ARTICLES

Cybersecurity and the Lawyer's Standard of Care

By Joseph Salvo and Brian Middlebrook – May 22, 2018

Attacks on the Rise

Law firms are the guardians of a wealth of confidential and valuable information, rendering them an ever-growing target of cyber attacks. Back in 2012, the *Wall Street Journal* reported that "cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients' secrets are having to reboot their skills to the digital age." Jennifer Smith, "Client Secrets at Risk as Hackers Target Law Firms," *Wall St. J. Law Blog*, June 25, 2012. In May 2014, New York Ethics Opinion 1019 warned attorneys about this threat, stating that "lawyers can no longer assume that their document systems are of no interest to cyber-crooks."

The passage of time not only has proven this to be true, it has burdened law firms of all sizes with the undeniable obligation to be cognizant of the risks posed by these breaches and to take affirmative steps to plan for and prevent breaches from occurring. The multitude of different attacks—business email compromise, data exfiltration, ransomware, and monitoring for insider trading opportunities, among others—has grown steadily over the past five years. As a result, the plaintiffs' bar argues that a breach of a law firm's information technology (IT) system is a breach of the firm's professional responsibilities.

Cyber attacks have become so frequent that it is no longer a matter of *whether* firms will be the victim of a cyber attack, but a question of *when* and *to what extent*. ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 477 at 2 (May 11, 2017). Cyber attacks are affecting firms across the globe. Law firms that have fallen victim to cyber attacks have reported business downtime or loss of billable hours or both, hefty fees for correction, costs associated with having to replace hardware and software, and loss of important files and information, not to mention harm to reputation and an erosion of the trust placed in them by current and prospective clients and the public alike. *See* Kathryn T. Allen, "Law Firm Data Breaches: Big Law, Big Data, Big Problem," *Nat'l L. Rev.*, Jan. 11, 2017.

For example, the well-publicized June 2017 "Petya" malware attack on DLA Piper shut down the firm's email, phone systems, and operations for three consecutive days, and before being reconnected to the firm's network, all computers and devices had to be inspected and cleared. Jeff John Roberts, "Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear," Fortune (June 29, 2017). In addition, in December 2016, three individuals were charged with hacking into at least seven law firms in 2014 with the intent of obtaining inside information about prominent merger and acquisition deals. These hackers obtained 40 gigabytes of confidential information over the course of 8 days, which they used to purchase shares of stock, which yielded a profit in the amount of $4 million. Daniel Solove, "Law Firm Cybersecurity: An Industry at Serious Risk," *Teach Privacy*, Feb. 16, 2017.

In 2016, the Federal Bureau of Investigation warned of a Ukraine-based Russian hacker known as "Oleras" who solicited other hackers to attack 48 top Chicago law firms, targeting company mergers and acquisitions information through phishing schemes. In the same year, 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. Yet, in 2015, the *ABA Legal Technology Survey Report* found that almost half of the 90,000 private practice attorneys polled said their firms have no data breach response plan in place. By 2017, the *ABA TECHREPORT* found that 22 percent of respondents overall reported that their firms had experienced a data breach at some time—up from 14 percent in 2016 and an 8 percent increase over the prior four-year average. David Ries, "Security," *ABA TECHREPORT* (2017).

The Lawyer's Cyber Standard of Care

While ethical rules, common law, contracts, and industry-specific laws and regulations have long required attorneys and law firms to protect confidential client information, cyber threats and attacks have changed the manner in which firms are required to protect that information. Specifically, the commentary to Rule 1.1 of the Model Rules of Professional Conduct expects attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Indeed, depending on a multitude of factors, including the practice and size of a firm, it may now be incumbent upon law firms to monitor network activity, review IT reports, and perhaps employ a chief information officer (CIO) in developing, implementing, and maintaining appropriate cybersecurity programs. *See* Ethan S. Burger, "Cyber Attacks and Legal Malpractice," *U.S. Cybersecurity Mag.*, July 15, 2016. Failure to take these precautions and affirmative actions can have dire consequences, including claims for legal malpractice.

