Law Firms and Cyber Attacks – What's a Law Firm to Do? Part Two

Targeted cyber attacks on the legal industry are a daily occurrence. What's a law firm to do? Part One in this two-part series examined how breaches are affecting law firms, the steps to take, and essential responsibilities of law firms and lawyers to help prevent cyber weaknesses. Part Two focuses on communications after a breach and reputation management.

Vivian Hood
CEO/Owner
Public Relations
904.220.1915
vhood@jaffepr.com

Imagine waking up to these headlines:

- "(Your Firm) First U.S. Firm Publicly Named in Data Security Class Action"
- "(Your Firm) Accused of Lax Data Security in Lawsuit"

It is hard to overcome news headlines like those, but they are some of the exact headlines that Chicago law firm Johnson & Bell faced two years ago.

Johnson & Bell is one firm named in a series of cyber-related class action claims against at least 15 law firms — and the only one with a publicly available complaint.

What is so unusual is that there was no actual breach of confidential client information; merely the possibility of a breach — the law firm was not hacked and there were no actual known data breaches. The class is alleging damage due to the risk of future compromise of their confidential information due to inadequate data security by the firm.

The complaint calls Johnson & Bell "a data breach waiting to happen" and alleges legal malpractice by breach of contract and negligence, unjust enrichment, and breach of fiduciary duty.

What does it mean if law firms can be sued for something that hasn't actually happened, but might occur? Being held accountable for a crime not committed sounds like a Hollywood movie script (*Minority Report*, anyone?), but is becoming more of a reality. The documentary *Pre-Crime* explores currently used criminal justice techniques that are based on Big Data and predictive analysis for measuring and spotting the likelihood of criminal activity.

Johnson & Bell has since countersued with a defamation suit. The case is in arbitration now. Time will tell how the legal system will approach data security and non-breach litigation, but this does mean that law firms and their clients must become even more proactive and deliberate about network and data security.

Cyber Breaches and Crisis Communications

The communications response to a cyber breach is a critical component to managing its impact and damage. Now more than ever before, transparency is necessary — even though it may seem like the least-desirable approach to take. Sharing news of a breach before someone else does gives the law firm the control and authority it needs in this situation. If someone within the firm leaks news of a breach before the firm decides to say anything, the firm's reputation will take an additional beating — one that could be avoided.

The Securities and Exchange Commission (SEC) recently fined Yahoo a $35 million penalty for misleading investors by failing to disclose a 2014 personal data breach affecting more than 500 million user accounts. Other companies that hid or didn't disclose their breaches sooner are also getting hit with massive fines and public backlash, and law firms aren't immune to that sentiment. The European Union's General Data Protection Regulation (GDPR) now requires quick disclosure (in some instances, within 72 hours of learning of a breach) and imposes substantial penalties for non-compliance.

Ideally, every firm, large and small, should have a crisis communications plan prepared that outlines all the firm's audiences: clients; the public at large; and internally, all the attorneys and staff at the firm, even vendors of the firm.

The plan should have a process for how and when to communicate, along with lists of action items in place before a crisis occurs — including identifying the law firm's spokesperson (usually the firm's managing partner) and other relevant contacts (like IT security), draft statements for media that account for several different scenarios, draft letters that can be updated quickly and sent to clients, along with plans for who sends them and how, as well as with reassurances about steps taken and in progress.

Internal messaging should provide instruction for how the breach is being handled and direction about how to manage media or client inquiries.

Have a general holding statement ready to share that addresses what you know now (at the time of the breach) and when updates or a final resolution can be shared. It doesn't have to commit to all known facts, but it should state that the facts may change as new information is uncovered. Then, follow up with more information as it becomes known. Initial communications should also include a sincere apology, if warranted, and convey compassion and reassurance.

As details emerge and new facts come to light, be ready to change direction quickly, no matter how difficult these are.

Don't overlook the importance of updated CRM lists. Many firms struggle with this, but if/when a breach happens is not the time to start cleaning up and organizing outdated names and contact information, and figure out proper ownership of such contacts. In the wake of a breach, information has to be shared quickly. A pending cybersecurity threat alone should be reason to make sure all firm contacts are prioritized and current.

Managing a Reputation After a Cyberattack

Firms must act decisively to protect their reputations. If treated like the crisis that it is, damage to a firm's reputation after a breach can be managed with full anticipation and preparation of these items.

Crisis Team. Identify and train a crisis team. At the very least, the team has to include the firm's spokesperson, firm's experienced PR or crisis communications expert, legal counsel to the firm, and the IT security lead.

Crisis Plan. A crisis communications plan must be ready — and that means updating it at least once each year as people and situations change.

Social Media Strategy. Monitor social media and news stories as they happen and have a strategy ready with responses that include key messaging.

Media Relations Strategy. Help push down the negative stories by sharing positive news about the firm, its attorneys and its successes. An ongoing and steady stream of news stories about the firm — not being anything related the breach — will help push that negative news down. Doing so requires a commitment and dedicated strategy and an understanding that it will take time. However, it won't make the negative news disappear overnight, since that takes time and other (good) news to take over the news cycle.

Every month and every day, ultra-sophisticated hackers are developing new threats to outsmart current technology and are working around existing barriers to get into law firm systems. Although most lawyers weren't expecting to have to deal with technology threats as part of their practice, that is today's reality. Firms with poor security will lose trust as well as clients, while firms with the tightest cybersecurity defenses will gain their clients' confidence, as well as establish a competitive advantage.

This article originally appeared on The National Law Review *website on August 3, 2018.*