Cybersecurity and Small Law Firms

Cybersecurity and Small Law Firms

It seems like a long time ago, but when many of today's attorneys began practicing law, client files were on paper, in locked file cabinets maintained behind locked doors. Moreover, save for court appearances, nearly all work took place in the office. In this environment, many law firms may not have developed stringent controls related to information security. Corporate lawyers sometimes worried about corporate espionage, but approximately two-thirds of attorneys in 2015 practiced in firms of five or fewer, according to American Bar Association data. When you're handling divorces and automobile collisions, the market for stolen information can seem rather limited. Personal bankruptcy matters always involved credit card numbers and other financial information, but the risk of theft was low. Even if information was missing, the fallout was manageable, as there was no way to disseminate it on a grand scale and—in most cases—no way to use it.

If attorneys learned these kinds of work habits in their first few years of practice, they almost certainly brought them along as their careers progressed. In the 1990s and early 2000s, given the relatively low risks and low amount of damages, many law firms could get by with a *doveryai, no proveryai* ("trust but verify") approach to information security. As long as a few protocols were at least theoretically in place, malpractice insurance companies were satisfied and it was business as usual.

But while this attitude may be understandable, such an approach is simply no longer acceptable. The problem is too big, oversight is too intense, and the stakes are too high. More importantly, clients have the right to expect their attorneys' best effort in everything they do, which includes the implementation of appropriate cybersecurity measures designed to protect client information.

The Problem

A popular but fading myth is that information security breaches primarily affect hotels, financial institutions, and hospitals. Certainly, these incidents have far-reaching effects and they receive intense media scrutiny. But almost all industries and professions are at risk for major security breaches, and that includes the legal profession. The bad

news is that about 80 of the top 100 law firms have been breached at least once in the last five years. The worse news (or the better news, if you're a hacker) is that many of these firms either did not discover the breach for several months or did not notice it at all.

Attacks are increasing in frequency as well as severity. For example, the United Kingdom's Information Commissioner's Office reported in 2016 that the number of incidents increased a staggering 125 percent in only a year. In the United States, the widely repeated benchmark is now at least one major security breach per week. Moreover, direct costs (such as hiring forensic experts, offering restitution to victims, and consulting legal counsel) have risen to $158 per record per document in 2016, up 2.6 percent over 2015, according to the Ponemon Institute. Therefore, a few hundred missing files can cost a firm tens of thousands of dollars.

It may be tempting to read these warnings, focus on the "top 100 law firms" line, and conclude that cybersecurity is an issue for large law firms, not smaller ones. That would be nice, but as we explain below, it simply is not true.

"Smaller law firms are every bit as susceptible to cyber attacks as the big firms are," according to Lisa Jaffee, a claims consultant in CNA's Management Liability, Financial Institutions and Technology group. "It's just that they're vulnerable in different ways. The things that large law firms can do to beef up security won't necessarily translate to a successful strategy for a small firm."

To be blunt, larger firms can and do devote more resources to robust cybersecurity measures than smaller firms can muster—and it's easier for hackers to go through an unlocked door than a locked one. Moreover, large firms often have greater resources that enable them to absorb the attendant costs of these breaches than smaller firms. In 2015, the Securities and Exchange Commission reported that the cost of a cyber attack rose by 140 percent in just one year. In fact, half of small businesses that experience security breaches are forced to close within six months. Observing these facts together, the problem that small law firms face becomes apparent.

The Threats

When designing a security system, one of the first rules is to identify the threats. Protecting one's house against armed robbers may require a much different approach than if the attackers were teenagers looking for an instant thrill. The bottom line for small law firms is that the threats may be no greater or lesser than those large organizations face, but they are different and should be handled differently.

Third-Party Intruders

About half of cyber-attackers are third-party hackers who have no connection whatsoever to the organization. There are basically four different categories.

Some hackers, although probably not the majority of them, are classic cyber-thieves. These attackers typically look for financial data to steal, such as Social Security numbers, credit card information, and bank account numbers. Once upon a time, only bankruptcy lawyers had this type of data, at least among smaller law firms, because almost all clients paid either in cash or paper checks. Now, the smaller law firms that continue to dominate the legal landscape routinely have this information, because most clients pay by credit card, wire transfer, or some other paperless method. Moreover, almost all firms use billing software that stores much or all of this information in one location. The relatively high amount of readily available information, coupled with the relatively inadequate security procedures in place at most small law firms, means that information attractive to hackers is easily accessible.

