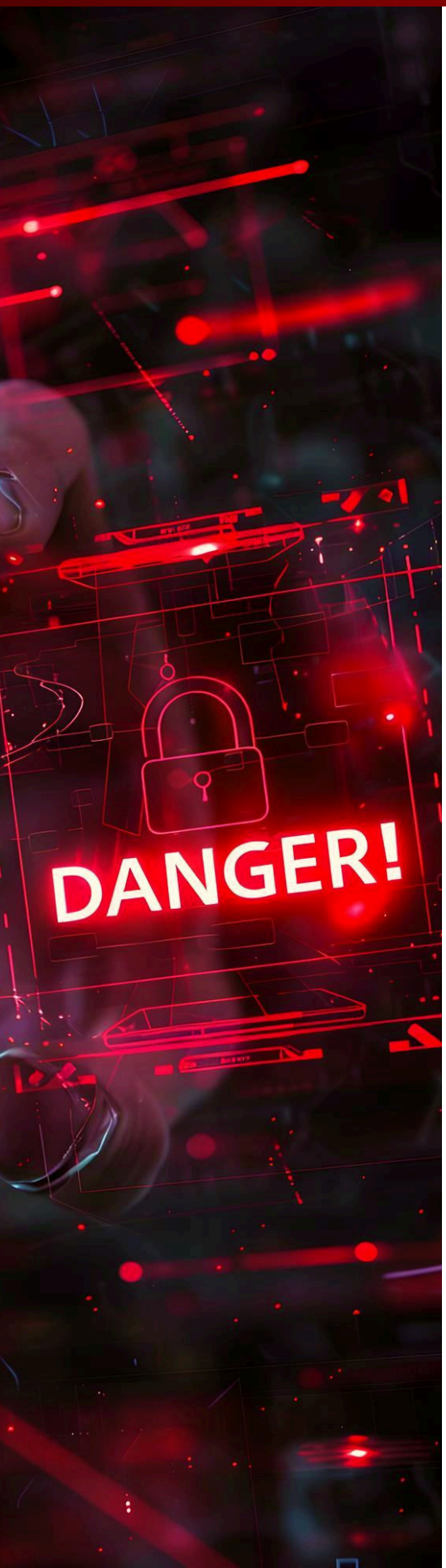
RIZE™ TECHNOLOGIES

8 Cybersecurity Threats Facing Mid-Sized Law Firms in 2026

www.rizetechnologies.com | info@rizetechnologies.com

Table of Contents



You Need to Protect Your Practice in Today's Evolving Digital Landscape

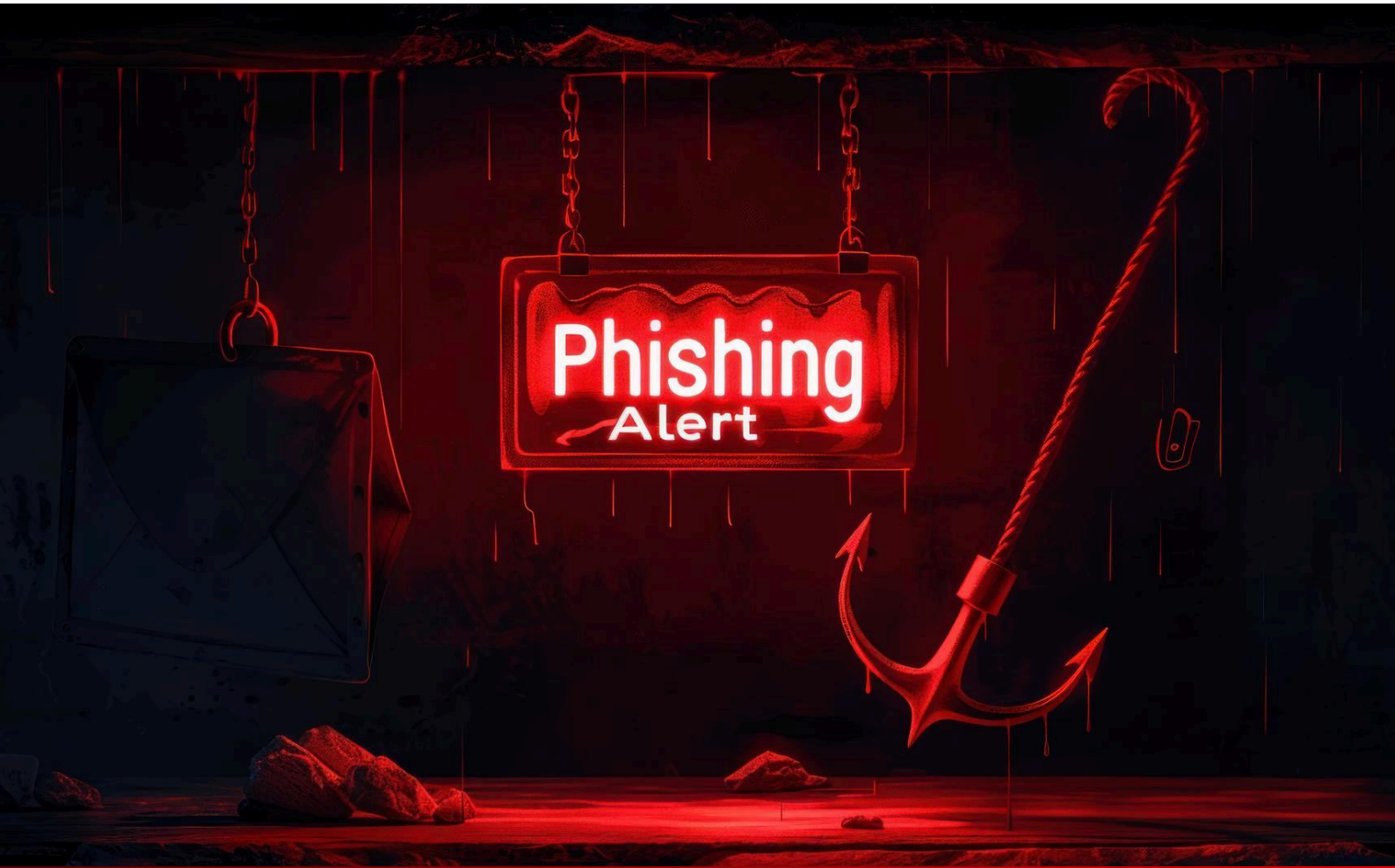
According to various industry research reports, nearly 90,000 law firms across the US have been the target of cyberattacks in 2025. When an attack is successful, data is compromised, and operations are disrupted, the average cost to a law firm is $5.08M.

If your firm hasn't yet been a victim, that's great. But don't be overconfident. The legal profession is a prime target for cybercriminals because law firms deal with valuable client data, financial information, and confidential case materials. If those things are valuable to you, then they're valuable to cybercriminals because they know you will be willing to pay a ransom to protect that data.

In 2026, cyberattack opportunities will keep expanding — driven by more aggressive ransomware groups, generative AI tools in the hands of attackers, fractured privacy rules across jurisdictions, and complex third-party ecosystems. **Despite these threats, many law firms simply don't make cybersecurity a priority until it's too late.** As we look ahead into 2026, there are eight critical cyber risks that mid-sized firms should be aware of – and prepared for.

01 AI-Powered Phishing and Social Engineering

Cybercriminals are leveraging artificial intelligence to create hyper-realistic phishing emails, voice clones, and deepfake videos. These AI tools enable cybercriminals to easily scale and accelerate sophisticated attacks that can impersonate senior partners, clients, or opposing counsel with alarming accuracy. Mid-sized firms often lack the extensive security training programs of larger organizations, making staff more vulnerable to convincing scams that can lead to wire fraud, credential theft, or data breaches.



02 Ransomware Targeting Legal Data

Ransomware attacks, which often follow social engineering events, continue to evolve, with criminals specifically targeting law firms due to their sensitive client information and pressure to maintain confidentiality. Ransomware is no longer just file-locking. Attackers now employ double and triple extortion tactics—encrypting data, threatening to release it publicly, and contacting clients directly. The reputational damage and ethical obligations make law firms more likely to pay ransoms, and that makes them attractive targets. Prepare for fast, high-impact incidents by hardening data backups, isolating critical systems, and preparing a comprehensive incident response plan.

03 Business Email Compromise (BEC)

Cybercriminals can exploit network vulnerabilities to gain access to the email accounts of leaders within a law firm. Once that happens, they quietly monitor communications on specific cases for days, weeks or even months at a time. Then, when the time is right, cybercriminals generate seemingly authentic emails from a compromised account to initiate wire transfers associated with cases involving cash settlements, real estate sales, client retainers, and more. These attacks often exploit the urgent nature of legal deadlines and large sums in trust accounts. Strengthen your defense with identity and access management (IAM) tools, email security, automated threat detection, and strict approval workflows for financial transactions.

