research

Rise of Law Firm Hacks Leads to More Scrutiny From Corporate Clients

Third-Party Cybersecurity Assessments Help Manage Risk

Karen Hornbeck, Consilio

Consilio®
Together. Stronger.

Rise of Law Firm Hacks Leads to More Scrutiny From Corporate Clients

Third-Party Cybersecurity Assessments Help Manage Risk

Last year was a lightning rod for law firm cybersecurity breaches. In March 2016, the FBI warned of "a financially motivated cybercrime insider trading scheme" that was targeting "international law firm information used to facilitate business ventures." That month, it came to light that several major American law firms had also been hacked in 2015. In one case, three hackers used the stolen information to net more than $4 million in an insider-trading scheme. Meanwhile, Panamanian law firm Mossack Fonseca was targeted by an anonymous source that leaked over 11 million documents to a German newspaper. The contents of the so-called "Panama Papers," published in April 2016 by the International Consortium of Investigative Journalists, created numerous, sometimes career-ending scandals for the firm's roster of high-profile clients, many of whom sought to avoid tax liability through inventive means.

But even with these highly-publicized incidents, too many law firms still lack adequate cybersecurity measures to effectively prevent breaches. A 2016 survey by the American Bar Association revealed that one in four small law firms (10 to 49 attorneys) and large firms (more than 500 attorneys) have suffered data breaches; 20 percent of firms with 100 to 499 attorneys reported breaches as well. It is time for corporate law departments to scrutinize their outside counsel's systems, processes and vendors for vulnerabilities and mandate the closure of data-security gaps. Otherwise, they risk becoming the next victims.

Why Do Cyberthieves Target Law Firms?

Law firms are an attractive one-stop shop for cyberthieves. Not only do their data coffers hold trade secrets and other confidential information about their corporate clientele, but they also include material nonpublic information about corporate development, business strategy and planned transactions (such as mergers and acquisitions), that thieves could use for a variety of uses including insider trading. Litigation strategies and case details might have an adverse impact on a company's value or reputation. Firms generally also store a wealth of personally identifiable information, including protected health information and payment information, for clients, parties, witnesses and employees.

Moreover, many law firms have yet to employ the rigorous data-security measures used in other industries. For example, they may not have adopted the latest security measures, perform needed audits or vulnerability assessments or conducted adequate staff training. Cyberthieves recognize that the path of least resistance to a target's information may therefore be through the target's law firm. And instead of infiltrating only one company's systems at a time, with a law firm, thieves can obtain information about numerous companies with just one attack.

How Are Law Firms Hacked?

Law firms are susceptible to breaches in many forms. Although hacking has recently garnered a lot of attention, firms also experience security breaches through employee negligence, such as when an employee's unencrypted computer, storage media or mobile device is lost or stolen. Sometimes, dishonest employees steal firm data. And more recently, malware attacks via phishing schemes have wreaked havoc for firms. Regardless of the cause, for law firms and their clients, the greatest risks are the loss of confidentiality from unauthorized access to client data and

potential malpractice claims and significant damage to reputation that ensues.

Indeed, a 2016 case, Shore v. Johnson & Bell Ltd., No. 16-CV-4363 (N.D. Ill.), may signal more cybersecurity-related lawsuits to come. In 2014, Jason Shore hired the law firm of Johnson & Bell to represent him in a lawsuit. Shore later sued the firm for breach of contract, breach of fiduciary duty, negligence and unjust enrichment because the firm exposed its clients to a "heightened risk of injuries" by leaving their "confidential information unsecured and unprotected." The lawsuit alleged that the law firm had three critical vulnerabilities involving its networks and email system, violating a lawyer's ethical duty to maintain client confidentiality. Note that Shore's complaint did not establish that any sensitive information was actually lost; it sued based on the potential vulnerabilities.

Other risks include the loss of attorney billable hours due to downtime for forensic investigations and infrastructure remediation. Financial costs include consulting fees for technical expertise and upgrades to software and hardware, not to mention fees for crisis management and public relations to deal with reputational damage. Lawsuits alleging ethical violations or malpractice could arise. Of course, additional regulatory fines may ensue, along with credit-monitoring costs if individuals are affected. Finally, law firms and their clients may suffer the loss or destruction of critical files and data.

What Are Lawyers' Obligations?

ABA Model Rule of Professional Responsibility 1.6 requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 explains the factors that should be used to evaluate the reasonableness of lawyers' efforts, including "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

Other laws and obligations can extend lawyers' responsibilities beyond the rule. For example, the Health Information Technology for Economic and Clinical Health Act (HITECH) creates cybersecurity obligations for Business associates of HIPAA-covered entities, including law firms. Similarly, the Federal Trade Commission Act, prohibiting unfair and deceptive practices, has been used against businesses that misrepresent their cybersecurity protections. State data-breach laws can also impose additional requirements.

