Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Tips For Law Firms To Maximize Cyber Coverage

By **Jeff Sistrunk**

Law360, New York (May 10, 2016, 8:00 PM EDT) -- Edelson PC's recent putative privacy class action alleging a Chicago-based regional law firm failed to take measures to effectively safeguard sensitive client data highlights the need for firms to obtain expansive cyber liability coverage.

There is a misconception among firms that adding a "network endorsement" to their lawyers' professional liability policy will cover most cyber risks, but that isn't the case, according to Eileen Garczynski, senior vice president of specialty insurance brokerage Ames & Gough.

"A lot of lawyers may think that adding a network endorsement to their professional liability policies will fill the gaps, but that endorsement typically doesn't cover lost billable time, regulatory fines or credit monitoring," Garczynski said. "They typically only cover the costs to fix your system."

As a result, purchasing a standalone cyber policy has become a must for law firms, Garczynski said.

Here, experts delve into what firms should do to make sure they're protected from cyber risks.

Ensure Confidential Client Info Is Covered

Law firms routinely handle a wide variety of confidential client data, including information about clients' business practices and intellectual property and details about legal strategies.

And because many cyber policies only cover claims resulting from the theft or inadvertent disclosure of personally identifiable information such as birth dates and Social Security numbers, it is crucial for a law firm to obtain a cyber policy with a definition of "confidential information" that encompasses all materials that fall under the attorney-client privilege.

"A law firm will have some [personally identifiable information], but perhaps the bigger concern is that someone will steal the firm's strategy, a client's intellectual property or confidential emails," Garczynski said.

The **proposed class action** that Edelson lodged against a Chicago-based regional law firm, which is currently under seal, illustrates firms' needs for a cyber policy with a broad definition of confidential information.

Edelson founder and CEO Jay Edelson told Law360 last week that the complaint alleges the unidentified law firm suffered from a "number of significant data security vulnerabilities," which resulted in "anyone with nefarious intent" — even if they were not a sophisticated hacker — likely being able to gain access to a "whole host of sensitive client data," including the law firm's line-item billing records and possibly email contents.

An effective cyber policy will offer coverage for claims stemming from the exposure of a full spectrum of client data, experts say.

Get a Broad Loss Definition

With all the potential costs and liabilities associated with data breach incidents, law firms must ensure that the definition of "loss" in their cyber policies is broad enough to extend coverage to expenses resulting from first-party and third-party risks. Examples of first-party risks include damage to the firm's own computer network, and third-party risks could be privacy class action complaints, as well as expenses tied to regulatory investigations, experts say.

First-party coverage can be particularly important for law firms because if a firm's network goes down for even a few days, attorneys may lose all that billable time, according to experts. But a cyber policy can reimburse a firm for lost net profit before taxes, Garczynski noted.

"A cyber policy will cover that lost billable time by averaging the last three months' billables," Garczynski said. "That way, a firm won't skip a beat."

Firms should also make sure that a cyber policy includes coverage for the costs of responding to investigations by both U.S. and foreign regulators, along with any potential regulatory penalties, experts say.

"For the better products, the coverage territory is worldwide, and there is not much of a distinction about the regulatory scheme that is the impetus for the loss," said Greg Podolak, leader of Saxe Doernberger & Vita PC's cyber risk practice.

Make the Policy Primary

Law firms should be careful to seek out cyber policies that provide primary coverage, which will respond immediately in the event of a data breach or other cyber incidents, according to experts.

"Probably eight of 10 cyber policies say they are excess over any other insurance," Garczynski said. "You really have to have a broker or someone who understands what they're reading to get you a policy that is going to respond timely and appropriately."

If a cyber policy provides excess rather than primary coverage, a law firm would likely have to exhaust other valuable forms of insurance, such as professional liability coverage, in order to tap the cyberinsurance.

"For example, you don't want your professional liability policy to be eaten up covering data breach-related costs when it should be reserved for legal malpractice claims," Garczynski said.

Include Cloud Providers

Like other businesses, many law firms have started to store more data in the cloud rather than on computer servers located onsite.

As a result, firms that use third-party cloud storage vendors to store sensitive data should make sure that a policy's definition of "computer network" encompasses those cloud providers, experts say. Otherwise, any claims that ensue if confidential information is stolen from a cloud provider may not be covered.

"To the extent a law firm is relying on cloud providers for storage, processing or some other service, 'cloud' or 'outsourced support' should be included in the policy's definition of a network," said Barnes & Thornburg LLP partner Scott Godes.

In lieu of a specific reference to cloud providers, some cyber policies will define a computer system as a system owned by, leased by or operated on behalf of the policyholder, according to experts.

"You can pick up coverage that way," Godes said.

--Editing by Christine Chun and Philip Shea.