5 Steps To Take When Your Firm Is Hacked

By Allison Grande

Law360, New York (July 22, 2014, 3:16 PM ET) -- While no industry is immune to the growing threat from hackers, law firms make an especially enticing target because of the juicy personal and corporate data they hold.

During the past few years, the news has become saturated with reports about criminal hackers and nation-states lifting consumer and business data held by a bevy of retailers, hospitals, financial institutions, energy companies and hospitality providers, including Target Corp., eBay Inc., Wyndham Worldwide Corp., P.F. Chang's China Bistro Inc., University of Pittsburgh Medical Center, JPMorgan Chase & Co. and U.S. Steel Corp.

While a law firm breach has yet to dominate headlines, the risk of being caught up in a cyberattack is just as real for law firms that hold a unique blend of personal and sensitive corporate data that clients are more than willing to fork over because of the promise of attorney-client privilege, according to attorneys.

“Every law firm needs to consider data security and cybersecurity just as any other industry would,” Pillsbury Winthrop Shaw Pittman LLP partner Brian Finch said. “There's no reason that law firms should think they're exempt. In fact, I would say that they are one of the most attractive targets out there.”

In order to minimize the damage to their reputation and valuable client relationships, law firms — just like any other business — need to be poised to respond nimbly and competently to a breach.

But the task is complicated by the reality that, unlike other industries, law firms are not only bound by the myriad state and federal breach notification laws that apply to personal information but also have additional duties under ethics and professional rules to be upfront with clients about the movement and safety of their data.

“Law firms that have a data breach face different challenges than most businesses because of the potential disclosure of attorney-client privileged information, which attorneys have the ethical duty to protect,” said Larry Kunin, Morris Manning & Martin LLP's data security and breach practice co-chair.

Here, experts offer five steps that firms should take post-breach to minimize risk and protect the unique ethical responsibilities they have to their clients:

Figure Out What Happened

As with any other business that has discovered that hackers have gained access to its system, the first step that law firms should take is to determine exactly how the intruders got in and what they took, according to attorneys.

“Law firms need to figure out as quickly as possible not only what was lost but also how serious a breach is,” Finch said. “Businesses don't always understand how large a breach is or how deeply it penetrated, especially if they're not looking in the right place.”

While the analysis can be done by an internal technology team with the help of the firm's lawyers and other relevant staff, experts advise that law firms should not hesitate to bring in outside professionals with more comprehensive training and experience in assessing intrusions.

“The analysis is very similar to the one done in any other organization,” said Lisa Sotto, head of Hunton & Williams LLP's global privacy and data security practice. “Once an anomaly is detected in their systems, law firms would be wise to retain an external forensic investigator because law firms typically are not set up to conduct their own forensic investigations.”

While outside experts can be valuable, law firms can also help their cause by ensuring that the forensics team they choose is vetted and chosen well before a breach is detected, by installing software that monitors data usage in their system and by not acting too hastily while waiting for the investigatory team to arrive, according to attorneys.

“The first thing not to do is panic and shut down a system immediately and scrub everything off the hard drive,” said Simon Shooter, a London-based partner and head ofBird & Bird's cybersecurity group. “It may shut down the threat, but it also means that no one will be able to conclude how the intruder got in or what has been taken.”

Assess Reporting Requirements

Once a law firm has ascertained what type and quantity of information was taken, it can begin determining whether the unauthorized disclosure triggers any of the patchwork of federal and state breach notification laws, which also apply to every other sector that holds sensitive client and employee data.

“What's important for law firms to keep in mind is that the exact same rules that apply to every other industry also apply to law firms,” said Gerald Ferguson, the co-leader of BakerHostetler's privacy and data protection team.

The point was driven home several years ago, when the Massachusetts Bar Association asked regulators to clarify whether the state’s unique law that mandates specific data security standards for businesses applies to law firms, which are already governed by security requirements detailed in their model rules of professional conduct, according to Ferguson.

“The Massachusetts regulator responded that the law applies to every business, and law firms,

that means you," he said.

