Getting Serious about Law Firm Cybersecurity

by Karen Painter Randall and Steven A. Kroll

One can hardly turn on the news these days without hearing about the latest victim of a cyber-attack. Industries across the board, from large retailers to healthcare providers to even the U.S. government, have been the targets of advanced cyber-attacks where millions of personal identifiable information (PII) was stolen. The legal profession is not immune from the threat of a costly cyber incident. In fact, the FBI has issued warnings and held meetings with nearly all of the top law firms in New York about the risk of a data breach and theft of confidential and proprietary client information. Since at least 2009, the FBI, the U.S. Secret Service, and other law enforcement agencies have warned law firms that their computer files were targets for cyber criminals and thieves in China, Russia, and other countries, including the U.S., looking for valuable confidential and proprietary information including corporate mergers, patent and trade secrets, litigation strategy, and more.

Many law firms have, in fact, suffered some sort of data breach. For example, according to recent reports, the computer networks of Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP and other major law firms were penetrated by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies. The FBI and federal prosecutors with the Southern District of New York have opened an investigation to determine if any confidential information was stolen by hackers and used for insider trading, according to the *Wall Street Journal*, which cited anonymous sources. Reportedly other prominent firms had their networks breached and hackers were threatening further attacks. Cravath said it suffered a "limited breach" of its computer network last summer, but that the firm was "not aware that any of the information that may have been accessed has been used improperly," according to the *Wall Street Journal*.

The American Bar Association (ABA) described law firms as both "attractive" and "soft" targets for a cyber-attack. Law firms are attractive targets because they handle a variety of high-value information, such as intellectual property, insider information on corporate deals and mergers, as well as the PII and protected health information (PHI) of both clients and other parties involved in a lawsuit. This includes heavily regulated information such as health and financial information. Moreover, law firms are considered soft targets because while

other industries have devoted a significant amount of time and money to ensure that sufficient policies and procedures are implemented to protect against a cyber-attack, law firms often dedicate less resources and simply lack awareness of the latest cybercrime trends.

In light of this, to take a proactive approach to cybersecurity, it is crucial that law firms understand the types of data being targeted by hackers, as well as both the legal and ethical responsibilities owed to their clients. If nothing else, from a business standpoint, many clients are now demanding that their law firms do more to protect their sensitive information to ensure they do not become 'back doors' for hackers.

For example, it has been reported that J.P. Morgan Chase & Co., Morgan Stanley, Bank of America Corp., and UBS AG are just a few of the larger financial institutions that have subjected outside law firms to greater scrutiny regarding their cybersecurity. This includes law firms completing 20-page questionnaires about their threat detection and network security systems, as well as some sending their own security auditors into firms for interviews and inspections. Thus, this article focuses on this new threat facing law firms, and some basic security steps that can be taken to protect against a costly cyber incident.

Ethical Obligations

Pursuant to the Rules of Professional Conduct, attorneys must take reasonable steps to protect their clients' information. Namely, RPC 1.6(a) requires an attorney not reveal confidential information, and RPC 4.4(b) discusses an attorney's duty to take reasonable steps in communicating with clients, as well as the duty to respect the privilege of others. Additionally, ABA Rule 1.1, Comment 8, makes clear that there is an ethical obligation related to competent representation that requires counsel to stay current on the risks posed by technology and take reasonable action to protect against those risks.

Despite these principles, many attorneys still fail to take the necessary steps to protect their clients' confidential information, even in the context of a small task such as sending and receiving emails. According to the 2015 edition of the annual Legal Technology Survey Report, compiled by the American Bar Association's Legal Technology Resource Center, only 35 percent of lawyers used email encryption. That percentage has remained virtually unchanged over the last four years of the survey, despite recent headlines regarding cyber-attacks on large corporations, such as Anthem, Inc., and the U.S. government.