Category two includes hackers with a political or social agenda they seek to pursue. They are often referred to as "hacktivists" in some circles. Some hacktivists steal information, but for the most part, the goal is to deface the firm's website or deny service to its clients, perhaps by disabling the communication and/or payment portals. Politically or socially active firms are especially vulnerable to these types of attacks, because there is often a not-so-subtle message that if the firm modifies its agenda, the attacks will stop. It should be noted that not all hacktivists are interested in headline-grabbing issues in the environment and politics. In fact, many are even more concerned about local land development issues and other matters that often involve area lawyers at a high level.

The third category relates to a subset of hacktivists who have no higher motivation or agenda to pursue. Rather, they attack to embarrass or annoy the lawyers in a firm. In other cases, the hacktivists send computer viruses or break into a law firm's system simply because they have the ability to do so if systems are not maintained in a secure manner.

Finally, there are "dumpster-divers" and other thieves who physically steal items, such as discarded credit card statements, or who break into off-site information vaults and storage lockers. This threat, while real, largely falls outside the cybersecurity realm.

Employees and Former Employees

All four of the outside groups noted previously have some nefarious intent, whether it be stealing information for personal gain or creating an unfavorable impression of the organization. When it comes to employees and former employees, however, the reasons for their actions vary.

As noted earlier, most legal work once took place almost entirely inside the office. Moreover, lawyers and staff worked on firm-provided equipment that was also firm-controlled. If the organization had confidential information in an electronic format, the data was stored on local servers that were kept under lock and key. Now, about three-fourths of all lawyers and law firm employees report that they work remotely at least a little, according to ABA data. Moreover, many law firms have established "bring your own device" (BYOD) policies—especially in smaller firms that pride themselves on creating a less formal environment. With the great number of tablets, laptops, and thumb drives utilized, it is not easy to keep track of all of these devices. In the foreseeable future, local servers may become extinct, similar to computer disk drives or VCR players, as offsite cloud storage continues to increase.

Inevitably, someone inadvertently walks out with confidential information, and most experienced hackers require only a small opening to wreak considerable damage. The working-remotely revolution also means that many lawyers use unsecured public Wi-Fi networks that almost any hacker may access.

Not all unintentional employee theft emanates from the firm's employees. For example, cloud providers may have insufficient security protocols or may not appreciate the difference between confidential and non-confidential information. In addition, the law firms that hire these providers are the ones responsible for such shortcomings.

Employee and provider breaches involve negligence, at best. However, with former employees, their motivations are often similar to thieves and hacktivists, and a disgruntled former employee also may become a cybersecurity risk. A former associate starting out on his own might tap into computer files to find personal information on former clients or former employees; a departing paralegal may believe she is owed money; or an ex-runner might be angry over a lack of promised opportunities.

The Rules

When a firm is aware of the threats to its security, the next step is to consult the applicable rules to determine what should be done to address it. Specifically, what legal and ethical duty do lawyers have to protect confidential information?

Ethical Responsibilities

The American Bar Association's *Model Rules of Professional Conduct* address information in both a general and specific manner. Under the rules, violations may or may not lead to disciplinary proceedings, but violations always mean that the lawyers have not met the expectations of their clients or themselves.

Rule 1.1 requires a lawyer to provide competent representation to a client. Typically, lawyers interpret this rule as applying to legal work performed on a client's case. A proper information security protocol is part of professional competence. Arguably, issues of trust arise, because lawyers who fail to safeguard client data may fail to safeguard other confidential information as well. The comments offer additional insight into this duty. Comment 8, which discusses the ongoing duty to develop and maintain competence, specifically mentions "the benefits and risks associated with

relevant technology."

Rule 1.6 is the confidentiality provision, which represents a primary tenet of the profession. The prohibition is absolute, because the rule says that attorneys shall not disclose such information relating to the representation of a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation, or is otherwise permissible under Rule 1.6. Rule 1.6 implies that disclosure can be either intentional or accidental. In fact, subsection (c) commands every lawyer 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 lists several factors to consider, including the economic and noneconomic costs of the security protocol (*e.g.* a software system which has so many security layers that it is difficult to use), the nature of the information, and the likelihood of disclosure. This same standard applies to information transmittal and to former clients.

Finally, Rule 1.15 involves the safekeeping of client property in an independent trust account. These trust accounts are created because a lawyer may not co-mingle client owned funds with the lawyer's own personal property. Currently, there are many check fraud scams that are targeting law firms. Essentially, the fraudster seeks to retain the lawyer through email communications. The lawyer is eventually sent a fraudulent check to deposit in the lawyer's trust account. The fraudster then demands release of the funds on an expedited basis prior to the banks discovering the fraudulent note. The net result is that the lawyer is duped into releasing client funds, for which the lawyer will then become personally responsible for replenishing.

