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

Law Firms View Cyber Coverage As Hot Ticket, Broker Says

By **Allison Grande**

Law360, New York (May 12, 2016, 11:39 PM ET) -- Law firms are increasingly snatching up cyber-specific insurance policies, as the growing exposure that firms are facing from cyber incidents begins to reveal gaps in their long relied-upon coverage, a Wells Fargo Insurance broker said Thursday while speaking on a panel about maximizing cyber insurance coverage in a range of industries.

Joshua Gold of Anderson Kill (from left), Meredith Schnur of Wells Fargo Insurance, Michael Hart of Isle of Capri Casinos, and Darin McMullen of Anderson Kill discuss cyberinsurance coverage at an Anderson Kill conference in New York on Thursday. (Credit: Allison Grande/Law360)

During Anderson Kill PC's second annual Cyber Insurance Recovery Conference in New York, Joshua Gold, the chair of the law firm's cyber insurance recovery group, broached the subject of the mounting cybersecurity risks facing law firms and other professional services. He pointed to examples such as the release of the so-called Panama Papers that exposed data held by a Panamanian law firm and reports that firms including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP had suffered data breaches by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies.

"Lawyers are now in the crosshairs," Gold said, before asking panelists what approach lawyers should be taking to obtaining coverage for claims related to cybersecurity incidents.

"Do we have to buy a cyber policy, or as professionals, are we still covered under our good old-fashioned [directors and officers] and malpractice insurance for something that clearly fits within this broad label of cyber?" he asked.

Meredith Schnur, senior vice president for the professional risk practice at Wells Fargo Insurance, responded that her firm has witnessed an increase in the purchasing of cyber insurance by law firms over the past two years, an uptick that she attributed largely to the growing realization that traditional coverage was not quite as comprehensive as many lawyers had once believed.

"Prior to a couple of years ago ... most lawyers you could have a conversation with, they were fairly certain and felt pretty secure that their malpractice policies would cover them for what they needed to be covered for," Schnur said.

But while many malpractice policies do cover the liability arising out of the failure to protect the privacy of confidential information, some other increasingly common cyber claims related to crisis management, the costs incurred to deal with an incident, cyber extortion and first-party business interruption are generally not covered under standard malpractice policies, according to Schnur.

"There's a lot of coverage that's not included," she said. "So today, what a lot of cyber carriers are doing are tailoring their cyber policies to sit difference and conditions over the [malpractice policy] where there is no coverage."

In crafting these policies designed specifically for the law firm community, the ultimate goal is to "make sure those policies are talking so that policy is filling in the gaps, while this policy is doing what it's supposed to be doing," according to Schnur.

"There's been a lot of evolution in I would say the past 12 months," she added.

Securing the appropriate coverage is becoming increasingly important in the wake of steps being taken by the plaintiffs bar to turn up the heat on attorneys and their law firms, the panelists added.

On May 5, plaintiffs firm Edelson PC revealed that it is moving to lift the veil on a putative privacy class action that it recently filed against a Chicago-based regional law firm that it accuses of failing to maintain robust data security practices. And last month, a New York couple filed a suit accusing their real estate attorney of negligently using a "notoriously vulnerable" AOL email account that was hacked by cybercriminals.

"What law firms can expect in the wake of a data breach is to have claims brought against them that really buck up against this being malpractice," Darin McMullen, co-chair of Anderson Kill's cyber insurance recovery group, said during the panel.

Although the claim environment for cyber has so far been "pretty good" because "nobody wants to be that carrier that is denying claims because the market is competitive," coverage for claims lodged against law firms isn't going to be cut-and-dry, and there's likely to be a "pivot point" where these types of professional liability cyber-related claims are going to run up against staunch resistance from carriers, according to McMullen.

"It's just too tantalizing for your carriers not to try to look for a gap," he said.

The risk of coverage holes when it comes to cyber claims is by no means limited to the legal industry, the panelists at the conference said.

Retailers that may think they are covered for costs that stem from an alleged breach of the Payment Card Industry's Data Security Standard may be surprised to discover that their policy covers assessments but not fines or penalties, or that coverage is barred by a breach of contract exclusion, while businesses in other sectors may be taken aback when they find that their crime insurance doesn't cover losses that stem from social engineering attacks, according to the panelists.

"Every carrier does it differently," Schnur said.

In light of these deviations, it's vital that businesses keep in mind that there are no one-size-fits-all

policies when it comes to cyber coverage, and that mapping out the specific financial and physical damages that they could incur from a cyber attack is likely to go a long way in helping them secure the most comprehensive coverage possible.

"Know what your exposure base is, tailor that coverage to the exposure bases," Mark Millard, a senior manager in Ernst & Young LLP's corporate insurance risk management and claims advisory services practice, said, adding that when purchasing cyber insurance, "nothing is certain, everything is up for negotiation."

Companies would also be wise to keep an eye on the growing regulatory and legal landscape for cybersecurity. In addition to enforcers such as the Federal Trade Commission and state attorneys general stepping up their activities in this space, the plaintiffs bar is becoming emboldened by favorable decisions that have recently been handed down in data security cases, including the Seventh Circuit's revival of putative data breach class actions against The Neiman Marcus Group LLC and P.F. Chang's China Bistro Inc. during the past year.

"Neiman Marcus was a real anomaly this year, and that actually proved to be a game-changer and has gotten some folks worried," Schnur said. "There's been no shift in the market or the pricing because of Neiman Marcus ruling, but if those increase and we start to see more payments by insurers for actual third-party liability and more settlements, of course there's going to be an answer to that."

--Editing by Catherine Sum.