The Foundation of Client Confidentiality is Rooted in Sound Law Firm Cybersecurity

This article was authored by Brian Boetig and Todd Renner, Senior Managing Directors, FTI Cybersecurity.

Law firms routinely partner with external cybersecurity experts to advise clients on the importance of proper cybersecurity practices to mitigate threats, but have recently experienced an uptick in cyber attacks facing their own organizations.[1] Threat actors looking for sensitive information use law firms as a soft access point to client data. While exposure of privileged and confidential information could be damaging to a client, it could have even more serious consequences for a law firm. The reputational impact of having lost client data, combined with mishandling the response, is challenging to overcome. By assessing internal controls and hardening defenses, law firms can better protect their assets and their clients from damaging cybersecurity attacks.

Why Do Threat Actors Target Law Firms?

Law firms generate the type of valuable data that threat actors seek; they are targeted because of their access to sensitive client data that they ultimately possess on their systems. When clients share sensitive and proprietary information with law firms, threat actors see an opportunity to access this coveted data through a potentially more vulnerable third party, rather than directly through the target organization.

Once a threat actor gains access to law firm networks, they can:

- Steal sensitive and proprietary information to hold for ransom or sell on the dark web
- Corrupt or destroy evidence collected in e-discovery to ruin cases
- Leak intellectual property (IP) patents before they are fully secured
- Use data to undermine legal negotiations
- Prevent law firms from accessing client or third-party systems
- Trigger breach notification rules and regulations for the law firm
- Prevent billable work for extended periods of time

How Can Law Firms Mitigate Cybersecurity Risk?

Law firms have a professional obligation to implement sound cybersecurity measures to protect their clients and their own practices. The sensitive nature of the information law firms handle daily requires participation from every

law firm employee and more than just basic cybersecurity practices. A focus on cybersecurity should be a fundamental business practice across all networks, devices, and personnel, from mobile devices and AI tools to operational cybersecurity training for all employees. Proper cybersecurity hygiene for law firms includes, but is not limited to:

Device Policies and Best Practices

Law firms should have bring your own device (BYOD) policies in place covering proper use of mobile devices, such as not using work devices for personal use. This also includes implementing multi-factor authentication (MFA) wherever possible, requiring employees to verify unsolicited requests for information before it is provided, and ensuring that systems and tools are regularly patched and updated.

Zero-Trust Architecture

Implementing a zero-trust architecture, meaning that all internal and external parties must be verified before accessing networks, adds additional protections to critical data. Further, limiting access to sensitive information to only those who need it creates fewer entry points for threat actors to exploit.

Conducting a Cybersecurity Maturity Assessment

Law firms should determine the current state of their cybersecurity practices, and identify any gaps that may exist in their infrastructure, through a cybersecurity maturity assessment using the National Institute of Standards and Technology (NIST) Cybersecurity Framework or other industry framework to ensure adherence to best practices. External experts can assist with assessments and provide recommendations for identified vulnerabilities.

Incident Response Planning

Having an incident response plan in place that includes not only how to contain an incident, but also how to continue helping clients if networks and servers are down, will reduce business disruption and allow for a speedier recovery in the event of a cybersecurity incident. This plan should also include considerations on creating a spin-off company after an incident, allowing for an immediate transition to a new infrastructure, if necessary, to continue operations.

Incident Response Training

Incident response plans are only effective if all involved parties understand their role in the response ahead of time. Training sessions, including table-top crisis simulation exercises, allow stakeholders to fully understand what is expected of them during an incident response, and for organizations to experience what could go wrong and how to mitigate those occurrences, before a real crisis takes place.

When clients are well-protected, law firms become the next target for threat actors looking to gain access to confidential and valuable information. While it is imperative to advise clients on the importance of proper cybersecurity measures, it is equally as vital for law firms to protect against the cybersecurity threats they face.

---

[1] Sam Skolnik, Skye Witley, Olivia Cohen, "Law Firm Cyberattacks Grow, Putting Operations in Legal Peril," Bloomberg Law (July 7, 2023), https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril.
