Cravath Admits Breach as Law Firm Hacks Go Public

Nell Gluckman and Christine Simmons, The Am Law Daily

March 30, 2016

While it’s no secret that law firms are often targeted by cybercriminals seeking sensitive client information, it’s rare for breaches to become public.

But not this week.

The Wall Street Journal reported Tuesday that hackers had gained access to the computer networks of law firms working on M&A deals, including Cravath, Swaine & Moore and Weil, Gotshal & Manges. A Weil spokeswoman declined to comment, but Cravath confirmed that the firm identified a “limited breach of its IT systems” in the summer of 2015.

“We have worked closely with law enforcement authorities who have jurisdiction over this matter, and we are not aware that any of the information that may have been accessed has been used improperly,” the firm said in a statement, adding that it beefed up its security measures after the breach.

Also this week, Crain’s Chicago Business reported that dozens of law firms were targeted by a Russian hacker seeking information on M&A deals. The cybercriminal, going by the name of “Oleras,” was discovered soliciting help from other hackers to try to gain access to computer systems at 48 firms, nearly all of which are among The Am Law 100.

When contacted by The American Lawyer, some firms said they became aware of the incident either in late 2015 or earlier this year.

“Certainly, we have long recognized that law firms face the same cyberthreats as other businesses,” said a Pillsbury Winthrop Shaw Pitman spokesperson. “Understanding that, we already implemented a number of defensive measures, including regular training for attorneys and our employees, to help them recognize possible cyberattacks.”

Wachtell, Lipton, Rosen & Katz; Paul, Weiss, Rifkind, Wharton & Garrison; Goodwin Procter; Shearman & Sterling; Pillsbury; and Kaye Scholer, which were all named in the Russian threat report, said they had no reason to believe that any of their information had been compromised. Many other firms declined to comment.

Douglas Ellenoff, a founding partner at the 69-lawyer M&A firm Ellenoff Grossman & Schole, said...
that he found out his firm was on the target list Wednesday after reading the Crain’s article.

“We were surprised our name was on that particular list,” he said, adding that it would have been a nice courtesy if he found out earlier. “We all have a responsibility to the public markets.”

Ellenoff said that the firm immediately asked its technology services vendor to conduct an audit of its systems, and preliminary data showed that the firm wasn’t affected.

A partner at another of the targeted firms, who did not want to be identified for fear of inviting other attacks, said his firm sees “many, many phishing attempts.”

His firm heard about the potential Russian threat from multiple sources in 2015 and tightened up on its data protection systems in response, he said. The firm also regularly reminds people not to open unusual emails or links.

Keeping below the radar

Cybersecurity professionals said that what’s new about these hacks and attempted attacks is that they’ve been disclosed, willingly or not.

Law firms will go to great lengths to keep attempted and successful hacks secret, because any sign that the data they store isn’t secure can result in a “huge loss of customer confidence,” said Austin Berglas, former head of the FBI’s cyber branch in New York.

“I think that the majority of the law firms don’t even know that they’re compromised,” said Berglas, who now leads the cyber investigations and incident response team at K2 Intelligence. He added that law firms are traditionally understaffed in cybersecurity, compared with large corporations and banks.

Berglas said he worked with a law firm recently that faced a ransomware attack, something he said he’s seeing more and more often. The firm did not know about the attack until the hacker sent a screenshot of the stolen data and a message that the information would be made public if the firm did not pay. This firm opted to comply and handed over a seven-figure sum, according to Berglas.

Daniel Silver, a former federal prosecutor who recently joined Clifford Chance, said it doesn’t surprise him that the most recently disclosed threat is coming from Russia. “They tend to be located in Ukraine, Russia or Eastern European countries that don’t have extradition treaties,” he said of the hackers.

Silver, a past chief of national security and cybercrime in the U.S. Attorney’s Office for the Eastern District of New York, said that in his experience, data breaches at law firms haven’t been a primary focus of prosecutors. A big reason for that, he said, is that incidents involving law firms are rarely reported to authorities.

Few reporting requirements

Firms tend to be reluctant to publicly identify themselves as victims, said Silver. And they usually don’t have to. While corporations are often required to report data breaches and hacking, law firms—which frequently possess sensitive material from the same corporations—are in a different category, he said.

Generally, there is no specific regulation directed at law firms requiring them to report data
breaches, Silver said.

"More often firms will turn to the private sector to try to fix a problem rather than call the FBI," he said. "It's a patchwork approach these days … and law firms fall into a black hole when it comes to these data breach issues."

Berglas said that typically disclosure requirements for companies or government agencies are triggered because health care records or personally identifiable information, such as Social Security numbers, are compromised. Information about M&A deals or IPOs does not necessarily need to be reported.

Meanwhile, an organization in which law firms can share data on cybersecurity threats anonymously launched in August and now has 77 law firm members. The group is affiliated with the financial industry's forum for cyberthreat discussion, FS-ISAC.

The law firm sharing forum is "actively sharing information among members" about threats and activities, said Cindy Donaldson, chief operating officer for FS-ISAC's sector services division.

"We're definitely seeing an increase in the level of sharing [of threat intelligence]," and the amount of alerts and adversaries sent to firms, said Donaldson, who could not discuss any particular alerts or threat intelligence. She partly attributed the increased communication to the growth of the organization since August, and said it may not indicate that firms are facing more threats.

The group, called the Legal Services Information Sharing and Analysis Organization, or LS-ISAO, shares information from member law firms if the firms choose, and also shares information from law enforcement.

Still, many observers say that firms should be doing more.

"Attorneys themselves and assistants are going to be the weakest point of any cybersecurity system," said John Reed Stark, a former SEC enforcement lawyer who now runs a cybersecurity consulting firm in Bethesda, Maryland. "I just don't get the sense that law firms really want to seriously engage for risk and security assessments."

Stark said that he could foresee a breach so catastrophic that it could be "the death knell of a law firm."

"I'm not sure that law firms truly appreciate that," he said.

Ross Todd and Michael D. Goldhaber contributed to this report.