Damage Control: Recovering Your Firm's Reputation After a Breach

You can regain trust after a cyber breach. Here's how.

Jaffe Staff

In March 2016, the FBI warned that hackers were targeting large international law firms to steal confidential client information and use it for insider trading, corporate espionage and other criminal purposes. Are law firms any more secure now? And the bigger question: Are they prepared to handle a cyber event?

As more and more clients send cyber due-diligence questionnaires to outside counsel to confirm that their sensitive information is secure, law firms have shored up their defenses, but a recent report by Logicforce found that is just not enough. Of the 200 law firms surveyed for their Q1 2017 Law Firm Cyber Security Scorecard, every one was targeted for confidential client data in 2016–2017, and approximately 40% did not know they had been breached. The report also found that the size of the firm made no difference: Large and small firms alike were targets. Logicforce's Q4 2017 Law Firm Cyber Security Scorecard didn't note much improvement by the end of the year. In fact, 48% of law firms had their data security practices audited by at least one corporate client in the past year.

With these jarring statistics, it is only a matter of time before another law firm is hacked. When it happens, will that law firm be prepared to mitigate the reputational damage that will inevitably follow? As with any crisis, a law firm's business and reputation hangs in the balance after a cybersecurity breach. If it's handled well, though, a firm can regain trust and rebuild its brand. Here's how.

Consider this scenario:

- 6:00 a.m. ET – A security operations monitor detects unusual activity on ABC law firm's network and alerts the firm's chief information officer (CIO).
- 6:20 a.m. ET – It is clear to IT personnel that the firm is under some form of cyberattack that is spreading to the firm's ten international offices.
- 6:25–6:30 a.m. ET – The CIO instructs the IT team to shut down all law firm network services and notifies firm leadership. The IT team begins to implement its response plan and loops in the crisis communications team. The crisis team includes a point person to receive information from the IT staff, a spokesperson, legal counsel, and an outside public relations agency that has already been vetted and is known for its crisis communications expertise.
- 6:30–7:00 a.m. ET – The crisis team formulates messaging for employees and clients in lockstep with legal counsel who ensures that the firm is meeting all reporting obligations of notifying the proper authorities in the U.S. and the EU of the breach. [Note: How to report a breach to the authorities has become quite complex with varying

requirements by jurisdiction. For a breakdown of reporting obligations, please see *Law360* article here. For the recently released ABA ethics opinion offering guidance to law firms on data breaches, see article here.]

- 9:00 a.m. ET – Because email and phone systems are down, ABC law firm posts a sign in the lobby instructing employees not to turn on their computers, to remove all laptops from docking stations, and to keep their laptops turned off pending further communication.
- 10:00 a.m. ET – A tipster walking by ABC law firm's lobby in New York sees the posted notice and texts a picture to a friend who is a cybersecurity reporter at the *Wall Street Journal.*
- 11:00 a.m. ET – ABC law firm's crisis communications team sees the picture on Twitter and suddenly realizes that news of their breach is now public.

How to respond

Assembling a crisis team – In this scenario, ABC law firm already has a crisis team in place whose members know exactly what they are supposed to do in the event of a breach and can spring into action immediately. They also have a crisis communications and response plan in place and have shared the firm's media relations policy with employees. Employees are well aware that they are not to provide comment to the press. ABC law firm also has already taken the critical step of identifying a spokesperson in advance of the crisis. The team and the pre-vetted agency have already strategized exactly how information will be communicated to clients, the firm's internal audience and the media in the event of a crisis.

Issuing a statement – As IT professionals scramble to bring operations back online, the firm's crisis team is forced to draft a statement based on what is known, particularly now that news of the breach is public and the firm's public relations director begins to receive calls on her cell phone from the media. A statement dispels rumors, allows the firm to control the narrative, and helps reassure its clients and employees. The statement focuses only on *verifiable facts*. Because email and phone service are down, the firm's PR director provides a statement to those reporters who call her cellphone.

When issuing the statement, the firm will need to effectively balance the urge to get as much information out as quickly as possible, with the need to ensure that all details that are shared are accurate and will not have to be retracted or changed later on. The statement should aim to explain:

- What exactly is the problem and when it occurred
- What is being done to rectify the situation
- How data is now protected
- What internal policies are now in place
- What clients/employees can expect in the future

Also, there should only be one firm spokesperson who is the only person allowed to speak and interact with the press. That spokesperson should not feel obligated to answer all questions that the reporters may ask, nor should they speculate. Just as when crime scene investigators speak to the press, they only comment on what they know at the time and promise to follow up with more information as it becomes available. It is wise for the

law firm spokesperson to take the same approach. A reporter can always update the story later when new details are available.

Timing – Realize that timing is everything. Delayed communications can quickly erode hard-earned trust among the firm's client base and cause speculation among employees and the public. Even if all the information is not yet known, the firm must at the very least acknowledge the situation in a tone that reflects transparency and honesty, and is in lockstep with the same information that is shared with the appropriate authorities. How that information is communicated to the public is important too. Interviews, which may subject a spokesperson to a long and difficult line of questioning, may not be the right tack. A more appropriate strategy might be to offer a simple written response to queries, a social media post to quell misinformation and negative chatter, a public statement on the firm's website, or a statement on background until more details can be confirmed. Whether you decide to use one or all of these communication methods, the messages and information must be consistent throughout.

Returning to normal and rebuilding a brand – Once the dark cloud of the crisis passes, it's time to think through how to go about rebuilding the firm's brand. Certainly, a media relations strategy that helps to push down the negative stories by sharing positive news about the firm, its attorneys and its successes will be necessary. Lateral announcements, new office openings, litigation wins, deal news, positive third-party commentary and speaking opportunities are all beneficial brand-building tactics. An ongoing and steady stream of news stories about the firm will eventually replace the negative news of the crisis.

This article originally appeard in The National Law Review *on October 16, 2018.*