Cybersecurity Legal Malpractice Claims

Cybersecurity legal malpractice claims typically sound in negligence for failure to protect client confidential and personal data or supervise members of the firm, as well as fraud and misrepresentation. Plaintiffs' attorneys are continually attempting to expand what constitutes an attorney's standard of care—that is, whether the attorney "failed to exercise the ordinary reasonable skill and knowledge commonly possessed by a member of the legal profession." *Rudolf v. Shayne, Dachs, Stanisci, Corker & Sauer*, 867 N.E.2d 385, 387 (N.Y. 2007). For example, in *Shore v. Johnson & Bell*, Case No. 16-cv-4363 (N.D. Ill. 2016), a putative class action was filed against a Chicago law firm over alleged cyber vulnerabilities—the first public class action against a law firm for alleged inadequate cybersecurity. In addition, in *Millard v. Doran*, Index No. 153262/2016 (Sup. Ct. N.Y. Cty. 2016), a malpractice suit was brought against a New York attorney after the attorney's email was hacked, which caused the plaintiff clients to wire $1.9 million to cyber criminals.

More generally, theories of liability for cyber claims overall also are continuing to expand beyond the common negligence claim for breach of a specified standard of care. Under the "overpayment theory," a plaintiff alleges that the price paid for the legal services to the attorney or firm included some indeterminate amount allocated to data security, and the plaintiff has not received the "benefit of the bargain" because of the data breach. *See, e.g.*, *In re VTech Data Breach Litig.*, Case No. 1:15-cv-10889, 2017 WL 2880102 (N.D. Ill. July 5, 2017). In addition,

some states that have enacted cybersecurity/data breach legislation authorize a private cause of action by the affected client against the firm in order to recover damages caused by the breach. *See, e.g.*, Cal. Civ. Code § 1798.80 et seq.

How to Avoid Claims

While the duty of a lawyer to protect confidential client information is sacrosanct, in the digital age, this obligation undoubtedly extends to taking affirmative steps to prevent the unauthorized access of client information. Law firms must be aware of the risks of these attacks and create a protocol to prevent them. The first step requires evaluating the type of information that the law firm possesses in order to determine the necessary protocol to put in place. Law firms' servers hold valuable information, such as business intellectual property, medical records, bank records, and government secrets, which makes firms a prime target for hackers looking for information that they can monetize.

Law firms also need to evaluate vulnerabilities in their systems and create a data security plan that speaks to every member of their team. This begins with effective employee training and education on a continuous basis. Given the evolving nature of the cyber attacks and development of technology, annual training is not enough. Employees should be educated on how to handle sensitive data securely, which should be tailored to the specific needs of each individual firm, depending on the type of data that the firm possesses. For example, if the firm routinely possesses sensitive medical information, all employees should be educated on how to handle, receive, and transmit this information in accordance with the firm's security plan as well as federal and state regulations related to the Health Insurance Portability and Accountability Act. This education also should include how to detect cyber attacks (e.g., a phishing email) and what to do in the event that an attack is perceived or actually occurs.

In addition, the law firm's data security plan should include protective measures such as two-factor authentication, encryption, and secure network use. Two-factor authentication is a process requiring two different authentication methods to prevent unauthorized access of private and sensitive information. Three main categories of authentication factors are, generally, something you know (password, personal identification number (PIN) code, Social Security number); something you have (USB security token, bank card, key); and something you are (fingerprint, eye, voice, face). The two-factor authentication process requires just that—two of these factors. According to Symantec, a leading authority in cybersecurity, 80 percent of breaches can be prevented by using multifactor authentication. MyPinPad, The Present and Future of Two-Factor Authentication (June 9, 2017).

