# Lawyers Increasingly Targeted by Cyberattacks

BY MARK SPITZ

In 2015, an attorney at Moses Afonso Ryan Ltd., a 10-attorney firm in Providence, Rhode Island, received an email from an unknown sender. When the attorney clicked on an attachment to the email, a malicious form of software called malware infected the firm's network and decrypted all of its data. The hackers demanded a "ransom" of $25,000 to provide a key to decrypt the data, which the firm paid in the form of bitcoin, only to find that the key did not work. By the time the firm was able to regain access to its data and electronic files, three months had passed. The firm claims it lost over $700,000 in revenue during that time as a result of the ransomware attack.[1]

## Cyberattacks on the Rise

Cyberattacks have become much more frequent in recent years, targeting both small companies and well-known companies such as Home Depot, Target, Yahoo!, and JPMorgan Chase. Cyberattacks can take many forms, including attempts to break into an organization's network; phishing emails or social media posts to someone within an organization containing an attachment or link with harmful software (often called "malware" or "ransomware"); or "denial of service" attacks that flood a website to the point that it crashes.

Hackers are often after customer credit card or bank account information, social security numbers, and other information they can sell for identity theft and other fraudulent uses. Or they may be after a quick "ransom" payment, as in the case of the attack on Moses Afonso Ryan, or the recent WannaCry attack in May of this year. Law firms find themselves increasingly at risk, however, and the size of the firm is no guarantee against an attack. For example, in 2015 Cravath, Swaine & Moore LLP, and Weil, Gotshal & Manges LLP, two large New York firms, were attacked, allegedly by hackers based in China. Just this year, DLA Piper fell victim to the Petya cyberattack, which affected computers and systems worldwide, losing access to its email and telephone systems for more than a week.[2]

How common are cyberattacks against law firms? The American Bar Association's 2016 legal technology survey report found that 15% of law firms surveyed, and 25% of law firms with at least 100 attorneys, had experienced a breach of some kind.[3] Due to the potential damage to a firm's reputation from publicizing a breach, however, it is quite possible that these numbers are much lower than the actual frequency of attacks.

## Why Target Law Firms?

One may ask, why do hackers go after law firms? The primary reason is that law firms have information that is attractive to hackers. In the attacks on Cravath and Weil Gotshal, the hackers sought confidential information on pending mergers and acquisitions so that they could trade in the shares of the companies involved before the information became public. Law firms have a great deal of sensitive client information involving pending transactions, bankruptcy filings, divorces, estate planning, and intellectual property, all of which could be profitable to hackers. The hackers may be acting independently, but might also be state-sponsored, especially when intellectual property is the target. In addition, hackers may be after employee information such as social security numbers to file fraudulent tax returns.

This type of attack has targeted organizations of all sizes in every industry.

### Law Firm Vulnerability

Limited resources and attention are most often the source of law firms' vulnerability. Many law firms, even larger ones, have not invested enough in their IT systems to prevent cyberattacks. They may not see the need to budget for the most up-to-date hardware and software, or realize that their IT systems do much more than just create and store documents. Mobile devices such as laptops, tablets, and smartphones are often more vulnerable than in-house systems, and lawyers are increasingly reliant on such mobile technology. Law firms may not be aware of the need for effective policies, procedures, and training that go beyond the IT function. Finally, many managing attorneys either do not understand IT issues or are intimidated by the subject; they just want to leave the problem to the "IT guy" to solve, without involving the attorney in the details.

However, cybersecurity is an enterprise-wide issue, and many potential clients, especially larger ones, are now asking law firms about their cyber- and data-security preparedness. The Association of Corporate Counsel (ACC), which has more than 40,000 members worldwide, found in its 2016 Chief Legal Officers Survey that two-thirds of general counsel ranked data protection and information privacy as "very" or "extremely" important.[4] In March 2017, ACC released safety guidelines for outside counsel to follow to protect client data. The guidelines include requirements on information retention, data handling and encryption, breach reporting, physical security, and cyber liability insurance.[5] ACC has also developed a checklist for corporate law departments to submit to outside counsel to assess their "cyber-readiness," putting pressure on law firms to demonstrate their ability to protect sensitive client data.

### Who Enforces Cybersecurity and Data Privacy Laws?

A variety of federal and state agencies have some level of jurisdiction over data breaches. At the federal level, this includes the Federal Trade Commission (FTC) for consumer protection;

## 10 TIPS FOR REDUCING RISK

**1. Software updates:** Make sure that all software and applications are the most current versions, and always accept patches and updates, which are often sent to fix vulnerabilities in the software (the May 2017 WannaCry attack exploited vulnerabilities in older Microsoft operating systems like Windows XP). Most software manufacturers release patches on the second Tuesday of the month, and your IT people, whether internal or outsourced, should be on top of this.

**2. Defensive software:** Make sure your network uses high-quality anti-virus, anti-malware, and firewall software.

**3. Backups:** Back up data in real time, not once a day or once a week, using a cloud service or other backup system that is secure and robust. Test the backups periodically as well.

**4. Password management:** Too many people still use weak passwords like "password" or "123456." A good password management policy requires the use of stronger passwords having a combination of letters, numbers, and special symbols; frequent changing of passwords; and multi-factor authentication. Passwords with more than 10 characters are much harder to break.

**5. Network access:** After a certain number of failed attempts to login, no more than three to five, the network should block the user from gaining access.

