Marcus Cusick
CUSICK INSURANCE BROKERS, LTD.

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
August 2025

Law firms cannot afford to overlook cybersecurity

CLIENT DATA TAKES PRECEDENCE IN PROTECTION FROM CYBERATTACK

Trust is a law firm's currency. Clients turn to lawyers during the most critical and vulnerable moments in their lives. That is why law firms deal with uniquely sensitive and high-stakes information. But in this era of the information revolution, all firms must adopt a proactive attitude towards cyber defenses and commit to continual vigilance. Having cybersecurity is not a choice, but a necessity in safeguarding the trust that law firms depend on.

Unfortunately, many leaders of law firms are still in the dark about how vulnerable their practices are. Too often, cybersecurity is viewed as an inconvenience or unnecessary expense. This is a shortsighted mindset that leaves firms dangerously exposed. The reality is, attackers are growing more sophisticated each day, and outdated defenses are leaving law firms exposed. Damaging ransomware, social engineering, business email compromise, funds transfer fraud and other cyberattacks are now the norm, not the exception.

This article seeks to provide a practical guide to understanding why law firms are being targeted, the types of attacks they face, how to effectively build a cybersecurity strategy and how to secure adequate insurance in the event of an attack. You can use this to evaluate your own defenses and remain vigilant.

The state of cyber threats against law firms today

Law firms are in the crosshairs, and not coincidentally. The valuable data held within law systems, including Social Security numbers, financial details, business contracts, medical records and other highly sensitive personal data are prime targets for attackers. At the same time, as hackers have proven, many law firms of all sizes lack the technological infrastructure or proactive attitude that are required for defending against sophisticated cyber threats. This combination of desirable data and weak protections makes law firms the frequent target of damaging cyber-attacks.

Lawyers are required by the ABA and State Bar Rules of Professional Conduct to be technologically competent, to make reasonable efforts to secure client data, supervise staff, and communicate with clients if a breach occurs. These rules have evolved in recent years to place increasing responsibilities on lawyers, and they will likely continue to expand moving forward.

Ransomware

One of the most dreaded and common threats is ransomware. It encrypts a company's files and locks up its systems, requiring their decryption through a decryption key, usually only provided upon the payment of a ransom. Even when a firm manages to close the vulnerability and quickly recover its data, the threat still exists as the bad actor will publish sensitive data online unless the ransom is paid. Cybercriminals typically use an exposed point of access not just for a one-time attack, but to evaluate the firm's broader vulnerabilities and choose how to strike next.

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
August 2025

Responding to these incidents requires law firm leaders to coordinate forensic investigations, determine what was accessed, identify and secure the exploited access point, negotiate with the threat actors, arrange ransom payments, and handle client notifications, regulatory reporting, hiring of breach counsel, and public relations. While the cost of these can often be covered by insurance, these incidents are highly distracting and stressful for the firm's leaders.

Social engineering

Social engineering, where firm employees or leaders are manipulated into revealing sensitive details or paying bad actors, is on the rise in terms of frequency, complexity, and difficulty to detect. This typically involves the firm voluntarily parting with funds rather than a "hack" of systems. For example, an employee may receive a convincing email from a seemingly regular customer or vendor that appears to be a routine payment or password request, or HR may receive payroll-change requests from what appears to be an employee. The recipient takes action and the firm loses funds or sensitive client data.

Social engineering and funds-transfer fraud exist in a gray area that often catches law firms by surprise. These attacks do not rely on breaking into systems; they rely on exploiting trust. Social engineering takes advantage of human nature, and so there is no perfect protection against the human-error element at any organization. Therefore, a commitment to training everyone at the firm is critical.

Business email compromise (BEC)

A growing source of attacks at law firms is BEC. In these types of attacks, firm members are tricked into providing email login credentials, allowing bad actors to monitor communications, sometimes for months, while waiting for the right opportunity. The attack may target payroll, vendor payment, client payment, or other sensitive transactions. BEC attacks can easily escalate into ransomware attacks or lead the firm to unknowingly send compromised emails to thousands of contacts, opening the door to further attacks on other firms, vendors, courts, clients and creating significant liability and embarrassment for the firm itself.

Funds transfer fraud

This outcome is often a result of social engineering or BEC. Attackers gain access to internal communications and wait for the right moment, such as settlement disbursement, to insert fraudulent banking details. Once the money is redirected or an unauthorized transfer is initiated, the error is often not discovered until it is too late. By then, the funds are typically unrecoverable, and law firms are left with both financial and ethical consequences.

Many times, the access point of an attack is used to initiate another type of attack. BEC often leads to funds-transfer fraud or ransomware distribution. Data breaches and leaks, while sometimes tied to ransomware, are often the result of improperly secured databases or weak authentication methods. Cyberattacks are disruptive in the short term, but their long-term impact can be even more severe. They can lead to regulatory fines, ethical questions, lawsuits by clients, costly public-relations efforts and permanent damage to a firm's reputation.