When the survey asked what security precautions attorneys were implementing when sending confidential and privileged communications to clients via email, the answer given by 71 percent of the attorneys was that they rely on the confidentiality statement in the message body. Additional methods used by attorneys to protect the information and content contained within an email sent to a client included: a confidentiality statement in the subject line, requiring clients provide written or oral consent, password-protecting documents and using registered email. Moreover, of the lawyers who responded that they use encryption, a third could not say what kind of encryption they implemented. Those who could say what type of encryption they used most commonly identified it as general-purpose software with encryption features that required the recipient to be sent a separate password. Thus, it is no wonder that a recent Citigroup internal report warned bank employees that digital security at many law firms remained subpar, and that law firms would continue to be targeted by malicious actors looking to steal confidential information.

Top Cyber Threats Facing Law Firms

Although there are many different forms of cyber threats, the following are a few of the top ones facing law firms today. The first form involves spear-phishing emails, or malicious messages tailored to individuals in order to appear legitimate, which are used to infect a specific target. For example, an attorney may receive an email from a hacker pretending to be a client, requesting that he open an important attachment. If opened, it infects the entire computer network with malware. According to the Justice Department's indictment of five members of the Chinese military in May 2014, spear-phishing emails were used to steal, among other things, privileged attorney-client communication related to SolarWorld's trade litigation with China.

The second form involves ransomware, which encrypts a victim's files and then attempts to sell the victim a key to unlock their data. In many cases, victims of ransomware either pay the extortion or lose access to the critical files if they are not backed up.

In Feb. 2015, the law firm Ziprick & Cramer, located in California, sent out a letter to its clients advising that on or about Jan. 25, 2015, the firm was the victim of a single cyber-attack, by a relatively new variant of a Cryptolocker-type virus. A Cryptolocker is a kind of ransomware used to encrypt files so they become unreadable, and the hackers then demand money to restore the data. The firm reported it to the FBI and called in a cyber forensic specialist to assess the damage and install safeguards to thwart future attacks. The publicity alone involving this cyber incident surely had an impact on clients' confidence.

The third form involves hacktivist groups such as Anonymous, which target law firms involved in controversial cases. While law firm Puckett & Faraj represented a staff sergeant accused of leading a group of Marines responsible

for the deaths of 24 unarmed Iraqi civilians, it had its email accounts hacked, and more than two gigabytes of correspondence stolen and leaked. The firm's Google email passwords were not secure enough to keep out hackers, who may have employed equipment that can rapidly use multiple possible combinations to break in. Fortunately, the firm characterized the stolen documents as "really innocuous."

Steps to Increase Cybersecurity

In light of the above, many law firms are now taking steps to increase data security and ensure that proper policies and procedures are in place to protect against a cyber-attack. First and foremost, preparation is vital to preventing any sort of attack. Thus, law firms should create a cross-organizational committee, which includes not only management but human resources, procurement, finance, internal and external cybersecurity counsel, and information technology (IT) to develop and implement a risk management plan for preventing a data breach. Moreover, many law firms are now using a chief technology or privacy officer to oversee the firm's data security and privacy, as well as technology infrastructure, to ensure the policies and procedures are consistent with the security plan and technology.

Once a committee has been established, policies should be implemented regarding the privacy and security of the firm's data, which includes the use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites. In addition, a law firm should conduct an inventory of the software systems and data, and assign ownership and categorization of risk. (The higher the sensitivity of the information, the stronger the security protections and access control must be.) Furthermore, the IT department should conduct third-party vulnerability scans, penetration tests, and malware scans to protect against potential data breaches. The use of antivirus software is simply not enough to detect sophisticated attacks, which sometimes go undetected for an average of 300 days.

Most importantly, after setting the tone from the top, law firms must train employees so they are aware of the company's security protocol and are protected against the potential for accidentally exposing a client's personal, confidential information with the click of a button. This also includes having all employees create strong and unique passwords to protect their computers and mobile devices in conjunction with a password management utility. In addition to implementing the use of secure account credentials, other commonly deployed methods and tools used to keep data safe include encryption, as well as physical securities.

