withum

How To Manage 6 Risks Affecting Cybersecurity for Law Firms

By Chris Mangano | cmangano@withum.com

Cybercriminals are increasingly targeting law firms; extortion is quickly realized, given the nature of highly confidential client data. Cybersecurity for law firms is a top priority today, as the digital footprint is constantly expanding, leading to more entrances to a firm's network infrastructure, which is a direct gateway to data. This expansion, combined with insider risks (a firm's own staff), makes having risk-control protocols of paramount importance.

We are all "custodians of data." Law firms specifically are stewards of some of the most sensitive information stored and shared; a fact that doesn't elude nefarious cybercriminal syndicates. Below are some of the top cybersecurity risks affecting law firms:

DISTRIBUTED DENIAL-OF-SERVICE (DDOS): Deliberate attempt to disrupt the traffic of a targeted edge device, network, or service by flooding the target with a surge of Internet traffic. Executed properly, a DDoS can bring down communications and result in massive disruption.

RANSOMWARE: Files/data are encrypted-locked-down, accompanied by a demand for money (generally Bitcoin) in exchange for a "key" to unlock the data. Once data is manipulated, future access remains a threat; paying the ransom is never advisable.

PHISHING: This tool is used to open the door to data control. Nefarious code, better known as malware, is embedded in an email. It generally asks the recipient to open a file or click on a link, launching a "payload" that propagates across the connected infrastructure, rendering much of the affected systems "locked." This leads to the "criminal ask," which is money for your data.

DATA BREACHES: Rather than locking data, the criminal will extract sensitive files/information with the intent to sell on the Dark-Web and/or "sell back" to the law firm of origination. Control of data can lead to a variety of extortion tactics.

WEBSITE COMPROMISE: Lawyers visit and use legitimate websites as a routine part of their investigative research. Many websites are not secure; this results in the delivery of code (Malware) nested in a user's system, often remaining dormant for months. The criminal can use the malware as a "window" to activity, ultimately scrapping data and/or locking files.

ENVIRONMENTAL CYBER THREATS: If law firms take little to no action in establishing best practices for data management, it makes a negligence suit more likely, in the event of a breach. Additionally, a lack of controls, policies and procedures allows disgruntled current/former staff to retaliate against the firm.

When an event, incident or breach becomes apparent, it's too late; the firm is in reactive mode, attempting to mitigate reputational harm, financial loss and widespread attention. Establishing cybersecurity compliance standards isn't just about adhering to what is "required", it is about doing what is necessary to operate in today's digital landscape.

According to the American Bar Association, virtual work environments (resulting from the pandemic) have fueled a sharp increase in breaches (25% up-tick). Federal laws governing cybersecurity are constantly evolving; this is no different for law firms. Clients span a wide range of industries; the required rules of engagement around cybersecurity best practices make a law firm's state of "readiness" a differentiator in obtaining and retaining a client.

The sensitivity of data in the financial and healthcare arenas translates to increased security safeguards that are expected on the part of the law firm involved. Accounting professionals must adhere to the Sarbanes–Oxley Act of 2002; this brings expanded commitments for law firms representing those markets.

Each state imposes its requirements; keeping up with these evolving standards has become a topic discussed at the highest leadership level. Past expectations have placed responsibility on members of a firm's Information Technology (IT) team (Chief Information Officer and/or Chief Technology Officer). Historically, these leaders are more fluent in modeling technology architecture, not managing governance. The result has been a confused understanding of who "owns" cybersecurity. Building out policies, procedures, internal controls, incident-response plans, continuance-of-operation protocols and security-awareness training often gets passed around between compliance, human resources, operations and IT.

Frameworks like NIST (National Institute of Standards and Technology) provide boundaries for law firms to demonstrate that they've made "best-effort" changes within their environments to align with requirements. Many law firms have neglected technology, expecting computers and primary network infrastructure to "last forever"; this is impractical and extremely risky. The need to refresh technology, maintain current operating systems, instill multi-form-authentication, perform an annual cyber risk assessment, an annual penetration test and routinely augment policies and procedures should be top-of-list in operational planning.

Law firm's engagement in strong cybersecurity practices results from one of three triggers: an active breach has occurred, resulting in damage-control/incident-response being deployed to mitigate loss; a regulatory/compliance requirement has moved the needle from "recommended" to "required"; or a firm proactively positions a cybersecurity hygiene model to be ahead of an inevitable compromise. Endeavor to subscribe to the latter.

For more information on this topic, please contact a member of Withum's Cyber and Information Security Services team.