New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 34
WEDNESDAY, AUGUST 19, 2015

Cybersecurity Data Sharing Is Now Available to Law Firms

BY CHRISTINE SIMMONS

LAW FIRMS now have access to a platform that allows them to share data on cybersecurity threats anonymously.

The Legal Services Information Sharing and Analysis Organization or LS-ISAO will announce its launch on Wednesday and will alert firms to potential cyber threats and vulnerabilities.

The Financial Services Information Sharing and Analysis Center, also known as FS-ISAC, the financial industry's forum for cyber threat discussion, is providing guidance and support to the law firm service.

Cindy Donaldson, FS-ISAC's vice president of products and services, said the center has been communicating with more than 180 law firms, and she expects more firms to express interest after the launch. She declined to say which firms or how many have applied and proven eligibility.

Davis Polk & Wardwell is among the firms that applied. "Today, law firms are working pretty independently on fighting off the different attacks that are coming toward us," said John Kapp, Davis Polk's global director of information technology. He said the new cyber group "is a force multiplier when we can share information amongst ourselves anonymously and we can be aware of what attacks are happening against other law firms. We protect our law firm and vice versa."

Cindy Donaldson, vice president of products and services at FS-ISAC

Although law firms receive threat data through trade groups and the FBI, Donaldson and law firm security directors said the legal information sharing office is the first of its kind to provide a centralized platform to share cyber threat information anonymously.

"It is the first formal attempt to pull law firms" into the threat information sharing environment, said Lisa Sotto, a Hunton & Williams partner who focuses on privacy and cybersecurity.

Earlier this year, President Barack Obama issued an executive order encouraging development of platforms where cybersecurity information can be shared within the private sector and between the private sector and government.

To become a member of the law firm forum, firms must submit an application, pay an $8,000 membership fee and meet eligibility criteria. The primary criteria is that a firm have the majority of its lawyers in the U.S., Canada or the United Kingdom, Donaldson said, adding that could change over time.

Firms of any size are eligible.

The forum was created after the financial services industry advocated for law firms to establish a platform.

In March, the New York Law Journal and affiliate publication The American Lawyer reported that a group of law firms—including Sullivan & Cromwell; Debevoise & Plimpton; Paul, Weiss, Rifkind, Wharton & Garrison; Allen & Overy and Linklaters—were helping to form the service (NYLJ, March 6).

Law firm members within the International Legal Technology

Association and its cybersecurity focused component, LegalSEC, also played a significant role in working with FS-ISAC to establish the service.

Law firm members of the service will receive email alerts and advisories on cyber threats and vulnerabilities, as well as physical threats such as weather events, for actionable intelligence in the hopes of preventing an attack. Firms will be able to submit information anonymously.

Donaldson said data will be provided by multiple sources, including the U.S. government and paid private sources of threat intelligence. Nonprofit FS-ISAC will provide the infrastructure for the service.

"The overall goal is to share information about cyber and physical threats and vulnerabilities to mitigate risks," Donaldson said, noting law firms handle some of their clients' most sensitive business data.

Legaltech News, a Law Journal affiliate, reported this week that Mandiant, a division of FireEye, found that 80 of the 100 biggest law firms in the U.S. have been hacked since 2011.

Several chief information officers and data security directors said they expected wide participation among law firms.

Winston & Strawn is among the interested firms. David Cunningham, Winston's chief information officer, said data protection is a security issue as well as a matter of meeting business expectations.

Winston & Strawn clients audit the firm about 15 to 20 times a year to make sure it's following established security guidelines, he said. Some audits involve questionnaires and in-person visits by clients.

Like other firms, Winston hires security companies to test the firm's strengths and weakness and spends hundreds of thousands of dollars each year to prevent and detect intrusions, Cunningham said. "It's a big area of investment for us."

Cunningham praised the establishment of a legal services information sharing organization. "Law firms don't really have that kind of forum to find what happened and why one firm had a breach and another didn't."

But he and others expressed some reservations.

Cunningham said if the firm experienced a data breach and told other firms about it, "we lose control about what people say about it" and it may not be not clear whether a client would want that breach further advertised. Keeping the information anonymous may not completely eliminate the risk, he said, if other members can infer who was targeted.

Christopher Ward, director of information security at Vinson & Elkins, said he is cautious about joining, noting the pool of cyber threat data he is seeking comes not only from other law firms but also from clients.

Firms face a risk in having access to an incredible volume of threat information but not being able to respond, said R. Jason Straight, a senior vice president for cyber risk solutions and chief privacy officer at UnitedLex Corp., which provides security consulting services to law firms and other businesses.

Straight said few firms realize the resources required to take action. "I'm a big fan of threat information sharing" among companies, he said, but "there's an underemphasis on orchestrating all the threat intelligence and doing something useful about it."

Daniel Garrie, co-head of Zeichner Ellman & Krause's cybersecurity practice who works with banks and law firms on protection, echoed these concerns.

"The problem is, what sorts of resources do law firms have? A lot of banks and other institutions have whole teams devoted to this. But law firms do not."

@ Christine Simmons can be reached at csimmons@alm.com. Twitter: @chlsimmons. Reporter Nell Gluckman of The American Lawyer contributed to this report.