Clearly, the use of encryption for emails is a must-have tool for attorneys. Encryption apps, such as Virtru, are very easy to use and protect clients' data and privacy when sending sensitive emails and attachments. Also, some law firms are instructing attorneys not to open attachments sent via email unless they are in a secure environment in the office, or using a firm laptop on an encrypted line. For particularly sensitive matters, some law firms are going so far as restricting work to stand-alone computers that do not connect to the Internet. Additionally, as discussed already, mobile devices are a particular focus, as many firms can wipe data from smartphones and laptops that are lost or stolen, as well as install some level of encryption.

Unfortunately, in the evolving technological world even the best security can be penetrated by skilled hackers from around the world. Thus, besides having policies and procedures in place to prevent a data breach, it is critical that a law firm be prepared to act quickly in the event a breach is detected. The cybersecurity committee must constantly collaborate to implement and test a rapid response plan to react to a cyber incident quarterly. The plan should identify rapid response team members from each office the firm operates, along with the contact information for key law enforcement, public relations and cyber forensic experts.

Once a potential data breach has been identified, a law firm should work with its cyber forensic experts to act quickly to identify what type of information was exposed and remediate while preserving the attorney-client privilege. It should be noted that each state has its own notification laws relevant to reporting a data breach; thus, the response team should be familiar with the notification requirements. For example, in New Jersey the statute is triggered upon discovery or notification of a breach of security. 'Breach of security' means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.[1] If the law firm that suffered a data breach affects a national client, the notification process may become even more complicated, since there are currently 47 states that have notification laws, which vary in scope.

Cybersecurity Liability

Aside from a claim for attorney malpractice, various state and federal regulatory agencies have taken the forefront in prosecuting claims against businesses that fail to have proper policies and procedures in place. For example, should general PHI be stolen this would implicate the Health Information Technology for Economic and Clinical Health Act

(HITECH). The law was enacted in 2009 as part of an overall effort to modernize medical record keeping and PHI, and update parts of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In particular, HITECH expressly requires HIPAA "covered entities" to report PHI data breaches affecting 500 or more individuals to the affected class, the Department of Health and Human Services (HHS) and the media within 60 days of an event.[2]

Although one may question how this requirement applies to law firms, as defined under HITECH, 'business associates' expressly include entities providing legal services to HIPAA-covered entities. Thus, there is no question that a law firm is a HITECH business associate, and, as such, responsible under the law to secure PHI, provide appropriate notification, and otherwise comply with HIPAA standards. Furthermore, HHS's Office for Civil Rights (OCR) enforces compliance with PHI data regulations. To demonstrate the potential for damages, on May 7, 2014, OCR issued a press release announcing that two healthcare organizations—New York and Presbyterian Hospital and Columbia University—agreed to resolve charges that they potentially violated HIPAA by failing to secure thousands of patients' electronic protected health information (ePHI) on their network. The monetary payments totaled $4.8 million, which is the largest HIPAA settlement to date.

In addition to HHS-OCR, another regulatory body enforcing cybersecurity compliance is the Federal Trade Commission (FTC). On Aug. 24, 2015, the Third Circuit affirmed the District Court of New Jersey's ruling confirming the FTC's authority to investigate and prosecute consumers' privacy by failing to maintain appropriate data security standards.[3] While there have been no instances reported, to date, where the FTC has prosecuted a law firm for cybersecurity issues, a law firm should be prepared to face scrutiny from the FTC, as the number and scope of enforcement actions involving cybersecurity continues to increase.

Sharing Data with Other Law Firms

It is also important that law firms keep abreast of the ever-changing landscape of cybersecurity and what types of threats and vulnerabilities are out there. Along those lines, in Aug. 2015, the Legal Service Information Sharing and Analysis Organization (LS-ISAO) was launched. It alerts law firms to potential cyber threats and vulnerabilities. The Financial Services Information Sharing and Analysis Center, also known as FS-ISAC, the financial industry's forum for cyber threat discussion, is providing guidance and support to the LS-ISAO.

