, outline actionable ways law firms can fortify their defenses while making security a pillar of client trust and firm reputation.

1. Prepare for the Vendor Cascade: Assess Risks Where They Actually Begin

While headlines sensationalize cybercriminals and hacking groups, research and direct experience confirm that most threats infiltrate organizations via a complex web of third parties such as cloud providers, court reporting platforms, e-discovery vendors, software-as-a-service solutions and other external partners. Your security is only as strong as the weakest link in your extended ecosystem.

Things You Can Do:

- **Map Your Third Parties:** Catalog every vendor that touches client data, however indirectly.

This goes beyond obvious partners to include any software or service with even marginal data access.

- **Acknowledge Client Expectations:** Clients now expect that their law firms not only vet their own tools but also demand and enforce security standards from all vendors.
- **Push Responsibility Downstream:** Your clients' regulatory and other obligations can transfer downstream to your firm, and then onward to each supporting vendor. Security isn't just a best practice; it's a shared mandate to be upheld by law firms and by enterprise clients.

2.Regulatory Compliance Isn't Optional: Make It a Proactive Value Proposition

Legal practitioners must view regulations — HIPAA, GDPR, CCPA, PIPEDA and more — not as bureaucracy but as risk frameworks protecting both the firm and its clients. Compliance isn't just about avoiding fines; it's an important differentiator, and one clients now notice.

Actionable Tips:

- **Know Your Obligations:** Different case types (*e.g.*, medical malpractice, IP, cross-border) may trigger specific compliance regulations. Understand which apply and how to operationalize them.
- **Demand Documented Proof:** Require that vendors prove ongoing compliance, not just by signing a business associate agreement (BAA) or contract appendix, but by furnishing concrete evidence of technical and organizational measures in place.
- **Educate Your Team:** Lawyers and staff must realize that compliance responsibilities cascade down. For example, if a client is subject to the GDPR, so is the firm and so are all vendors handling that data.

3. Treat All Client Data as Gold — Not Just "Official" Records

Too often, law firms focus their rigorous controls on traditional confidential firm data (financials, billing records, etc.), while underestimating the sensitivity of working files — transcripts, video depositions, background research and other litigation support materials. In the world of breaches, all data is valuable.

Best Practices:

- **Have One Standard for All Files:** Establish that any document, recording or data tied to client representation deserves the same level of protection as a retainer agreement or other client financial record.
- Concrete Example: In litigation, video depositions or IP-related transcripts may contain trade secrets or HIPAA-protected details. Treat these with full-spectrum security controls, including access restrictions and audit trails.
- **Cultivate a Cultural Shift:** Embed security thinking into the firm's culture so that everyone — lawyers, paralegals and administrative staff — understands what's at stake and takes precautions accordingly.

4. The New Standard: Vet and Score Your Vendors

Vendor selection is no longer just about features and price; it's a security arms race. Vetting must become systematic, actionable and comparable across vendors.

How to Do It:

- **Develop a Standard Questionnaire:** Use resources like the standardized information gathering (SIG) questionnaire from Shared Assessments, a robust, industry-accepted set of security-related questions that probes a vendor's readiness, controls and compliance. While some firms have a member of the team designated to ensure all third parties are vetted and assessed for risk, there are also providers you can work with,

sparing your firm the heavy lift involved in starting a program such as this. When deciding to engage with a provider, look for one that specializes in the legal space, such as Prevalent.

- **Apply Multilayered Reviews:** Don't just ask your vendors if they are secure; demand proof. Conduct interviews with their IT teams, and require independent audits (such as SOC 2) as part of your procurement process.
- **Require Disclosure and Attestation:** For every regulation relevant to your firm or clients (HIPAA, GDPR, CCPA, PIPEDA), demand that vendors sign off and demonstrate compliance.
- **Confirm Supply Chain Integrity:** Ask your vendors how they vet their own key subcontractors or software suppliers. Your risk trickles down throughout the chain.

5. Encryption: Maximize the (Mostly) Invisible Shield

While security innovation accelerates, some fundamentals remain necessary, and encryption is a core factor. Both data at rest (stored on servers or devices) and in transit (moving through the internet or between offices) must be encrypted.

