LAW360

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

So Your Outside Counsel Was Hacked. Now What?

By **Michele Gorman**

Law360 (January 17, 2023, 4:47 PM EST) -- Cyberattacks on law firms, like the 2020 attack on Covington & Burling LLP that became public in a filing last week, are out of general counsel's control. But top corporate lawyers can take preventive measures now to avoid panicking later, like knowing the kinds of data the company shares with outside counsel and how it's stored and writing data security requirements into their contracts to ensure they're notified soon after a breach happens, experts say.

Last week, a filing with the U.S. Securities and Exchange Commission disclosed for the first time that Covington was among the victims of a November 2020 cyberattack on Microsoft Exchange email servers used by thousands of companies across the globe. The episode affected 298 of Covington's clients, including seven that had material nonpublic information exposed.

It's crucial for general counsel to seriously consider data breaches, in part because the incidents can affect their relationships with both customers and firm lawyers, said Sharon Cruz, an attorney at DiCello Levitt LLC who specializes in privacy compliance, data management and cybercrime and spent years prior to law school working as a computer support technician.

"The biggest mistake a lot of corporations make is assuming that data breaches [are] just an IT problem," Cruz said. "It is not."

Hundreds of BigLaw firms and solo law offices have reported data incidents in recent years. While there are ethical rules and state laws that apply to law firms, their security infrastructure might not be as robust as that of, say, health care providers or financial institutions, said Anna Mercado Clark, leader of the data security, privacy, e-discovery and digital forensics practice teams at Phillips Lytle LLP.

And a hacker could be interested in breaching a law firm for a variety of reasons, including obtaining intellectual property or business information about multiple clients — potentially including the government, she said.

"I think what's interesting here is people typically think of data breaches as bad actors trying to get at personal data: Social Security numbers and credit card information," Mercado Clark said. "But we're seeing increasingly these state-sponsored [attackers] are not interested in that."

"Certainly, if I'm the GC, I would want to know if the law firm that I have data stored at ... has experienced a data security incident, regardless of whether my company's data has been impacted.

KAMRAN SALOUR
Troutman Pepper

The attack on Covington — which U.S. authorities have attributed to Chinese military spies — was "principally directed at a small group of lawyers and advisors" at the law firm in a bid to "learn about policy issues of specific interest to China in light of the incoming Biden administration," according to a legal filing from the firm's outside counsel made public on Jan. 10.

Covington has a deep roster of former high-ranking U.S. public officials, including former U.S. Attorney General Eric Holder.

When a company's data is compromised from an external entity, one of the most difficult aspects for general counsel and their teams is their informational disadvantage, said Kamran Salour, a partner at Troutman Pepper who helps clients with cybersecurity and privacy issues.

"A lot of times what will happen is the company that has been impacted will not tell you until they know for sure. They may not tell you at all if your data has not been impacted," he said. "Certainly, if I'm the GC, I would want to know if the law firm that I have data stored at ... has experienced a data security incident, regardless of whether my company's data has been impacted."

"I think what's interesting here is people typically think of data breaches as bad actors trying to get at personal data: Social Security numbers and credit card information.

ANNA MERCADO CLARK
Phillips Lytle

General counsel need to protect their companies as much as possible and obtain as much information as often as they can. With this in mind, they can get ahead of a potential breach before one happens by negotiating upfront with their outside counsel the firm's obligations to reveal details about a possible future incident, Salour said.

"If the client doesn't have these contractual provisions in place, and the law firm suffers an incident, typically the law firm is going to remain silent until they have a full understanding of what happened," he said. "Certainly, if Client X's information was not impacted, from the law firm's standpoint, they probably don't want to tell Client X that there was an incident."

In Covington's case, the SEC is seeking a court order that would force the firm to reveal which of its clients were affected by the 2020 cyberattack. The firm has refused to disclose that information, saying it would breach attorney-client privilege.

While the SEC may find some traction — given that courts are divided on whether the fact that a law firm is representing a specific client is privileged information — the fight now playing out on a public stage is likely to make clients more acutely aware of both their law firms' cybersecurity posture and the risk that the government may be able to access information they share with their attorneys.

In their contracts with outside counsel, top corporate lawyers should consider including language requiring that a firm doesn't disclose the name of the company — even if there's a subpoena, Salour said.

"Obviously, there are lots of wrinkles with that," he said. "But from my view, as the GC, you want to protect the organization as best you can, and one way to do that is to have as many layers of defense [as you can]."

He added, "If I'm the GC, I don't want the SEC now asking me questions about an incident that happened to a third party where I'm not necessarily privy to what happened."

Whenever a breach occurs, it's crucial for general counsel to keep calm, experts say. And prevention now is key to avoid panicking later.

Salour suggested general counsel take certain steps when they initially disclose information to their lawyers. For instance, they should know what kinds of information they're sharing and where and how the firm will store the data. The cloud? A server? Will it be backed up? General counsel should also find out how long their attorneys will retain the information.

While getting answers to some of these questions can be difficult, "you don't want perfection to be the enemy of good," he said. "Having some understanding is better than having no understanding at all when it comes to that."

General counsel should also be mindful that third-party breaches can affect their customers, and communicate with them in a timely manner, experts said.

Even without a legal obligation, though, some firms might choose to inform their clients because it can become a point of contention in the attorney-client relationship.

"It's not good for the GC, because now the CEO is like, 'Well, how come we're reading about this in a media [report],' and then … [ask] the GC, 'Why didn't you have these protections in place?'" Salour said.

Mercado Clark recommended general counsel consider scheduling regular meetings to receive updates about the breach to avoid constantly emailing and calling their outside lawyers. And if there's a development in between the scheduled conversations, the firm can provide updates as needed.

Salour recognized that the immediate period after a breach can prove stressful for general counsel and their legal teams as they answer stakeholders' questions and make decisions internally. And sometimes details about an incident aren't available in the first few hours, or even days.

"It's important," he said, "to really have as much visibility as you can when a third party is experiencing an attack that could impact your information."

--Additional reporting by Ben Kochman, Xiumei Dong, Stewart Bishop and Allison Grande. Editing by Alanna Weissman and Jill Coffey.