Law firms' disclosure of hacking incidents will most likely be triggered by reporting requirements contained in the patchwork of 47 state data breach notification laws that apply to all businesses that store personal information, attorneys say.

Law firms that do work for health care providers also need to be mindful of the Health Insurance Portability and Accountability Act, which was recently strengthened to extend certain data security and reporting obligations to the business associates of covered entities, according to attorneys.

"Federal health regulators have made it clear that they are more than willing to bring actions against business associates," Ferguson said. "Law firms shouldn't assume they're immune just because they're law firms."

In drafting a required notice to a client or regulator, experts recommend that law firms should be honest about what they know and understand at the time of the disclosure, even if their investigation is still going on, attorneys say.

"If there's no question that the incident will become public because it's covered by a breach notification law, then the best thing to do is get out in front of it," Sotto said. "For law firms, public relations issues are going to be that much more acute, given that there is an absolute expectation of confidentiality within the law firm and that expectation has been compromised."

Consider Ethical Obligations

Where law firms do differ from other industries is that they hold privileged client data that they are bound by ethics rules and professional duties to protect, according to attorneys.

"Attorneys have a set of ethics rules and a fiduciary duty to their clients that are far stronger than most data breach laws," Adams and Reese LLP partner Lucian Pera said.

Under ABA Model Rule of Professional Conduct 1.4 , attorneys are required to keep clients "reasonably informed" about any material developments in their case, an obligation that could easily apply to the unauthorized disclosure of client data.

"If some of the client's private confidential information has been released into the world, that seems like a pretty material development in their representation," Pera said, adding that even if the ethics rules didn't exist, attorneys still have a fiduciary duty to clients that requires them to be candid about these issues.

While not every loss of data may be found to be significant and it is up to law firms to evaluate the risk of making a compromise known, attorneys advise law firms to err on the side of being as open as possible with clients about hacks.

"It is probably a good idea to notify a client of a security incident affecting their information,

even if there is no legal obligation to do so," said Al Saikali, the co-chair of Shook Hardy & Bacon LLP's data security and privacy group. "Lawyers have a special relationship with their clients, who trust them with the confidence of their information. If the incident is properly explained, it can be a nonissue and the client will appreciate being informed." Attorneys also need to be mindful of their obligations under ABA Model Rule 1.6, which requires them to proactively adopt reasonable security safeguards to protect client data and could open them up to liability if they fail to properly secure the data, according to experts. "Clients have a right to expect that their confidential information is being kept safe and secure," Shooter said. "So if a firm has lax data security, clients could sue for breach of confidence."

Make Sure Threat Is Removed

While dealing with the fallout from a data breach, law firms need to make sure that they not only understand and alert affected individuals about the threat but also ensure that the risk is expunged from their system, attorneys say.

"The firm must determine if the compromise has been terminated and if the incident has been remediated," Saikali said. In working to restore systems to working order, law firms should not be afraid to take any issues or questions to experienced technology professionals and to heed their advice in order to avoid problems with getting their systems back online quickly.

"Forensics folks know the best way to remediate the situation," said Gordon MacKay, the chief technology officer at security risk assessment firm Digital Defense Inc., adding that companies have run into trouble in the past by electing to shut down their systems after discovering a breach and being unable to restore backups that allow them to continue normal operations.

Learn From the Incident

Once the threat has been expelled, law firms should turn their attention to ensuring that history doesn't repeat itself. "Learning from the mistakes is always the answer," Shooter said. "If you don't, the same attack can happen tomorrow because the firm hasn't been able to close the door."

Following a breach, law firms should aim to take steps such as ensuring that firewalls are up to date, that effective incident response policies are in place, and that staff and vendors are trained on data security, according to attorneys.

The measures can help firms reduce the risk that they will be targeted a second time and also win favor with clients, who attorneys say are increasingly scrutinizing law firms' data security and demanding that law firms be able to demonstrate that they have strong protections in place.

"The real lesson is that it is important for law firms to recognize the need to take affirmative steps to avoid disclosure of attorney-client privilege," Kunin said. "It hopefully goes without saying that law firms need to have secure networks."

-- Editing by Jeremy Barker and Brian Baresch.