What should be clear is this: Law firms can no longer afford to approach cybersecurity as a secondary concern. Threats are evolving, attackers are relentless, and the legal sector, due to the value and sensitivity of its data, makes a high-value target for bad actors.

How attacks happen and why they matter

As noted earlier, many cyberattacks do not start with a dramatic hack or a breach of firewalls. Instead, they begin with an email. Or a password. Or a moment of distraction. The most common attacks facing law firms today stem from basic entry points that are all too often left unguarded.

Phishing emails remain the most widespread attack vector. A member of the firm receives an email that looks legitimate – perhaps a message from a colleague, partner, or supervisor with an attachment, or from a client following up with a question. In reality, the email is fake. Clicking the link or downloading the attachment installs malicious code or redirects to a fake login site set up to capture login info. Once inside, attackers can move laterally, gaining control of sensitive files, client records, or even entire databases.

Credential stuffing is another major threat. Many professionals reuse passwords across different services, making it easier for attackers to use leaked or stolen credentials from one platform to access another. Once a single account is compromised, especially an email or administrative account, the firm's internal communications and confidential data are laid bare.

Cloud misconfigurations also deserve close attention. Many firms assume that because their case-management or other technology-driven provider is a tech company, security is already built in. In reality, while these providers often offer strong security features, such as two-factor login security, those features must be requested or enabled by the firm. We have been told by a prominent legal practice-management-software provider that a sizable majority of its client law firms decline to use two-factor login security, a feature the software company can turn on with a click, because firm leaders (owners and partners at the firm) consider it too cumbersome. As more firms transition to cloud-based systems, failing to properly configure access controls, encrypt stored documents, or restrict public exposure of databases can allow attackers direct access without needing to exploit traditional technical vulnerabilities.

A successful cyberattack can bring a law firm to its knees. Attorneys may lose access to all active case files. Staff may be locked out of the billing system. Deadlines can be missed, motions may not be filed, and the court may be unsympathetic to technical delays. Every hour lost to a

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
August 2025

breach costs the firm in billable time and damages client relationships.

Real-world examples of high-stakes data breaches

Successful cyberattacks happen every day, yet most are never made public. Still, we see regular public announcements of law firms being breached. Those that are made public represent only a tiny fraction of successful attacks. Whether because of state-specific reporting requirements, uncertainty over what was compromised, or private ransom payments, the public, regulators and law firms remain unaware of how widespread these attacks have become. In reality, countless firms have faced ransomware attacks, paid ransoms, or lost funds to bad actors, without ever directly notifying clients or disclosing the event publicly. Nearly every lawyer seems to know at least one firm that has experienced a significant cyber event, underscoring just how pervasive and underreported these threats truly are.

Understanding your network and securing it

Securing a law firm begins with understanding where your data lives and how your network operates. For many practices, especially those that have evolved over time or adopted hybrid-work models, that answer may be more complex than expected. Data may be scattered across local servers, cloud storage, third-party platforms, and personal devices, each of which presents different risks and requires specific safeguards.

A firm's network is not just its internet connection; it is every connected device, user, software platform, email account, and communication channel. On-premises setups involve physical servers located in the office, which can offer greater perceived control, but demand constant updates, secure backup systems, restricted remote access and physical protections. On the other hand, cloud-based platforms offload infrastructure maintenance to providers but still require strict access controls, encryption, user monitoring, and due diligence on vendor security.

The hybrid model, now common across the legal field, requires a synchronized and consistent cybersecurity strategy. It is not enough to secure just one side. Data flowing between cloud and local systems must be encrypted, user credentials must be protected across both environments, and IT oversight must cover every platform equally.

How to talk cybersecurity with your IT team

Cybersecurity does not fall solely on IT, but the strength of your defenses depends on the quality of your support. Whether you have in-house personnel or an outside vendor, your firm's leadership must engage directly. Delegating without understanding is what leads to blind spots and breaches.

First, make sure that your IT consultant can explain the answers in plain English. If you get deflection, confusion, or jargon-heavy responses, that is a warning sign. If you have any doubt about their cybersecurity expertise, get an outside review from a recommended cybersecurity firm.

Ask simple questions and expect clear answers. Ask them to rate your security and identify vulnerabilities. Ask about the cost and work involved in improving any known weakness.

Cybersecurity discussion questions:

- Where is our sensitive data stored, and how is it protected? Has the restoration process been tested recently? Many firms only discover flaws in their backups during a crisis, when it is already too late.
- Who has network access, and how is that access granted, monitored, and revoked?
- Is multifactor authentication implemented across all systems including email and network administrators/privileged users?
- Are personal devices allowed access to firm resources, and if so, under what controls?
- Are our backups isolated, encrypted, and tested regularly?
- What alerts or monitoring do we have in place? Do we have endpoint detection and response systems? How would someone be informed in the case of an incident?
- What would we do today if we experienced a breach?
- How can we strengthen our cybersecurity culture and improve our current employee training?