**6. Data access:** Not every employee requires access to all firm data. Categorize the types of data and limit access to those who need to use it.

**7. Remote access:** Install VPNs on all laptops and mobile phones to protect firm data when someone is working remotely. Wi-Fi networks in public places like airports and coffee shops are easy for hackers to exploit.

**8. Encryption:** Many breaches have resulted from lost or stolen laptops, tablets, or smartphones. All such mobile devices should use encryption software to protect data, as well as software allowing remote wiping of all data if the device is lost. Colorado's breach notification law arguably exempts from its requirements a covered entity that encrypts its data (CRS § 6-1-716(1)(a)).

**9. Phishing:** Don't click on suspicious links or attachments in emails or on social media posts. Many breaches result from these phishing emails. If you receive an email from an unknown sender, delete it. If you know the sender but did not expect the attachment, call the sender to confirm he or she sent it.

**10. Training:** Teach both attorneys and non-attorneys good cybersecurity practices. Training should cover treatment of suspicious-looking "phishing" emails and social media posts, password management, and mobile device usage. Repeat training periodically so it becomes a habit.

the Department of Health and Human Service's Office of Civil Rights for health-related data; the Securities and Exchange Commission for public companies, investment advisors, and broker-dealers; the Federal Communications Commission for telephone carriers and Internet service providers; and the Federal Bureau of Investigation for violation of criminal statutes. Arguably, any one of these federal agencies might assert jurisdiction over a law firm data breach, depending on the nature of the compromised data.

At the state level, 48 states and several territories have enacted statutes that require organizations suffering a data breach to notify the persons whose data has been compromised. Many of these statutes also authorize the state attorney general to enforce the notification requirements, and some—but not Colorado—create a private right of action. In addition, organizations suffering a data breach or cyberattack face litigation from customers, vendors, and other affected parties, including class action suits.

## Ethical Implications for Lawyers

Unlike other types of organizations, law firms face an additional risk in the event of a breach: possible discipline for ethical violations. Disciplinary action would likely arise from the attorney's obligations to (1) provide competent representation to clients, and (2) preserve the confidentiality of information relating to that representation.

Colorado Rule of Professional Conduct (Rule) 1.1 requires an attorney to provide "competent representation" to a client, which requires "the legal knowledge, skill, thoroughness and preparation" necessary for that representation. Comment 8 to Rule 1.1 states that lawyers must stay familiar with changes in "communications and other relevant technologies" to remain competent as required by the Rule. If a lawyer does not personally have the technical expertise required, he or she may seek expert advice or services to assist with compliance.[6]

A lawyer's obligation of confidentiality regarding client information also applies. Rule 1.6(c) states:

> A lawyer shall 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 to Rule 1.6 explains that various factors will help determine if the efforts to prevent inadvertent or unauthorized disclosure are "reasonable," 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).

## Methods for Lowering Risk

As lawyers and law firms become more frequent targets of cyberattacks, they must do more to enhance their data security, lower the chances of an attack, and mitigate their liability if an attack does occur. A comprehensive approach to cybersecurity includes the following steps:

- Assess what data the firm has and how it is maintained.
- Use an outside IT expert to assess network gaps and vulnerabilities.
- Develop a written information security plan.
- Implement policies and procedures for handling data and for use of computers and other devices.
- Conduct training for all employees, not just support staff, on protecting the firm's data.
- Develop an incident response plan to implement in the event of an attack.

The extent of this planning depends, of course, on the size of the firm, the type of data it maintains for clients, its resources, and the consequences to clients of a data breach. It is important to bear in mind, however, that cybersecurity is not just an IT issue, but a firm-wide effort. The accompanying sidebar lists steps a firm can take right away to reduce risk of an attack.

## Conclusion

Unfortunately, law firms of all sizes are increasingly attractive targets for hackers. Besides the desire to protect the firm's reputation and brand, attorneys owe an ethical obligation to their clients to be current on cybersecurity threats and take stronger steps to thwart hackers. Taking these steps will help to prevent cyberattacks, and if one does occur, reduce the resulting damage and potential liability. CL

**Mark Spitz** is the founder of Spitz Legal Counsel, a business law firm in Denver serving small- and medium-sized business clients on entity formation, transactions, acquisitions, and cybersecurity planning—(720) 575-0440, mark@spitzlegalcounsel.com.

**Coordinating Editor:** Joel M. Jacobson, joel@rubiconlaw.com

### NOTES

1. Mulvaney, "'*Ransomware*' locks down prominent Providence law firm," *Providence Journal* (May 1, 2017), www.providencejournal.com/news/20170501/ransomware-locks-down-prominent-providence-law-firm.
2. Thompson, "DLA Piper still struggling with Petya cyber attack," *Financial Times* (July 6, 2017), www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.
3. *ABA TechReport 2016*, www.americanbar.org/groups/law_practice/publications/techreport/2016/security.html.
4. *ACC Chief Legal Officers 2016 Survey*, www.acc.com/vl/public/Surveys/loader.cfm?csModule=security/getfile&pageid=1422254&recorded=1.
5. "ACC Issues Guidelines for Law Firm Cybersecurity Measures," ACC (Mar. 29, 2017), www.acc.com/aboutacc/newsroom/pressreleases/outsidecounselcybersecurityguidelines.cfm.
6. Colo. RPC 1.1, cmt. 8.