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' Reported Cyberattacks Are 'Tip Of The Iceberg'

By **Xiumei Dong**

Law360 (November 4, 2020, 6:25 PM EST) -- Two recent high-profile data security incidents at BigLaw firms have once more drawn attention to law firms' cybersecurity vulnerabilities, and with the coronavirus pandemic forcing lawyers to adapt to a remote work environment, experts warn that the disclosed events are just the "tip of the iceberg" of such attacks.

In October, Seyfarth Shaw LLP and Fragomen, Del Rey, Bernsen & Loewy LLP both disclosed security incidents, including a malware attack, that put clients' sensitive information at risk.

"In terms of the number of firms and potential clients that have called us regarding potential incidents, that number seems very small," said Michael Maschke, CEO of Virginia-based digital forensics firm Sensei Enterprises, noting that there are "a lot more attacks that have occurred and are currently going on" against law firms but have not been reported.

Depending on the nature of the attack, some law firms, particularly smaller ones, may even decide not to disclose the incident in order to minimize liabilities and avoid potential fallout from clients, Maschke added.

"We really are at the tip of the iceberg," said Michael Gold, a partner and co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP. "The frequency and magnitude of ransomware attacks are increasing. The hackers are getting way more sophisticated at executing these attacks, and this situation is not going to get better anytime too soon, unfortunately."

A ransomware attack, in which criminals freeze victims out of networks and then demand payment to restore access, is likely what led to the **temporary shutdown** of many of Seyfarth's systems last month, the firm said in a statement posted Oct. 10. In an update nine days later, the firm reported it had restored all critical systems from a malware attack and that none of its client or firm data was accessed or removed.

Fragomen wasn't as lucky. In a data breach notice filed with the California attorney general's office on Oct. 23, the firm wrote that "an unauthorized third party" **gained access to a file** containing Google staffers' I-9-related employment eligibility data, but did not specify how the data was accessed.

According to Lindsay Nickle, a Lewis Brisbois Bisgaard & Smith LLP partner and a vice chair of the firm's data privacy and cybersecurity practice, the language "access by an unauthorized individual" is often used when the victim does not know or does not want to identify the nature of

the attack.

"It means that somehow or another, someone's access credentials, their username and password, were compromised and used by someone else to get into a computer system and access information," Nickle said.

While malware, which is short for malicious software, is a common technique used by cybercriminals, that isn't always how sensitive data is accessed, Nickle said. Other possibilities include employee mishandling of company accounts or even insider threats.

Referring to Fragomen's case, Nickle said, "In an incident like this one, my reading of their report is that this is probably more related to a credential compromise than potentially a malware situation."

The "Human Factor"

Law firms have become **attractive targets for cybercriminals** in recent years because they handle large amounts of sensitive client information, data and money. However, many firms have "less-than-optimal information security practices and procedures," Gold said.

"There is, in many law firms, a premium on unimpeded workflow, which can create reckless information security behaviors by end users. And by end users, I mean lawyers and their assistants," Gold said. "And all of this has been compounded by the risks associated with work-from-home environments."

On top of that, there are just too many methods that bad actors can deploy to gain access to a firm's system or database, said John Reed Stark, a former U.S. Securities and Exchange Commission internet enforcement chief and the president of data breach response and digital compliance firm John Reed Stark Consulting LLC.

Just looking at cyberattacks alone, Stark listed multiple techniques such as ransomware, phishing scams and advanced persistent threat, in which an intruder gains access to a network and remains undetected for an extended time.

"In general, the biggest vulnerability that companies have comes down to people," Stark said. "So while there are plenty of technologically complex attacks, the vast majority of them start with somebody clicking on something they shouldn't, or somebody creating a vulnerability by not securing their own system access properly."

Because a lawyer's job often requires extensive communication with clients, many attorneys tend to neglect the steps needed to ensure cybersecurity and data security when responding to a client's urgent matters, Stark said.

"It's very difficult to sort of corral lawyers into specific behaviors because they're all essentially ... working 24/7 with clients around the world using multiple platforms of technology, right?" Stark said. "Their desktops, their laptops, their phones, their tablets — there's just so many different kinds of things and they're using all types of connectivity."

Especially in the COVID-19 era, Stark noted, lawyers and law firm staff working from home are particularly vulnerable to attacks such as phishing scams due to human error, and they often have weak security protocols on their Wi-Fi networks, which can allow hackers easier access to a network's traffic.

Moreover, because lawyers' work is often publicly displayed on their website, it allows bad actors to use that information to orchestrate a social engineering scheme in which they'll pretend to be colleagues or clients of a lawyer and trick the firms into giving up valuable data, Stark said.

"Lawyers are especially vulnerable because their biographical information is so easily figured out, [which] makes them more susceptible," Stark said. "Law firms are a treasure trove of just really good information."

Data Security Incidents Are Not Necessarily Breaches

According to Sara Jodka, a partner with Dickinson Wright PLLC and leader of the firm's U.S. data privacy and cybersecurity practice, cyberattacks against law firms have "surged" since the onset of the COVID-19 pandemic, which has forced many lawyers and law firm staff to work remotely.

"Law firms are a significant target, and I've only seen those numbers increase year after year after year," Jodka said.

However, it is difficult to pinpoint just how much that activity has increased, since not all cybersecurity incidents needed to be reported to the state attorney general's office, Jodka said. Most states' security breach notification laws only require businesses or state agencies to report attacks that have infiltrated data containing personally identifiable information, she added.

"In a typical ransomware [event] where it's only the encryption, you're dealing with a security incident. You're not dealing with the data breach," Jodka said, stressing that when the data is encrypted, it doesn't necessarily mean that an unauthorized person had obtained the information.

"'Data breaches' are a term of art, so when we work with clients whenever they have had an incident, we really caution them not to use the B word ... because as soon as you say it's a breach, your time clock for getting your notifications starts ticking," she added.

Most state data breach notification statutes require businesses or agencies to notify federal authorities and victims within 30 to 45 days of the determination of a breach, according to Jodka. Firms that fail to meet their obligations after experiencing a data breach could face reputational harm and even lawsuits, Jodka said.

For instance, Warden Grier LLP, a Kansas City, Missouri-based personal injury firm, was **sued** in March for allegedly not notifying clients of a data breach. Hiscox Insurance, which had hired the firm to represent policyholders, alleges Warden Grier breached its contractual obligations and its fiduciary duties by failing to notify the company of the breach and is seeking $1.5 million in damages.

"When a notification is warranted, to not notify could constitute a violation of the attorney's professional obligations to its client," said Gold of Jeffer Mangels. "The result of that can be that if the client directly or indirectly learns of the incident from someone other than the law firm, there likely will be an impact, and not a good one."

--Editing by Alanna Weissman and Jill Coffey.