How Vendors Are Data Security Soft Spots For Law Firms

law360.com/pulse/articles/1352290

By Steven Lerner | February 4, 2021, 4:39 PM EST

A recent data breach at a BigLaw firm underscores the need for legal professionals to consider the potential cybersecurity risks associated with third-party vendors.

An **internal memo obtained by Law360** on Tuesday from Goodwin Procter LLP managing partner Mark Bettencourt revealed that a small percentage of clients had confidential information exposed as part of a security breach with an unspecified file transfer vendor on Jan. 20.

Goodwin has declined two requests to comment this week.

Claudia Rast, Butzel Long PC's cybersecurity group leader and co-chair of the American Bar Association's cybersecurity legal task force, told Law360 Pulse that firms have to rely on their vendors' data security, which is risky.

"When those vendors are hacked and the information that those vendors may have, such as the email addresses for those lawyers and the kind of information that may be hosted and processed, that's an open pathway and a great risk for lawyers," Rast said.

Frank Gillman, a principal at Vertex Advisors LLC and a former chief information officer for Lewis Brisbois Bisgaard & Smith LLP, told Law360 Pulse that law firms need to dedicate more resources to vendor risk management programs.

"I recognize that resources are spare in any organization," Gillman said, "but I think you can supplement those resources by outsourcing some of the reporting functions."

Firms must identify tiers of risk and develop rules for each vendor, he said. This might include the types of data that the vendor is allowed to store, how the data is shared with the vendor and requirements for the security systems it has in place.

Any third party that has access to a firm's data could pose a risk, not just file transfer vendors like the one associated with the Goodwin breach. Even if the data is encrypted, Rast said that firms should restrict access through a secure virtual private network and ensure that credentials are strictly maintained.

Goodwin's memo said the firm responded to the security breach by disconnecting service to the vendor, hiring an outside forensic expert and launching an investigation. The experts generally agree that those were the right steps for a law firm to take.

"You don't want to just shut things down and delete everything," Rast said. "You need to know how it happened and what kind of steps to take to make sure it doesn't happen again."

Whether an attack was caused by something internal or an outside vendor, Gillman said the response should be the same.

"A lot of firms need to be more aware that you're just as likely to be a target through an external vendor as you are from an internal attack," he said. "Be more aware that third-party attacks are on the rise."

In January, Law360 Pulse **identified nearly 50 data breaches** in law firms in 2020. External breaches, including from third-party vendors, were among the most reported incidents.

Given the threat, law firms need to be on the lookout for anomalous behavior associated with the connections to third-party networks.

Rast said law firms should screen vendors' security requirements.

"What a lot of law firms are doing right now is sending out questionnaires to their vendors, making those vendors respond, updating those questionnaires, doing security checks and also requiring various audits," she said.

One of the best things firms can do, according to Gillman, is develop a system that alerts their security teams about any unusual activity as quickly as possible. From there, firms should assess the threat and respond with a defined set of actions.

Now more than ever, law firms have a target on their backs, and they must take these vendor-related risks seriously.

"Firms large and small need to understand that they pose and present a rich target for hackers that are looking for information and access," Rast said. "And we pose a rich target because we represent clients that have potential information, whether it's trade secrets, financial information, potential mergers and acquisitions dealing with publicly traded companies and all kinds of data."

--Editing by Brian Baresch and Jill Coffey.

0 Comments