Cyberattacks on Law Firms Are Rising. Here's What's Driving It.

By Michael C. Maschke, Sharon D. Nelson, Esq., and John W. Simek

Law firms have always been attractive targets for cyberattacks. That part is not new. What is new is the pace, scale, and success rate of those attacks.

According to a recent annual data security report highlighted by FindLaw, attacks on law firms are not only ongoing but also increasing. In some categories, incidents nearly doubled year over year, primarily driven by ransomware campaigns that show no signs of slowing down. The report clearly indicates that law firms are firmly in the crosshairs.

This is no longer solely a concern for the tech department; it has become a business risk and, more recently, a legal ethics issue as well.

The Attack Surface Is Expanding

The FindLaw report explains how attackers gain access, and it's not usually very clever. Phishing remains one of the main ways breaches happen. Third-party vendors are also a big weak spot, involved in about a quarter of incidents. In other words, attackers aren't breaking down the front door. They're walking right in because someone clicked a link or a vendor relationship created a direct way in. This should change how companies view cybersecurity. It's not about just defending the perimeter. It's about human behavior, managing vendors, and internal controls.

Ransomware Has Become a Business Model

Once inside, attackers usually act openly by stealing data, encrypting systems, and demanding payment – sometimes all three. The report highlights how expensive this has become. Average ransom demands have risen above $4 million, a significant jump from the previous year, while actual payments are still averaging in the hundreds of thousands. Add in the costs of forensic investigations, downtime, regulatory notifications, and reputation damage, and the financial impact quickly adds up. This is no longer a random crime; it's a structured business model, with law firms being prime targets due to the data they hold and the urgency to regain access.

The AI Factor Makes It Worse

The report also notes that attackers are increasingly using artificial intelligence to scale and enhance the effectiveness of their campaigns. Phishing emails are more convincing,

social engineering is more targeted, and attacks can be spread across organizations with minimal effort.

At the same time, companies are creating their own risks with what the report calls shadow AI. Employees using unauthorized AI tools might accidentally expose sensitive information or open new vulnerabilities in company systems. This results in a dual-risk environment, where AI is both a tool that attackers can exploit and a liability for the company when used without proper oversight.

As an example, don't ask AI how to open a port in an XYZ firewall running 123 version of the software. You've then potentially exposed a security technology used at your firm.

Why This Is a Legal Problem

Law firms are different from other businesses. They manage confidential client information, data, litigation strategies, and privileged communications. When that data is compromised, the fallout extends beyond just operational issues.

The report emphasizes the downstream implications, including breach-notification obligations, potential contractual breaches, and ethical duties related to confidentiality. Additionally, client expectations are rising. Clients expect their law firms to safeguard sensitive information. When that expectation is not met, the consequences go beyond financial loss. They can damage reputation and, in some cases, pose an existential threat.

The Real Issue Is Not Technology

It's easy to see this as just a technology problem. Upgrade the firewall. Add another security tool. Run another scan. But that misses the point.

The report emphasizes what many in the industry already understand. Most breaches are not caused by sophisticated attacks but by basic failures. These include unpatched systems, poor credential management, lack of user training, and weak vendor oversight.

These are governance failures, not technical limitations.

What Firms Should Actually Be Doing

If attacks are increasing and becoming more costly, responses cannot be incremental. Firms need to concentrate on fundamentals.

First, strengthen user awareness and phishing defenses. Your greatest vulnerability remains your people.

Second, strengthen vendor risk management. If a third party can access your systems, they are part of your security posture, whether you like it or not.

Third, implement a real incident response plan. Not just a document that sits on a shelf, but a proven process that can be executed under pressure.

Fourth, control the use of AI tools within the organization. Unauthorized experimentation with sensitive data isn't innovation; it's a risk.

The Bottom Line

Cyberattacks on law firms are here to stay. The report makes that clear. The real question isn't whether firms will be targeted, but whether they are prepared. The harsh truth is that many are not.

And when a breach occurs, it won't be blamed on the hacker. Instead, it will be blamed on the firm that didn't take the risk seriously enough.

That is no longer a technology failure; it's a leadership failure.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com.*