What to Emphasize:

- **Firm Policy:** Mandate encryption for all confidential client files, work product and communications—no exceptions. Don't assume "the cloud takes care of it."
- **Vendor Responsibility:** Confirm that every vendor storing or transmitting your data applies strong encryption protocols as a requirement of doing business.
- **Keeping It Simple:** You don't need to become technical experts. Just demand clear yes or no answers and review contractual language stipulating encryption at every stage.

6. Multifactor Authentication: The Baseline of Security

The era of passwords alone is over. Implementing multifactor authentication (MFA) — requiring not just something you know (a password) but also something you have (a phone, app or token) — is now baseline security across law firm systems and third-party platforms.

Steps for Implementation:

- **Apply Across Systems:** Enable MFA for remote access, document management, email and every cloud-based service that offers it.
- **Make Demands of Vendors:** Insist that all partners with access to your firm's data offer MFA as an option, and recommend your clients look for the same.
- **Communicate to Clients:** Be transparent with clients about these measures. It demonstrates proactive stewardship and reassures them of your seriousness around security.

7. Beyond the Basics: Utilize Ratings, AI Oversight and the Human Firewall

Some of the greatest advances — and greatest risks — now come from the expanding environments in which law firms operate.

Use Independent Ratings to Evaluate Vendor Security

Just as credit providers use credit scores, firms should leverage services like SecurityScorecard and Bitsight. These agencies rate vendors on objective security criteria and can provide valuable third-party validation when comparing or selecting partners. Ask your current and prospective vendors to share their security ratings or provide reports from these agencies as part of your annual review.

Address the New AI Frontier

With generative AI tools becoming common in legal workflows, new security concerns are emerging. Make sure you are not using client data to train AI or large language models (LLMs), or risk that sensitive information leaks far beyond

your firm. Insist that your vendors set up policies and technical controls to prevent accidental exposure, minimize risk of hallucinations, prevent training LLMs on your data and guard against unintentional sharing of data through AI systems. Lastly, vet how vendors use AI behind the scenes. Do they have employee training and written standards governing responsible AI use?

Make Ongoing Employee Training and Testing the Norm

Humans remain the single biggest vulnerability, with 60% of breaches being caused by the human element, but we can also be the greatest line of defense — if properly coached. Institute monthly phishing and security drills for all employees, including attorneys, support staff and leadership. Treat mistakes as learning opportunities, with progressive reinforcement not punishment. Increase the sophistication of security exercises as your team improves. Foster a "can you beat the test?" culture.

Ask your vendors not just about their technical defenses, but also about their ongoing employee training and outcomes as well. Remediation and reeducation after failures should be standard for your firm and suppliers.

Conclusion: Security As a Trust Multiplier

The stakes of law firm cybersecurity go far beyond technical metrics or compliance checklists. When you fortify your ecosystem — from the files you store to the vendors you hire to the training you impart to your staff — you're not only defending against costly breaches, but also cementing your reputation as a diligent, client-first organization. Clients increasingly demand proof that you go above and beyond, because their own obligations and brand equity are also on the line. The legal industry is poised for a new era: one in which security isn't just a background IT function, but a visible, proactive differentiator for every practice. Firms that seize this opportunity will strengthen client loyalty, protect their own futures and set the pace for how legal work, and legal trust, should be protected in a digital world.

Action Checklist

- Inventory all third-party vendors and demand documented security compliance.
- Ensure encryption and MFA are enforced across your environment and vendors.
- Leverage standardized security vetting questionnaires and rating agencies.
- Require proactive policies around AI use, including clear lines around model training and data sharing.
- Make security training and testing a monthly firmwide discipline.
- Position your firm not only as a guardian of information, but as a leader in building client trust through world-class digital hygiene.

*****

Jacob Mathai is the chief information officer for Veritext Legal Solutions, the leader in technology-enabled court reporting services and litigation support solutions.

The views expressed in the article are those of the authors and not necessarily the views of their clients or other attorneys in their firm.

Reprinted with permission from the September 30, 2025 edition of the Law Journal Newsletters © 2025 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-256-2472 or asset-and-logo-licensing@alm.com. # LJN-10062025-68346