LAW FIRM CYBERSECURITY

"Law firms must be proactive in protecting the storage of the vast amounts of client data they possess and are entrusted to safeguard."

Earlier this year, a Russian hacker, using the name "Oleras", extracted the confidential details of clients from 50 law firms that had been targeted throughout the U.S.. The hacker's plans were to discern which companies were to be merged in the future, then use this information to conduct insider trading. The same hacker also singled out eight lawyers for phishing attacks. Pretending to be an assistant at a trade journal, the hacker emailed each lawyer under the pretense of conducting research for an upcoming article featuring excellence in M&A. This is just one of a number of instances of hackers targeting law firms.

Law firms are becoming increasingly conscious of potential security breaches by criminal hackers who seek to gain financially by stealing sensitive client information. Firms are an attractive target because of the large repository of confidential information they hold. Providing a strong defense against these cyber-criminals is now considered a requisite duty for law firms large and small. When hiring cybersecurity vendors to safeguard client information — a necessity for law firms with insufficient cybersecurity staff — firms must conduct due diligence to prevent opening themselves up to liability.

THE HIGH COST OF BEING HACKED

A successful cyber attack can lead not only to significant revenue loss, including the result of malpractice suits, but also the loss of reputation and business. The average cost of a data breach per organization is now at an all-time high of $7.01 million. Such an amount is troublesome for larger firms, but could spell bankruptcy for many smaller law practices.

The costs incurred after a security breach include the following:

- Hiring a computer forensics expert to determine the extent of the breach
- Costs associated with complying with the notice requirements of the state(s) of residence for the clients whose information was compromised
- Repair to the hardware or software systems of the firm
- Business interruption
- Consulting fees for firms hired to block future criminal access
- Malpractice or negligence suit damages pursued by clients who suffered harm as a result of the breach

Many firms have discovered that their professional liability insurance, general liability insurance and property insurance do not cover all of the costs caused by cyber-attacks.

continued on page 2

Attorneys have a common law duty to protect their client's confidential information. The Rules of Professional Conduct, and federal and state laws, also impose on attorneys the duty to protect client data. Additionally, most states have enacted laws requiring notification to individuals whose personal information has been accessed by an unauthorized person as a result of a data breach.

Law firms exist and thrive on a foundation of trust that they have built with their clients. They must maintain this trust or risk losing those relationships. Clients entrust confidential information to law firms and expect firms to take proper and adequate steps to safeguard it. News of a security breach at a law firm will cause current and potential clients to lose confidence in the breached firm.

TIPS FOR PROTECTING CLIENT DATA

Law firms must be proactive in protecting the storage of the vast amounts of client data they possess and are entrusted to safeguard. The Federal Trade Commission (FTC), Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) have all published helpful tips that law firms can take into consideration when reviewing their cybersecurity process.

To help mitigate risk of security breaches, law firms may wish to:

- Identify a point of contact within law enforcement. Prior to the occurrence of any breach, law firms should foster connections with law enforcement so that a trusted point of contact is available if or when a breach does occur.
- Create or update a strategy to prevent and detect cybersecurity threats and an incident response plan within the firm. The DOJ states that such a plan should be actionable and address factors such as how to contact critical personnel and what data or networks should be prioritized.
- Periodically review and update the firm's policies.
- Train employees on how to detect and prevent potential security breaches. A former SEC enforcement lawyer who currently heads a cybersecurity consulting firm states that the "attorneys themselves and assistants are going to be the weakest point of any cyber security system." One survey of 150 firms showed that law firms' top cybersecurity concern, greater than hackers or malware, is "careless employees".

Firms should regularly provide security training that includes sessions on the topic of phishing. Phishing occurs when an outside source sends an email from a seemingly trustworthy entity asking for sensitive information.

- Regularly remind employees to follow basic data security guidelines. Some frauds involve hacking the email accounts of attorneys at a firm. Firms should instruct employees to protect their data by using complex passwords, changing passwords at least every three months, updating antivirus software regularly and not logging onto firm email accounts while on public wireless networks.

"Providing a strong defense against these cyber-criminals is now considered a requisite duty for law firms large and small."

- Run analysis programs to detect unusual activity (host-intrusion program "HIP"). These programs work to detect malware and abnormalities that antivirus programs miss and will include the installation of security software on computers, servers and mobile devices.
- Consider joining a cyber-threat-sharing network. The Legal Services Information Sharing and Analysis Organization (LS-ISAO) allows firms to benefit from sharing anonymous information about cyber threats. Each firm should assess the risk of such an approach, as other firms may potentially be able to discern which law firm has been breached and use such information to their own advantage.
- Consider purchasing stand-alone cyber liability insurance. There are a number of costs incurred as a result of cybersecurity breaches that are not underwritten by a firm's typical coverage. Insurance brokerage Aon states that, within the past two years, more than 60 of its 250 medium- and large- sized law firm clients have bought cyber insurance. Firms with such coverage are often better protected, as the purchase of cybersecurity coverage often necessitates a strict underwriting process, where firms undergo cybersecurity wellness tests.
- Hire thoroughly vetted outside security consultants.

continued on page 3

PROPERLY VETTING CYBERSECURITY CONSULTANTS

One important step firms can take to protect themselves against a data breach is to engage outside security partners. Firms must practice due diligence when engaging a cybersecurity firm; otherwise, they may become liable in the event of a future security breach. Trying to save money by employing less expensive — and probably less experienced — consultants and managed security service providers (MSSPs) could cost law firms greatly in the long run.

Due diligence requires formulating a thorough discovery process for potential consultants or providers. There are a number of questions a firm should pose to potential security vendors prior to engaging their services. These include:

- What is your relevant IT security experience?
- What do you believe to be our law firm's biggest security risks, and are you equipped to address these?
- Which regulatory and compliance requirements should our firm be concerned with, and what do you know about them?
- How do you monitor for and identify both known and unknown threats?
- Given that security threats evolve constantly, do you have a team that regularly reviews your processes?
- Which of your personnel will be performing the work?
- What type of support do you need from our law firm to accomplish your work?
- How will you coordinate communication between your firm and our law firm?
- Where do you keep your data, and how do you protect it?
- What deliverables will you provide to our firm, and when?
- Have you provided these services to other corporations in the legal industry, and can you provide us with their contact information for use as a reference?
- Will you provide training to our employees?

In cybersecurity as in law, reputation is everything. Speaking with references provided by the consulting firms is essential. Be sure to ask direct questions of these references, as your objective is to determine which consultants will be best suited for a long-term relationship with your law firm.

By training employees, creating cybersecurity plans and conducting due diligence prior to hiring cybersecurity vendors, law firms can take a giant leap towards protecting the sensitive data of their clients and preserving their trustworthy reputation.

LEARN MORE

To learn more about how CT can help you with your due diligence requirements, contact your CT representative or call 844-409-1386 (toll-free U.S.).

Join the conversation. Follow us on Twitter, LinkedIn, Google+ and Facebook.