Legal's weakest link? Proactively securing your third-party ecosystem; here's how to address it

By Melissa Griffins Paulk

Law firms and legal departments require heightened data privacy and cybersecurity risk policies because of the wealth of privileged, confidential and regulated information—including personal data, trade secrets, financial data, employee information and intellectual property they control. To mitigate risks, legal professionals must elevate their security strategy to a risk-driven approach.

Modern legal services leverage digitization, cloud platforms and artificial intelligence tools, expanding the firm's data ecosystem. Law firms increasingly rely on external providers to support core legal and technological functions. While vendor relationships drive efficiency, they also expand the firm's scope of attack beyond its internal environment.

Third- and fourth-party vendor services and technologies represent one of the most significant, and often least visible, cybersecurity threats for law firms today. Unlike other industries, law firms must manage cybersecurity risk, along with ethical obligations, privilege concerns, fiduciary responsibilities and contractual commitments. A vendor-caused security incident may expose a law firm to malpractice claims, bar discipline and regulatory enforcement, even if the firm was not breached directly.

Primary vendor-related threat vectors impacting law firms include:

1. Vendor data processing and hosting

2. Inadequate vendor security governance and controls

3. Software supply chain vulnerabilities

4. Fourth-party and subprocessor risk

5. Weak contractual safeguards and enforcement

6. AI-enabled vendor risk

Vendor data processing and hosting

It is common for legal vendors to store, transmit or process privileged and confidential client information, so a cyberattack on a single vendor platform could expose the data of hundreds of law firms.

When a vendor experiences a security incident, law firms often have limited visibility into its timing, scope or impact but remain responsible for client notification and other ethical and regulatory obligations. Additionally, many law firms do not have a measurable, repeatable approach to evaluate and manage risk in vendor relationships.

Legal organizations can mitigate vendor processing and hosting risks by implementing a vendor data handling and security policy that defines data classification categories and logic, data minimization requirements, secure file transfer standards, and data access protocols and contractually requires data encryption in transit and at rest. Additionally, law firms should document and implement formal vendor risk assessment, scoring and management procedures.

Inadequate vendor security governance and controls

Some legal vendors lack mature cybersecurity programs. Gaps may include irregular penetration testing, limited security monitoring and logging, weak employee security training, and lack of independent security audits or certifications. Bad actors exploit these holes to gain indirect access to law firm systems and data, making preengagement due diligence imperative.

Law firms should require all vendors to complete a vendor security questionnaire and provide independent security audit documentation and certifications. Law firms should also establish minimum nonnegotiable security controls, such as multifactor authentication, incident response plans and security risk scorecards to track the vendor's risk appetite and cyber program maturity and automate reassessment on a regular basis or with material changes to the service(s) or product(s).

Software supply chain vulnerabilities

Law firms depend on vendor software updates, plug-ins, application programming interfaces and integrations. If malicious code is introduced through an update or open-source components, clients may be negatively impacted downstream.

In 2023, the popular managed file transfer product MOVEit Transfer employed by law firms, legal service providers and other organizations was exploited by a ransomware group (https://www.ncsc.gov.uk/information/moveitvulnerability). Attackers found a vulnerability in the MOVEit web application, allowing them to gain unauthorized access to MOVEit

servers and the large volumes of sensitive data from clients, courts, opposing counsel and vendors stored within the platform. Numerous law firms and legal providers faced exposure of privileged legal communications and disclosure of client personal data, medical information and financial information. Even law firms with strong internal cybersecurity controls were not immune.

In hindsight, organizations might have been able to reduce the risk of potential harm through rapid vulnerability notification language in vendor contracts, date retention limits on file transfer platforms, and maintaining a current inventory of vendor software used to process client data. For law firms, software supply chain risk must be treated as a legitimate operational and professional responsibility.

Contractual safeguards and enforcement

Vendor contract language is often too weak to give law firms the leverage necessary to enforce cybersecurity and data protection obligations. Common gaps include a lack of minimal security standards, no audit rights, no breach cooperation requirements, insufficient restrictions on subcontracting, and lack of data deletion or return obligations.

To bolster enforceability, law firms could standardize key contract clauses across the vendor portfolio to include a uniform data protection and security addendum, clearly defined audit and assessment rights, indemnification for vendor-caused security incidents, certified data return and secure deletion requirements, and termination rights if vendors fail to meet security obligations.

To draft stronger, more comprehensive vendor agreements, lawyers and law firms will have to learn and recognize cybersecurity risk, to some degree. Lawyers should begin familiarizing themselves with industry-agnostic risk frameworks and translate risk controls into contractual language.

Law firms and lawyers may also rely on AI to strengthen contracts. Increasingly, AI tools can provide robust contractual terms that align with industry standards and risk frameworks. AI tools also routinely redline commercial terms and suggest alternative language crafted from regulatory requirements. Law firms may also invest in specialized AI, where an AI tool is customized for a specific organization, and automate law firm risk standards, template development, and first pass contract reviews.

Fourth-party and subprocessor risk

Third-party vendors regularly rely on their own subcontractors, cloud service providers, analytic tools or offshore service providers. These fourth-party relationships are often undisclosed or opaque to the law firms directly engaging the vendor. The most common

fourth-party risks include unauthorized subprocessing of client data, contractual security obligations not flowing downstream, and unknown data storage locations or cross-border transfers. Even with due diligence on a primary vendor, law firms may remain unaware of critical downstream dependencies introducing material risk.

Law firms must manage fourth-party risk the same way they manage third-party risk. They should implement mandatory requirements for vendor disclosure of all subprocessors prior to onboarding and require notice of any changes. Model contractual clauses should specify restrictions on data storage and processing locations and mandate vendors impose equivalent security and confidentiality obligations on their subcontractors. Law firms should also maintain a contractual right to approve or object to new subprocessors and terminate if the risk is unacceptable.

AI-enabled vendor risk

AI-enabled tools increasingly drive efficiencies across multiple business sectors. However, as law firms deploy them, new risks emerge around confidentiality and professional responsibility. Frequently, law firms are unaware of or underestimate the extent to which AI features and tools access or use client data. Training AI models on client data without proper authorization or a lack of transparency into AI data flows is a common occurrence.

To limit the risk, law firms must be intentional with robust controls around vendor and subprocessor AI use. Law firms must require disclosure of all AI use, training data sources and model purpose from applicable providers. Vendor contracts should explicitly prohibit firm or client data in AI training, require human review of all AI outputs used in legal workflows, define escalation paths for AI-related data leaks or hallucinations, and monitor how AI tools are applied within legal workflows.

Legal organizations must treat third- and fourth-party risk management as a core component of any cybersecurity strategy. The risks cannot be mitigated through assessments alone. Law firms must employ robust operational controls, enforceable contracts, strong technical safeguards and repeatable procedures that extend security standards across the entire enterprise vendor ecosystem. Managing vendor risk is a fundamental responsibility to protect client trust, preserve privilege and meet evolving regulatory and ethical obligations.

Melissa Griffins Paulk is the director of data privacy and security solutions at QuisLex (https://quislex.com). She specializes in data privacy, AI governance and complex technology transactions. She currently advises corporate clients on building and improving strong privacy and AI compliance programs.

Mind Your Business is a series of columns written by lawyers, legal professionals and others within the legal industry. The purpose of these columns is to offer practical guidance for attorneys on how to run their practices, provide information about the latest trends in legal technology and how it can help lawyers work more efficiently, and strategies for building a thriving business.