Why You Need a Law Firm Data Breach Response Plan

Carlos Arcos
Senior Vice President
Public Relations
713.826.5195
carcos@jaffepr.com

It appears that every week, the news media informs us that another major company has been hacked. The latest victim is Ashley Madison, the online dating and social networking service marketed to people who are married or in a committed relationship, and the Excellus health insurance system. The Ashley data breach resulted in the release of the email addresses and other personally identifiable and sensitive information of millions of people, mostly men, who had registered for the website. As a result, Ashley Madison has been hit with more than half a billion dollars in lawsuits, threatening the financial stability of the company. The impact on Excellus is not yet known.

Cybercriminals are constantly looking for easy targets and sources of potentially valuable data that can be used to steal identities, which criminals can then use to commit fraud. As some businesses make it harder for criminals to penetrate their respective IT networks, the next line of potential targets are those businesses that keep a significant amount of data containing personally identifiable information but lack adequate protective data security, such as law firms.

Law Firms in the Crosshairs

Since law firms act as warehouses of extremely sensitive client and employee data, they should recognize that they are prime targets for cyber-attacks. In the new, highly connected reality we operate in now, law firms must consider the risks these cyber threats pose and take the data protection steps necessary to reduce those risks. Otherwise, the oversight may prove costly.

It should be noted that, historically, most data breaches experienced by law firms are related to the loss or theft of a laptop, thumb drive, smartphone, tablet or other mobile device that contains sensitive client information. Such theft can be an open door for cyber criminals to gain easy access to a firm's corporate network and steal confidential information. All that said, cybercriminals are much more savvy than ever before and have developed means of hacking into protected networks without using a piece of the organization's hardware.

Communicating a Data Breach

Since no one can fully prevent the risk of a data breach, it's important to have a crisis communication plan in place to inform stakeholders, and the media should they cover the story. The goal of the plan should be to address the situation as quickly as possible and restore trust with stakeholders. Tactics should include:

- Identify a spokesperson for the firm.

- Prepare written statements for employees, clients and media.
- Craft message points for any media interviews.
- Call key clients to inform them personally of the breach.
- Post a statement on the firm's website where it can be easily found.

As for the media, law firms should avoid the instinct to take a "head in the sand" approach. The conversation in the media, especially over social media, will take place whether you participate or not. It's important to be honest and direct when telling your story. This will allow the law firm to better control the narrative.

As I mentioned earlier, the risk of your law firm's computer network being hacked can never be completely eliminated. Just ask Ashley Madison – or the Pentagon for that matter. As the threat continues to increase, it's critical to create a crisis communications plan to mitigate the fallout and reduce the likelihood that it will have a long-term negative impact on your firm's reputation or bottom line.

If you need assistance with developing or defining your crisis communication plan, contact Carlos Arcos at carcos@jaffepr.com.