The Persistent Reality of Cyberattacks on Law Firms

Despite warnings, advice and threats, cyberattacks targeting the legal industry continue to make headlines, cause disruption and wreak havoc on unprepared law firms. Letâ▯▯s take a look at emerging threats, cyber risks at law firms, steps to protect against and prepare for cyber breaches, and the importance of a crisis communications plan.

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

Nation-stateâ▯▯sponsored cyberattacks

Nation-stateâ▯▯sponsored attacks have emerged as highly sophisticated and complex cyber hacks that are driven by political motivations, not profits. We frequently see headlines about Russian cyberattacks in response to sanctions and support for Ukraine, but in fact, Russian state-sponsored cyber actors have targeted U.S.-cleared defense contractors for several years. The U.S. government also identifies state-sponsored malicious cyber activity by the Peopleâ▯▯s Republic of China as a major threat.

Other nations often target sensitive information about new technologies, data, defense development, testing, designs and more. Since law firms represent these companies and industries, extra cautions are more important than ever. Whether attacking companies or their law firms, hackers constantly refine their tactics, requiring relentless protection and monitoring to avoid disruption, extra costs, loss or theft of important data, and other damage.

The Biden Administration has made cybersecurity defense a top priority for our country, most recently by signing the Strengthening American Cybersecurity Act into law in March 2022 to improve the cybersecurity of the federal government and identify security incident reporting requirements, among other measures.

Current state of cybersecurity risks at law firms

Here are some key law firm cybersecurity findings from the ABAâ▯▯s annual 2021 Legal Technology Survey Report, as reported by the Bressler Risk Blog on law firm risks:

- â▯▯Many law firms report that they are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.â▯▯
- â▯▯25% of respondents overall reported this year that their firms had experienced a data breach at some time â▯¦ This year [2021], the reported percentage of firms experiencing a breach ranged from 17% of solos and firms with 2â▯▯9 attorneys, about 35% for firms with 10â▯▯49, 46% with 50â▯▯99, and about 35% with 100+.â▯▯
- â▯▯Reported consequences of data breaches are also significant. Downtime/loss of billable hours was reported by 36% of respondents, consulting fees for repair were

reported by 31%, destruction or loss of files by 13%, and replacement of hardware/software reported by 18% (percentages for firms that experienced breaches).â

This survey shows that these numbers keep increasing year over year. Firms â especially smaller ones â should heed these statistics as red flags if they havenât devoted enough attention and resources to prepare for and protect against cyber breaches. Itâs a matter of when it will happen, not if.

What should a law firm do to prepare for and prevent a cyber breach?

Legaltech News recently reported on steps law firms can take to strengthen their cybersecurity now to prepare for an increased volume of breaches and cyberattacks, given the global impact of the conflict between Russia and Ukraine.

Jaffe also offers several recommendations here. For a more complete list, see our previous article, âLaw Firms and Cyber Attacks â Whatâs a Law Firm to Do? Part One.â

- **Budget.** The expense of having robust cybersecurity measures and planning in place is never going to be as high as the costs of a breach fallout in terms of money, time and reputation. Make room in the budget for cybersecurity.
- **Educate**. Firms need to train staff and lawyers about their policies and procedures for preventing cyberattacks, and actively discuss or drill a couple of times per year. Update policies at least once annually to stay on top of technology best practices.
- **Prepare.** Ensure the firm has a crisis communications plan in place for itself and its clients in the event of a breach.
- **Explain.** Law firm clients are paying more attention to how their outside attorneys protect their data. Describe the firmâs cybersecurity measures in RFPs and to clients and make it a differentiator that assures clients they made the right choice in hiring your firm and that their information will be protected. Law firms could face federal regulatory enforcement actions from the Federal Trade Commission if they donât protect client data sufficiently.
- **Refresh.** Do not overlook what is often the first touchpoint with a law firm: its website. Law firm websites have to follow the most current and best practices for data security. An outdated website content management system can alert hackers that a firm may not be diligent about updating security practices.

Cyber breaches and crisis communications

Letâs take a deeper dive into the âprepareâ recommendation. Some key points we expressed in our earlier article âLaw Firms and Cyber Attacks â Whatâs a Law Firm to Do? Part Twoâ still ring true and bear repeating today; review the full article for additional insights.

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 â 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 inside the firm, a client or some other entity leaks news of a breach before the firm decides to say anything, the firmâ€™s reputation will take an additional beating â€“ one that could be avoided.

Ideally, every firm, large and small, should have a crisis communications plan in place and known throughout the firm that outlines all the firmâ€™s audiences â€“ clients, the public at large, firm vendors â€“ and all of its attorneys and staff, and what staff should do in the event of a crisis.

The comprehensive crisis plan should include at least these elements:

- A process for how and when to communicate, along with lists of action items, before a crisis occurs. The protocol should identify the law firmâ€™s spokesperson (usually the managing partner) and other relevant contacts (such as IT security) and include draft language that can be updated quickly and sent to clients, along with plans for who sends them, when and how.
- A timeline or schedule of what is needed when; timing for communications is critical.
- Internal messaging that provides instruction for how the firm is handling the breach, as well as direction about how to manage media, client or general public inquiries.
- A general media holding statement (or several statements that account for different scenarios), ready to share immediately upon request, that addresses what you know now (at the time of the breach). It doesnâ€™t have to commit to all known facts, but it should state that the facts may change as new information is uncovered.

Important note: Assume that any internal communications about a breach will be shared with a member of the press and published publicly, so be mindful of messaging.

Also, donâ€™t overlook the importance of updated CRM lists. If/when a breach happens is not the time to start cleaning up and organizing outdated names and contact information. In the wake of a breach, information has to be shared quickly. The potential of a cybersecurity incident alone should motivate the firm to prioritize and update firm contacts regularly and maintain a schedule for updating frequently throughout the year, every year.

Law firm risk from cyber breaches and data security vulnerabilities is a top concern for clients, corporate boards of directors and management, government agencies and the public. Cybersecurity incidents constantly affect law firms, and new technologies and sophisticated hackers challenge current safeguards daily. The risks are great, including loss of clients, data, trust, competitive advantage and reputation. However, law firms do recover from their breaches, and our article about â€œDamage Control: Recovering Your Firmâ€™s Reputation After a Breachâ€ offers valuable advice, including the importance of timing.

To help ensure your crisis communications plan is ready before a cybersecurity attack happens to your firm or client, letâ€™s review it together and update it as necessary. Contact Vivian Hood at vhood@jaffepr.com to discuss ways Jaffe can help your firm shore up its protection against the fallout from a breach.