Through answering the questions honestly and thoroughly, law firms can be proactive rather than reactive. True security does not mean preventing all attacks, but being resilient with the capacity for reaction, containment, and quick recovery when one does take place.

Does employee training really matter?

Without a doubt, employee training is usually the most overlooked aspect of a cybersecurity strategy. However, there is not any antivirus product, detection tool, or firewall that can rival a watchful, informed workforce. The greatest cyber weakness for any organization is the human factor, but it is also the greatest potential defense.

Attorneys, paralegals, assistants, and administrative staff handle sensitive information daily. An impersonated vendor or well-crafted phishing email could easily trick even the best of professionals, especially amid high-pressure or high-volume periods. Training for that reason cannot be a one-and-done deal in onboarding. It must be ongoing, focused, and energized by authentic, real-life scenarios.

The most effective programs use short interactive sessions and open dialogue to foster awareness and build reflexes. When employees understand the tactics attackers use and feel empowered to speak up about suspicious activity, the firm becomes significantly harder to penetrate.

Culture matters too. Employees should never be afraid to report mistakes. Fear of blame or disciplinary action can delay reporting, giving threats more time to spread. Instead, leadership must frame training as a form of empowerment, a way

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
August 2025

for every individual to actively protect the firm, clients, and themselves.

When security awareness becomes part of the firm's DNA, it creates a ripple effect. People pause before clicking links. They double-check sender addresses. They know how to verify wire instructions. They become part of the defense.

Insuring against cyber events: What your BOP or legal-malpractice policy does not cover

Many law firms hope or assume their liability and property (package), Business Owner's Policy (BOP), or legal-malpractice insurance will step in during a cyber event. But most of these policies include little, if any, meaningful cyber coverage; and even when they do, the limits are often far too low, and the coverage is severely limited. It is meant only to be a basic grant of liability coverage. This leaves firms dangerously exposed.

Cyber-insurance considerations

Robust, standalone cyber insurance is now essential for law firms. While there is no universal industry standard for coverage or policy language, there is increasing consensus around key coverage components, making cyber-insurance quotes more easily comparable. There are two main categories of coverage included: first-party coverage, which addresses direct losses to the firm, and third-party coverage, which applies to liability arising from the breach.

First-party coverage typically includes breach response and remediation, business interruption, ransom payment, cybercrime, and social-engineering losses. Third-party coverage addresses the firm's liability to others, including cyber and privacy liability, regulatory fines, and the cost of defense during investigations.

Equally important, many policies grant access to breach-response teams. These are specialists who can guide your firm through every step of the crisis, technical, legal, and reputational. They often assist with securing the point of breach, negotiating with bad actors, and even paying the ransom.

Watch for the word "reimbursement" in your cyber-insurance proposal or policy. This indicates that the firm would be responsible for paying, and possibly negotiating, the ransom upfront and then seeking reimbursement from the insurer afterward. "Pay on behalf" coverage, which is widely available, is preferred over reimbursement since it allows the insurer to handle the payment directly.

Finally, carefully consider when or if your firm sends wire transfers. Wires are frequent targets of bad actors and some cyber-insurance policies have a "callback" requirement for coverage related to funds-transfer fraud. These requirements only grant coverage if the firm called to verify a wire request before sending.

Cyber insurance is not going to prevent an attack, but it is going to provide experts to help you recover and protect the firm from significant financial loss.

Social engineering and funds-transfer fraud coverage via cyber insurance and crime insurance

Neither cyber insurance nor crime insurance were initially designed to cover the new threat of social engineering. The cyber policy was meant to cover hacks, intrusions, breaches, compromise, but social engineering often occurs without any of those triggers. Commercial-crime policies were designed to cover direct theft, computer fraud (where a computer system is directly manipulated by an external party), or funds-transfer fraud where the bank itself is duped.

Both provide other valuable coverage for law firms not covered by the other and most firms can greatly benefit from having both and maximizing the social-engineering coverage available from each. Even with the social-engineering limit maximized on both, the total combined limit may only be $350-$500k.

In the event of a claim that may trigger both the policies, the "other insurance" provision could lead to a pro rata situation for loss payment. Alternatively, the policies can sometimes be "coordinated," where one is primary and the other excess. Ideally the policy with a lower retention/deductible is made primary.

Depending on the total coverage available for social engineering, a firm may also consider obtaining separate excess social-engineering coverage via a separate policy.

A final word on accountability and leadership

For law-firm leaders, cybersecurity is no longer something to delegate blindly or revisit once a year. It is a moving target that demands ongoing attention, clear communication, and personal involvement. The decisions made at the top, about budgets, training priorities, vendor contracts, and insurance coverage, determine the firm's overall resilience.

Cybersecurity leadership does not mean solving every technical challenge, but it does mean setting the tone, asking the right questions, and ensuring that security is not treated as an afterthought, but as a cornerstone of ethical, modern legal practice.

Marcus Cusick is an insurance and risk advisor. He is the founder of Cusick Insurance Brokers, Ltd., *a specialized brokerage that has served the legal sector's insurance needs for over 20 years.*