



Cyberattacks against law firms are becoming more widespread, sophisticated and costly. Law firms are especially attractive targets: they hold valuable, confidential client data — including personally identifiable information (PII), protected health information (PHI) and payment card or banking information (PCI) — along with sensitive intellectual property, business intelligence, and details on significant business transactions. Add in a heavy reliance on email and, in many firms, inconsistent cybersecurity practices. The result? A combination of high value and real vulnerabilities spurring breaches that carry major business consequences.

According to the American Bar Association's *Cybersecurity Tech Report*, nearly one in three law firms have experienced a security breach, yet only 40% of law firms report having Cyber Liability insurance. With law firm breaches costing an average of \$5.08 million, as cited in IBM's Cost of a Data Breach Report, the financial stakes of a breach far outweigh what most firms are prepared to absorb. Mitigating cyber risks starts with understanding the nature of these threats and closing gaps before they're tested.

Most Common Cybersecurity Threats in the Legal Industry

Industry studies and real-world claims point to a consistent set of cyber threats driving law firm losses. Understanding these is the first step toward closing the gaps in your firm's defenses.

The top five cybersecurity threats based on the number of claims we see are:

1. **Ransomware attacks** that lock down a firm's IT systems until a ransom is paid
2. **Business email compromise**, such as spoofing, that impersonates trusted contacts to access sensitive information
3. **Funds transfer fraud** resulting from spoofing emails that direct wire transfers to cybercriminals instead of the intended accounts
4. **Hacking and unauthorized access** where cybercriminals tap into sensitive information that should be under counsel's care, custody and control
5. **Staff mistakes**, including employees manipulated by phishing and social engineering, or unintentionally exposing data through remote work without proper firewalls or secure Wi-Fi

Beyond these top threats, third-party and vendor vulnerabilities are another common risk vector putting firms, and any client information those vendors can access, in jeopardy.



Cyber Coverage Misconceptions Putting Law Firms at Risk

Despite these growing threats, many firms continue to operate under risky misconceptions about cyber insurance — creating a false sense of protection and leaving them exposed to serious risks.

“Our General Liability policy covers cyber risks.”

FACT: Most commercial General Liability policies explicitly exclude cyber-related losses.

“Crime insurance will protect us from cyberattacks like phishing or hacking.”

FACT: Traditional Crime policies typically cover theft and fraud, not cybercrime or broader cybersecurity events.

“Our Lawyers’ Professional Liability policy already includes cyber coverage.”

FACT: LPL policies may provide limited cyber coverage for third-party losses, but about 70% of financial damages are first-party losses, such as IT response, forensics, and data recovery costs. These are generally not covered, as LPL responds only when there is a demand for money or services.

“Business Interruption coverage will respond to a cyber incident.”

FACT: Traditional Business Interruption or Business Income coverage is triggered by physical damage to insured property, leaving law firms on their own to absorb the cost of lost billable hours for days or even weeks following a cyber incident.

“We’re too small to need separate cyber coverage.”

FACT: Cybercriminals frequently target small and mid-sized law firms due to their limited IT resources, leading to even greater risks that require dedicated protection. These misconceptions highlight not only how easily firms can overestimate their existing insurance coverage, but also why there is a bona fide need for dedicated cyber protection.

Proper Cyber Protection for Law Firms

A dedicated Cyber Liability policy — designed to cover exposures that General Liability, Crime and Professional Liability policies don’t — is a critical piece of a comprehensive risk management strategy. While there are many standard policies on the market, law firms are best positioned to manage their unique cyber exposures with coverage built specifically for the legal industry.

To address the specific risks facing law firms, USI Affinity offers comprehensive Cyber Liability insurance that enables legal professionals to effectively prepare for, respond to and recover from cyber incidents. This includes:

- **Standalone Cyber Liability coverage built specifically for law firms**, rather than a limited add-on to a General Liability, Crime, or Lawyers’ Professional Liability policy
- **Protection against the threats law firms actually face**, including ransomware, social engineering, wire fraud, and data breaches

- **First-party coverage** for costs such as IT forensics, data recovery, breach notification, crisis communications and lost billable hours
- **Third-party coverage** for costs arising from claims brought by clients or regulators after a breach, including legal defense, settlements and regulatory fines or penalties
- **Support before, during and after an incident**, including access to breach response resources such as forensics, legal counsel and recovery assistance
- **Flexible coverage tailored to your firm's operations and risk profile** that can scale with your firm's size and the sensitivity of the data you hold

Insurance alone isn't a complete risk management strategy, but the right Cyber Liability protection becomes part of your firm's broader defense, working alongside key internal practices that reduce your overall exposure.

Additional Risk Management Strategies

Beyond insurance, day-to-day practices play a critical role in reducing cyber risk. Taking these action steps can help prevent an incident and limit the damage if one occurs.

- Conduct a comprehensive risk analysis.
- Adopt strong data encryption practices.
- Implement multi-factor authentication (MFA).
- Enforce strong password management policies.
- Limit user access to only the data and systems necessary for each role.
- Regularly update software and apply security patches.
- Provide ongoing employee training and education.
- Develop and maintain an incident response plan.

None of these practices are groundbreaking, but consistently applying them strengthens a firm's preparedness and speeds recovery if or when an incident occurs.



Closing the Gap

No set of safeguards can eliminate cyber risk entirely. Pairing strong internal practices with the right cyber insurance coverage is what protects your firm when prevention isn't enough. Understanding your actual exposure, not just what you assume is covered, is foundational to keeping a single incident from becoming a firm-defining loss.

If you're interested in speaking with a cyber insurance specialist to make sure your coverage matches your firm's actual risk, visit [usiaffinity.com](https://www.usiaffinity.com). ■

This article was prepared by the USI Affinity Lawyers' Professional Liability Team. Please note that it is intended as a general guide and opinion only, not a complete analysis of the issues addressed, and readers should always seek specific legal guidance on particular matters.

About USI Affinity

USI Affinity is a national leader in designing malpractice insurance solutions for over 22,000 law firms nationwide. We specialize in insurance, like you specialize in a specific area of practice. USI Affinity offers a proprietary, comprehensive Lawyers Professional Liability program specifically designed to mitigate risk and close gaps in coverage.

For more information, visit www.usiaffinity.com/for-your-profession/lawyers/professional-liability.

