Why Should Law Firms Care about Cybersecurity Breaches?

By Nicolle L. Schippers

As lawyers, no matter the size of your practice or your practice areas, you wear many hats—including staying on top of what is influencing your practice and your license. With the implementation of technology into our practices, even a simple e-mail communication can have a significant impact. While at one time law firms seemed to be immune to the data breaches and cybersecurity issues that plagued other businesses, this is no longer the case.

LAW FIRMS UNDER CYBER-ATTACK

Data breaches in law firms made the headlines throughout the last two years. As recent as late June 2017, global law firm DLA Piper suffered a data breach that led the firm to shut down digital operations around the world. This breach came on the heels of another incident that made headlines in 2016, when the Panamanian law firm, Mossack Fonseca, suffered a data breach in which more than 2.6 TB of data were stolen and 11.5 million sensitive records were taken without the firm detecting any sign of theft—an event dubbed the "Panama Papers."

In related news, *Big Law Business* reported in March 2016 (tinyurl.com/zdbxccb) that the FBI issued an alert after they had discovered a post on an undisclosed cybercriminal forum of a person wanting to hire hackers to break into international law firms' computer networks and use the data for insider trading. The former head of the Cyber Security Crime Division of the U.S. Attorney's office in Manhattan said this wasn't the only investigation and that other federal criminal investigations were opened in response to law firm breaches. It was clear any "immunity" law firms may at one time have held from data breaches and cybersecurity issues was gone.

In fact, the above-mentioned firms aren't the only examples of firms that had data breaches, and regrettably there will be others . . . and small and solo firms are not excluded. Also unfortunate for firms is that with data breaches come threats of litigation. According to Jay Edelson, founder of Edelson PC, a plaintiffs' class action firm, his firm conducted a year-long investigation and identified 15 major law firms with inadequate cybersecurity and is taking action. It appears that many firms have cybersecurity policies in place; however, they are not enforced. This is ill advised as law firms, regardless of size, have data that is of very high value, specifically business transactions and personal information data that can be linked easily to financial gain for hackers or their clients.

Law firms once seemed immune to data breaches. This is no longer the case.

These headlines along with the Panama Papers scandal have, according to Nicholas Gaffney, "put an uncomfortable spotlight on law firms and their data security programs. This may be the much needed wake-up call to law firms—big and small—to conduct an audit of their information security systems and protocols, and be more proactive in their efforts to prevent data breaches that could potentially have significant ramifications, both for their clients and their livelihood" ("Law Firm Data Hack Attack, Part 1," *Law Practice Today,* April 14, 2016, tinyurl.com/hqofudx).

"The legal industry is the latest gold mine for hackers, whose attacks continue growing in sophistication, frequency and motivation," says Mark Stevens. "Most law firms do not have basic cybersecurity controls in place for detecting and mitigating data breaches. The incident at Mossack Fonseca just scratched the surface of demonstrating the lack of cybersecurity resources within the legal sector, as 90 percent of law firms have five or fewer employees dedicated to information security and safeguarding the business' crown jewels" ("A Brief History of Law Firm Cyberattacks," *Law360,* June 2, 2016, tinyurl.com/ybvp6twp).

According to Vincent Polley, coauthor of a book for the American Bar Association on cybersecurity, "A lot of firms have been hacked, and like most entities that are hacked, they don't know that for some period of time. Sometimes, it may not be discovered for months and even years."

Jody R. Westby puts it another way: "Law firms have never been very good with technology, and now they are struggling, as breaches in firms have made headlines, and clients increasingly are asking questions about their security programs" ("Cybersecurity & Law Firms: A Business Risk," *Law Practice*, July/August 2013, tinyurl.com/ybja9ble).

THE ETHICS OF CYBERSECURITY

Regardless of this struggle, what firms and attorneys must remember is they have ethical duties that require them to protect and maintain confidential attorney client information and work product information. Specifically, the following ABA Model Rules of Professional Conduct come into play with cybersecurity (please note this is not an exhaustive list):

Competence. According to Model Rule 1.1, "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Comment 8 to Rule 1.1 (Maintaining Competence) states:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

This Comment makes it clear that lawyers need to stay on top of technology advancements, including staying up-to-date on the latest security standards. It arguably includes examining information about security providers and understanding the safeguards in place at those providers who store your data.

iStock

Confidentiality. Model 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."

Note that a client may require a lawyer to implement special security measures not required by the Rule, or the client may give informed consent to forgo security measures that would otherwise be required by the Rule.

Don't wait for your firm to be hacked—it's not a matter of if, but when.

Comment 18 of the Rule provides more guidance: "Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."

The Comment further states:

> The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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).

The Model Rules appear to say a law firm can avoid an ethics violation stemming from a breach if the firm has a strong security program and acted in a competent manner to protect its client data from disclosure.

The Model Rules do not appear to address whether an attorney has to tell clients about a breach. However, according to law professor Benjamin Cooper (in an interview in Jody R. Westby's article cited above), "If the lawyer's conduct of the matter gives the client a substantial malpractice claim against the lawyer, the lawyer must disclose that to the client. . . [F]irms have a duty under Rules 1.1 and 1.6 to effectively protect their clients' information. If a firm is negligent in carrying out that duty because it has been lax with its security, and that resulted in client files being disclosed, it is potentially a problem." Even if a firm has a very good security system, he observes that "the attorney absolutely has a duty to inform clients under 1.4 that their confidential information has been compromised."