The bottom line is this: corporate law departments must assess the security and privacy controls in play whenever they send information to any third-party vendor. Outside counsel firms should not be immune from these assessments, given these risks and the breadth of sensitive and confidential information they receive from the Office of the General Counsel.

How Can Corporate Law Departments and Their Law Firms Address the Risks?

As corporate law departments seek to manage the potential security threats posed by hacking and other types of cyber incidents, they should engage in comprehensive assessments of the security and privacy controls of their third-party vendors, focusing on law firms. A security assessment of any third-party vendor should include two components: a quantitative data-driven assessment, such as a survey instrument or scorecard, and a qualitative inquiry, such as an interview. Armed with this information, corporate law departments can retain their partner firms based on objective metrics.

As corporate law departments assess these partner firms they should look, at a minimum, for the following elements, which can create the foundation for a rigorous, effective cybersecurity program for any law firm.

Follow standardized best practices.

In creating cybersecurity assessment procedures, review standards from reputable organizations, such as the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST). The Association of Corporate Counsel (ACC) has also established Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information. The Model Controls establish baseline security measures that corporate counsel can use to set appropriate expectations for their outside vendors' data-security practices.

Look for basic policies and procedures.

Law firms should have internal policies designed to protect the privacy and security of client information. Typical policies should address information security, asset management, physical security measures, data privacy, access controls, business continuity, training and compliance and incident response. A dedicated person or team should hold primary responsibility for managing the firm's cybersecurity program.

Require encryption.

Law firms should encrypt all client information stored on their systems (including any third-party systems) or transmitted over any non-secure channels. Because lawyers and their clients are constantly transmitting privileged materials, attorney work product, client trade secrets and other proprietary and confidential materials through cyberspace, emails should have the highest level of security. All laptops and mobile devices that are used for any law firm work should also be encrypted.

Ensure that appropriate physical, administrative and technical security measures are in place.

To prevent unauthorized access, law firms must implement physical security measures such as identification badges, access controls for areas where computer equipment is stored and video cameras. Law firms should also limit access to data by compartmentalizing access according to authority and job function. Finally, firms should require their employees to use strong passwords on computers and mobile devices and deploy antivirus and other protective software applications.

Mandate strong, consistent information governance policies and procedures.

Corporate law departments need to ensure they are applying their information governance policy as forcefully to outside vendors as they are to their internal records. Know what data the firm maintains, how it is stored, who has access to it, how the firm decides what to discard and what to retain and what recovery capabilities are available. Law firms should only keep matter data as long as necessary to satisfy their legal obligations to the company or to meet any applicable laws, regulations or ethical requirements. Furthermore, they should only collect essential personally identifiable information. At the end of any engagement, law firms should promptly return or destroy client information.

Review the firm's Incident Response strategy.

It is important that the law firm take a proactive approach to protecting its clients' data and information. A solid Incident Response plan will include protocols for containment, notification, remediation, monitoring and related issues. It will also assign specific responsibilities to designated personnel and have third-party vendors on standby to ensure that important tasks do not fall through the cracks. With an Incident Response plan in place, law firms can respond rapidly to a breach, limiting its scope and reducing damages.

Require cyberliability insurance.

Law firms should have cyberliability insurance from a carrier with a minimum credit rating of A- from a reputable rating agency. Coverage should be at the level of $10 million or more. Vendor firms should name the company as an additional insured on their cyberliability policies.

Review the firm's training protocols.

Employee training is critical to preventing cybersecurity breaches. All too often, criminal intrusions occur through carelessness: an employee clicks on a malware-infected link or accesses a law firm's network from an unsecured connection. Employees should be comprehensively trained on the firm's procedures for protecting data and have that training updated at least annually.

Obtain expert advice.

Partner with outside cybersecurity experts, particularly those with law firm experience, to perform both penetrations and vulnerability assessments and make recommendations. Corporate law departments and their law firms typically lack the requisite expertise to anticipate and fend off every potential cybersecurity threat; outside firms can fill those knowledge gaps.

Conclusion

As business drivers to share critical information continue to increase and hackers utilize more sophisticated and aggressive tactics, corporate law departments too must step up their efforts to evaluate with who and how their data is shared and protected. Third-party cybersecurity assessments, as part of a comprehensive defensive strategy, can serve as an effective shield against cyberthieves, allowing corporate law departments to partner together to protect their confidential data, their reputations and the bottom line.

info@consilio.com
www.consilio.com

Consilio®
Together. Stronger.