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

Clients Likely To Grill Law Firms After Vendor Data Breaches

By **Ben Kochman**

Law360 (February 26, 2021, 8:20 PM EST) -- Revelations that hackers may have stolen documents from Jones Day and Goodwin Procter LLP during cyberattacks on third-party vendors underscore how essential it is to be upfront about data security events with clients — or risk losing them.

Clients of BigLaw giants and firms of any size are likely to demand answers about how such attacks unfolded and what steps firms took to prevent them, including whether they vetted the security of third-party products used to transfer sensitive data, attorneys say.

Jones Day is **currently investigating** whether its documents were stolen after an attack on its file transfer software vendor Accellion, in news that broke weeks after Goodwin Procter **disclosed internally** that hackers may have also stolen some of its clients' confidential data after a breach at a file transfer vendor.

Both firms have said they notified affected clients of the incidents, but the stakes of the likely ongoing conversations in the wake of the attacks are large, cybersecurity experts say, with firms likely to face detailed questions about how data may have been stolen on their watch.

"If I were a client of a big law firm that experiences a breach, I would be on the phone with them first thing, demanding to know what happened and to speak with an independent forensic analyst," 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.

Law firms that aren't adequately transparent with clients about data breaches "run the risk of violating their ethical and fiduciary agreements, and they run the risk of clients leaving," Stark added.

Cybercriminals have **targeted** law firms more frequently in recent years, experts say, viewing the legal industry as ripe given the sensitive data lawyers have and the heightened obligations to keep client dealings private.

Small and mid-size firms are considered in some ways to be more vulnerable to attacks than larger firms, given they usually have a smaller budget and fewer resources devoted to cybersecurity.

"Every single one of us knows of firms that have been hacked," said Brett Krantz, a partner at

mid-size firm Kohrman Jackson & Kranz LLP in Cleveland, Ohio, who oversees the cybersecurity standards of Meritas, a law firm network with 186 members in more than 90 countries. "This is and was already at the top of all of our minds."

Meritas' standards call for firms to establish a formal information security plan and to plan ahead on how to handle cyberattacks. Part of that response must include informing clients about an attack or breach even if the specifics of what data may have been exposed are being investigated, Krantz told Law360.

"You need to be quick, you need to be thorough, and you need to be honest," Krantz said. "If a client is going to be upset, the best way of dealing with that is showing that you are doing what you can to let them know what happened and how you are working to prevent that from happening again."

The American Bar Association also released ethics requirements in 2018 directing that attorneys **notify clients** in the event of a breach and keep them updated on investigators' findings. A report released in May by the nonprofit research organization Sedona Conference, meanwhile, concluded that firms should tell clients if their sensitive data has been exposed **even if it's unclear** whether state or federal laws require them to do so.

Law firms are likely to face the same level of client scrutiny if the breach originated at a third-party vendor rather than on the law firm's own network, attorneys say.

"From a reputational perspective, it doesn't matter that it was a vendor because, from a client's point of view, they will say we provided you with our confidential data and it was compromised," said Sachin Bansal, general counsel at the cybersecurity company SecurityScorecard.

News that BigLaw giants were affected by data breaches at third-party vendors should lead to clients at other firms asking questions about which third-party vendors their attorneys use, Bansal said. "They will be saying, 'Look what happened to Jones Day and Goodwin Procter. What measures are you taking?'"

Attacking third parties has become a common tactic for hackers seeking to target several potential victims at once, including in the recent cyberespionage campaign that **exposed the data** of U.S. government agencies and private companies using network monitoring software from SolarWinds Corp.

"Pointing the finger at a third party is never worth doing because every breach I get involved in affects some sort of third party," Stark said. "The reality is that third-party attacks are extremely common. Every company uses an array of third parties — that's how many breaches happen."

Cybersecurity consultants or experienced chief information security officers are likely to be in high demand for law firms as they continue to navigate the threat of cyberattacks and try to demonstrate to clients they have a plan in place to either avoid episodes or mitigate the damage, attorneys say.

"Certainly, telling clients who are thinking about hiring you about investments you've made in cybersecurity should only help enhance your ability to get that client," said Jason Kellogg, a partner at boutique litigation firm Levine Kellogg Lehman Schneider & Grossman LLP in Miami. "And who knows — perhaps getting that client helps pay for the implementation of those cybersecurity programs going forward."

--Editing by Philip Shea and Jay Jackson Jr.