Other safeguards and protective measures include continuous maintenance of operating systems and software programs; installation of antivirus and firewalls to prevent common malware infections; conducting third-party vulnerability scans, penetration tests, and malware scans; and ensuring that the firm's protective measures extend to its remote access programs (e.g., Citrix, iTwin, Remote Control) for employees who use remote access. Many firms have begun to develop "cybersecurity incident response plans," which strategically identify the protective

measures that the firm has in place, what to do in the event of an attack, and long-term and short-term plans for updating the program overall. In addition, firms have appointed "cybersecurity information officers" responsible for implementing and overseeing these plans.

Ninety-seven percent of cyber attacks can be thwarted by common security practices that law firms of any size can employ. Robert Hilson, "This Article on Lawyer Cybersecurity Will Scare You Out of a Malpractice Suit," *Logikcull*, June 10, 2016. These are the statistics used by plaintiffs in arguing that a law firm failed to exercise reasonable care. If confidential information is obtained through a cyber attack, a multitude of statutory, tort, and contractual theories of liability in legal malpractice may exist. Accordingly, it is imperative for all firms, big and small, to take a long, hard look at their cybersecurity practices and implement proactive measures to mitigate the associated risks.

Cybersecurity insurance coverage also is an effective tool for law firms to mitigate liability and financial loss in the event of a cyber attack. With cyber attacks on the rise, cybersecurity insurance coverage, whether it be through a rider to the firm's professional liability policy or a separate cyber policy, is a must. However, this requires careful examination of the terms of the policy and applicable exclusions. Many law firms mistakenly believe that their traditional malpractice policy will cover any number of cyber-related claims, even those that do not result in a traditional malpractice claim.

The available coverage in the event of a cyber attack has been the subject of much litigation in recent months, with insurance companies arguing, for example, that events such as the fraudulent transfer of funds in response to a phishing attack are not covered under the policy's computer fraud, funds transfer fraud, and forgery clauses. Such policies often are not as comprehensive as one might think. The safest route is usually to purchase a policy that is specific to cyber-related issues, which often are unrelated to traditional legal malpractice claims.

Conclusion

Ultimately, a lawyer's or law firm's standard of care is a moving target in the digital age. As firms progressing into the digital age more frequently use artificial intelligence (AI) services to perform legal research and write briefs, it is likely that a data breach will occur when using these services and that a malpractice claim will arise, alleging that the firm failed fully to protect the clients' data when using the AI services. While firms may see AI services as a source of client development and revenue generation, firms still need to implement the protections set forth above when using these services. Even more, a firm that is the victim of a ransomware attack also may be subject to a malpractice claim, raising the question of whether the firm owes the client a duty to pay the ransom to retrieve the sensitive information that was accessed and whether the firm violates that duty should it choose not to pay the ransom.

Undoubtedly, the publicity that data breaches receive and the growing body of legislative and regulatory efforts put the onus on not only those in custody of private information but also those hired by such entities to meet stringent data protection requirements or face fines, penalties, and

civil liability. *See, e.g.*, N.Y. Gen. Bus. Law § 899-aa (giving the state attorney general the right to bring an action against a business for violation of New York's cybersecurity regulations); N.Y. Comp. Codes R. & Regs., tit. 23, pt. 500 (governing institutions regulated by the New York Department of Financial Services); European Union General Data Protection Regulation (requiring businesses in the European Union (EU) to protect the personal data and privacy of EU citizens for transactions that occur within EU member states). Many states have regulations similar to New York's, which allow the attorney general or another governmental entity to bring an action against the business for violation of the state's cybersecurity regulations.

The "police" are no longer interested in only the "bank robber"; they are coming after the "bank." That inherently must change the way those with access to private information protect that information, including lawyers and law firms.

Joseph Salvo and Brian Middlebrook are partners in the New York City office of Gordon Rees Scully Mansukhani, LLP.

None of this information/material is offered, nor should it be construed, as legal advice. Communication of information by or through this publication and your receipt or use of such information is not intended to create an attorney-client relationship. You should not act or rely upon information contained in these materials without specifically seeking professional legal advice.