Common Law Standards

Confidential information is confidential information, whether it is a trade secret, a client's identity, notes from an expert witness, or financial information, and disclosure of such information has significant consequences for everyone involved.

In addition to the ethical rules, many courts rely on the *Restatement (Third) of the Law Governing Lawyers* when determining the nature and extent of professional liability. Section 50 of the *Restatement* imposes a duty of care "in pursuing the client's lawful

objectives in matters covered by the representation." So, anything contrary to the client's interests, which includes inadvertent information disclosure, violates the duty of care.

Government Requirements

A number of federal laws relate to cybersecurity and information disclosure, but the two statutes that directly affect the practice of law most directly are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Fair Credit Reporting Act (FCRA). HIPAA covers protected health information, which is individually identifiable information pertaining to diagnosis or treatment of a medical condition. Meanwhile, the FCRA limits disclosure of personally identifiable information (PII), including Social Security numbers, driver's license numbers, credit card numbers, financial account information, medical information, and (in some states) online passwords.

Obviously, health care attorneys are not the only legal professionals who obtain health care information. Such data is an integral part of negligence, workers' compensation, and criminal cases. Other matters also may involve a person's physical, mental, or emotional condition. As for PII, most billing software programs on the market require users to enter at least some of this information.

Notably, 47 states now have security breach notification statutes. Requirements vary by jurisdiction, but most of these laws have specific requirements in terms of applicability, what constitutes "personal information," and notice requirements in the event of a breach.

The Solution

Given the scope of the issue and the applicable liability rules that affect law firms, what are the features of a reasonable cybersecurity solution?

"Partners at small firms know better than anyone that one size definitely doesn't fit all," according to Michael Barrett, Risk Control Director for CNA's Lawyers Professional

Liability Program.

To create a security policy that confronts the threats and follows the rules, Barrett said, "small firms should choose a coverage strategy that stresses prevention over response and treats even one data breach as one too many."

These preventive measures are best practices that even the smallest law firm can implement to fulfill their duties in the fight against cyber threats:

- Encryption: Sending e-mails and storing information in plain text is simply not acceptable, because it is easy and cost-effective to convert such information to ciphertext. As a bonus, encrypted information is verifiable in terms of source and authenticity, which makes audits more effective.
- Cloud Providers: It is not against the law or the rules to store data offsite in order to save some money, but such a task should not be outsourced to an individual or company that does not guard information with at least the same diligence that you use yourself.
- BYOD: Consider limiting bring-your-own-device and unsecured Wi-Fi practices. For example, allow paralegals to work at Starbucks, but forbid them from pulling up confidential information over latte.
- Training: These programs must be more than *pro forma*. While online videos and self-study sessions can be viable learning opportunities, these resources should probably be augmented by regular joint live training sessions.
- Passwords: In another few years, biometrics and facial recognition may make passwords obsolete. But for now, a simple requirement, such as using special characters, significantly upgrades security.
- Insurance: A cybersecurity insurance policy is often a good investment. In addition to coverage, an insurance company is a resource that can help you identify shortcomings and head off future claims.

Diligent execution is an important part of a preventive plan. Cybersecurity is not like fire insurance and should not be kept under a glass that says "break only in the event of a breach." By the time a breach occurs—and it will happen sooner or later—the best security plan in the world will be absolutely meaningless.

Although the problem is daunting and the stakes are high, with just a few basic

safeguards, your law firm can comply with the rules and requirements while it increases client confidence in your services.

For more information about CNA's business insurance products, visit www.cna.com.

SOURCES:

2016 Ponemon Cost of Data Breach Study, The Ponemon Instute

Data Security Incident Trends, United Kingdom Information Commissioner's Office

Cyber Claims Study, 4th edition, NetDiligence

Lawyer Demographics, 2015, American Bar Association

"13 Important Virtual Workplace Statistics and Trends," Brandon Gaille

Model Rules of Professional Conduct, American Bar Association

Virtual Law Practice – ABA Tech Report 2014, American Bar Association

"The Restatement of the Law Governing Lawyers: A View From the Trenches," *Hofstra Law Review*

Security Breach Notification Laws, National Conference of State Legislatures

Summary of the HIPAA Security Rule, Department of Health & Human Services

Fair Credit Reporting Act, Federal Trade Commission