Supervision of staff. Model Rule 5.3 states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer: (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer; (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer.

This Rule requires you to train your staff on your cybersecurity policies—not only initial training but continual training when policies are updated or new information on security standards is learned by the lawyer. Some would argue the lawyer should audit the staff to ensure employee understanding and compliance with firm polices.

According to Berkeley Research Group's 2016 Cybersecurity Preparedness Benchmark Study (tinyurl.com/yaaglrbw), current employees of organizations are the likely cause behind most cybersecurity breaches—in fact as high as 45 percent of organizations reported that current employees were the likely source of a breach, followed by 22 percent of breaches caused by hackers and 13 percent by former employees. "Organizations must do more to deter [data] theft by educating and regularly training employees on cybersecurity or other protocols."

RANSOMWARE

Another important reason for training of the staff on cybersecurity issues is ransomware attacks. According to a survey by the security firm Malwarebytes (tinyurl.com/y7dwzlx4), nearly 80 percent of U.S. companies suffered a cyber-attack in 2015, and 50 percent experienced a ransomware attack (tinyurl.com/y9zlrbva).

What is ransomware? According to David Meyer, ransomware is a particularly nasty stain of cybercrime where criminals break into the victim's computers and encrypt files or whole drives, then demand payment to return access to the data ("The Ransomware Epidemic

Is Growing and Hurting a Lot of Businesses," *Fortune,* August 3, 2016, tinyurl.com/y8tol8u7).

The important thing for law firms to remember is that many times the attacks resulted from employees' clicking on something in an e-mail they shouldn't have. The e-mail can contain a link or attachment. The e-mail is addressed to them and for all intents and purposes looks legitimate. When recipients click on the URL or attachment, they are directed to a website that infects their computer with malicious software. These types of e-mails prey on employees, and it only takes one click for your entire firm to be compromised.

How can ransomware impact you and your firm? Unfortunately, results include the inability to access your data and your clients' data, disruption to your firm's operations, financial losses incurred to restore systems and files, possible ethical violations, and potential harm to the firm's reputation. Many times you are unaware of the attack until you can no longer access the data or until you see unusual messages on your computer demanding payment in exchange for a decryption key.

WORKING WITH CYBERSECURITY VENDORS

One method to help ensure your firm is protected as much as possible is to hire a vendor who specializes in cybersecurity prevention. Whenever hiring such a third party, you should remember to include the following recommended provisions within your contract (please note it is important you gain advice from a lawyer who specializes in these types of contracts; also note that not all these clauses may be appropriate for certain transactions):

- **Indemnification provisions.** If the vendor has access to confidential data, it should be responsible for its breach of the data and indemnify you for such breach.
- **Limitations on liability.** As with indemnification, it is important to review any limitations on liability to ensure that if there is a breach and it was caused by or should have been prevented by the service provider, the limitations of liability isn't such that you have no ability to adequately recover.
- **Warranty provisions.** A service provider cannot warrant everything. However, if the provider waives all warranty provisions, is that something you are willing to accept? Beware of allowing waiver of warranty for the very thing you are paying them money to do.
- **Privacy and confidentiality requirements.** It is very important that the service provider has security measures and privacy policies in place to protect any confidential data received from you. It is also important you not only include this provision but you ask the vendor about its measures and policies, including exercising the right to review a copy if appropriate.
- **Cybersecurity insurance policy requirements.** Not only should your firm look into cybersecurity insurance to protect your business, but you should determine whether to require your service providers to have cybersecurity insurance.
- **Right to audit to monitor compliance with agreement terms.** All the above provisions are good, but it is important to include a provision whereby you have the right to audit the provider to determine if it is in compliance—even if you decide not to use it.
- **Adherence to all applicable federal laws regarding privacy and confidentiality of certain data.** It is important to include a provision that requires all parties to comply with applicable federal laws.
- **Notification of a breach or suspected breach.** It is important to include a provision stating who is required to notify the other party about a breach or suspected breach and during what time frame. Most sample notification provisions entail the vendor providing this notification to the law firm, but ensure you also include *when* the vendor must notify you and through what method of communication.
- **Destruction of information upon termination of the contract.** If the service provider has or will have access to confidential data of yours, it is important to include a provision about what it must do with the data upon termination of the contract. Many such provisions state the provider must return the data to the lawyer or destroy the data and provide you with a certification of such destruction.

CONCLUSION

The above provisions and ethical requirements only touch the surface of what an attorney must know about this increasingly complex cyber-world, but hopefully they will get you started. There are many resources out there, and it is recommended you review them as well as seek the assistance of a lawyer who is well versed in such contracts.

Be proactive and increase your security standards now. Don't wait for your firm to be hacked—it is not a matter of if, but when. ■

Nicolle L. Schippers (araglegal.com; Twitter: NSchippers1), JD, is the Associate General Counsel and Legal Industry Advocate at ARAG, an international legal insurance provider, where she advocates for closing the access-to-justice gap, encouraging dialogue and a proactive approach in the legal profession. She serves on the Association of Corporate Counsel (ACC) Board of Directors, the Iowa State Bar Association (ISBA) Board of Governors, and the Iowa Access to Justice Commission. This article is based on a presentation originally given at ABA TECHSHOW 2017.