Although law firms normally receive their information regarding a potential cyber threat from other sources, such as trade groups, the LS-ISAO provides them with a centralized platform to share information anonymously. This service is consistent with an executive order issued by President Barack Obama this past year, which encourages the development of platforms where cybersecurity information can be shared within the private sector, as well as with the government.

In order to become a member of LS-ISAO, a law firm must submit an application, pay a fee, and meet certain eligibility criteria. Once enrolled, law firm members will receive email alerts and advisories on cyber threats and vulnerabilities, as well as physical threats. Moreover, law firms will be able to submit their own information anonymously regarding a cyber incident.

Although there are some who believe this new information-sharing forum will not significantly benefit law firms in preventing a cyber-attack, many believe the creation of the LS-ISAO is a step in the right direction for law firms to become more proactive in protecting against a potential cyber breach. Ultimately, the goal of LS-ISAO is to share information about these potential cyber-attacks and help law firms mitigate their damages.

Damages

According to a 2015 study conducted by the Ponemon Institute, the average cost of a data breach is $6.5 million, or $217 per lost or stolen record. This includes first-party losses such as retaining a forensic IT investigation firm, network remediation, data recovery and restoration, implementation of new safeguards, and the cost of business interruption. Moreover, should a law firm become involved in a civil lawsuit, or the target of a regulatory enforcement action, this would constitute third-party losses such as paying legal defense costs, credit monitoring services, and any other connected damages or fines. Besides the obvious financial cost of a cyber-attack, a law firm would also have to deal with damage to its reputation; in particular, seeking to regain the trust of clients who entrusted the firm with their confidential information.

As a result, lawyers and law firms that do not want to face cyber liability and wish to transfer some of the risk to other sources should consider cyber liability insurance. Besides being covered for first- and third-party losses, often the insurer will get involved at the early stages to appropriately guide its policyholder and retain counsel, public relations firms, IT consultants, and similarly experienced professionals, while actively managing the risk and cost. Thus, a law firm should consider reviewing its current insurance policies to see what is and is not covered, and then meet with an insurance broker well versed in cyber coverage about procuring insurance. When the average cost of a cyber-attack is $6.5 million, cyber insurance appears to be worth the expense.

Conclusion

In a profession based upon tradition and precedent, the practice of law must keep pace with the changes in technology in order to continue to preserve the legal and ethical duties owed to clients. Unfortunately, most cyber experts say it is not a matter of if, but when. Thus, law firms must be prepared for a cyber incident or face the costly ramifications of a cyber-attack involving clients, regulators and law enforcement. With so much at stake, at the very least law firms should have a basic understanding of the cyber risks facing them today, so they can manage risk and compliance relevant to PHI, PII and privacy issues. Under best practices it is critical that cyber liability insurance and a reasonable security program are put in place to protect clients' data, and that a rapid response and business continuity plan be prepared and rehearsed periodically to protect the firm and mitigate damage. ⚖

Karen Painter Randall, *a certified civil trial attorney and complex litigation partner with Connell Foley LLP in Roseland, is co-chair of the firm's cyber security and data privacy and professional liability groups. A member of the International Association of Privacy Professionals, she counsels clients, including law firms, on the data protection and regulatory compliance laws tailored to the enterprise and develops proactive plans to reduce the risk of a cyber-attack.* ***Steven A. Kroll*** *is an associate with Connell Foley LLP in Roseland. In addition to representing professionals in various areas, he concentrates his practice in the areas of professional liability, cyber liability, general insurance litigation and employment law handling matters in both New Jersey and New York.*

ENDNOTES

1. N.J.S.A. 56:8-163–66.
2. 42 U.S.C. § 17932.
3. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).