04 Supply Chain Vulnerabilities

Your firm's security is only as strong as the weakest vendor in your supply chain of information partners. Law firms rely on cloud providers, eDiscovery vendors, expert-witness platforms, and more. Mid-sized firms often work with numerous third-party vendors without a comprehensive vetting process, creating blind spots in their security posture. Each vendor can serve as an entry point for attackers, and a breach at any one vendor can quickly cascade into your firm without your knowledge. Implement strict least-privilege access, vendor security assessments, and segmentation of third-party connections — and require vendors to demonstrate SOC2, NIST, and ISO compliance and incident response plans.

05 Insider Threats and Data Exfiltration

Disgruntled employees, departing attorneys, or compromised credentials can lead to intentional or accidental data breaches. The legal industry's high turnover rates and the competitive nature of lateral moves increase this risk. Data exfiltration can be subtle and, without proper access controls and monitoring systems, departing staff may take client lists, case strategies, or confidential documents to competing firms. Policies for offboarding, forensics-ready logging, endpoint DLP (data loss prevention), and clear rules about client data ownership help limit your exposure.

06 Cloud Misconfigurations

As law firms increasingly adopt cloud-based practice management and document storage solutions, misconfigured settings create significant vulnerabilities. Publicly accessible case files, improper sharing permissions, and weak authentication protocols can expose confidential client information. Many mid-sized firms migrate to the cloud without leveraging dedicated IT security expertise to properly configure and monitor these systems. Regular cloud posture reviews, automated configuration scanning, and strict IAM policies help to reduce this risk. And always be sure to encrypt sensitive data in transit and at rest.

07 Authentication Attacks & MFA Bypass

To ensure that the identity and access rights of an employee are properly validated, most law firms require multi-factor authentication (MFA) as part of the user login process. This is essential, but attackers increasingly use “MFA fatigue” (repeated push notifications) and session hijacking to trick users into approving logins. Strengthen login controls by favoring phishing-resistant MFA methods (FIDO2/security keys), conditional access policies, and blocking high-risk authentication attempts. Be sure to monitor and alert when you detect any anomalous login behavior

08 Zero-Day Vulnerabilities in Legacy Systems

Mid-sized firms often run a mix of modern services and legacy on-premise apps that don’t receive timely and continuous security updates. These include older practice management software, document management systems, or outdated operating systems due to cost constraints or integration challenges. These legacy systems often contain unpatched vulnerabilities. Attackers scan for known and zero-day vulnerabilities to gain footholds. Reduce your risk with a rigorous vulnerability-management program, prioritized patching, application inventory, and compensating controls if patching is delayed.

Summary and Next Steps

Perhaps the most critical vulnerability is the lack of a comprehensive incident response plan. When breaches occur, firms without clear protocols waste valuable time, make poor decisions under pressure, and fail to meet ethical notification requirements. The absence of regular security training, tabletop exercises, and relationships with forensic specialists and cyber insurance carriers can transform a manageable incident into a firm-ending crisis.

That's why mid-sized law firms must recognize that cybersecurity is not merely an IT issue—it's a fundamental business risk and ethical obligation. The threats outlined here require a multi-layered approach combining technology solutions, staff training, vendor management, and if necessary, strategic IT services and support from a respected MSP.

Start by conducting a comprehensive security assessment and establishing clear policies for data handling and device usage. Regular security awareness training should be mandatory for all staff, not just IT personnel. Consider engaging cybersecurity consultants who specialize in law firm environments and ensure your cyber insurance coverage aligns with your actual risk profile.

The legal profession demands the highest standards of client confidentiality and data protection. By proactively addressing these top cybersecurity threats, your firm can protect client trust, maintain ethical obligations, and ensure business continuity in an increasingly dangerous digital environment.

About Rize Technologies

At Rize Technologies, we understand the complex cybersecurity challenges facing law firms today. For more than 10 years, we have been the trusted technology partner for law firms across the US, addressing project needs and providing comprehensive co-managed IT services that allow attorneys to focus on what they do best - serving their clients. Rize Technologies offers a free IT assessment service to law firms that are concerned about their security posture and ability to defend against the complex cyberattacks described in this document. To be clear, there is no cost or obligation. Learn more about Rize Technologies and schedule a convenient date and time for your free IT assessment report.

rizetechnologies.com