New Jersey Law Journal

JANUARY 27, 2020 ESTABLISHED 1878

IN PRACTICE

CYBERSECURITY

Data Breaches: Adding a New Layer to the Risk of Legal Malpractice

By *Karen Painter Randall and Steven A. Kroll*

The news these days is filled with reports of significant data breaches. In fact, most experts opine that it is not a matter of "if" but "when," as to whether an entity will fall victim to a cyberattack. Unfortunately, those in the legal profession are not immune to a data breach. What's more, ethical obligations put lawyers and law firms at even greater risk for significant business, financial and reputational harm should they experience a cyberattack. More firms are falling prey to schemes as simple as "phishing" tactics or as sophisticated as a coordinated cyberattack, exposing client data that could include sensitive financial information, market-influencing mergers and acquisitions intelligence, and intellectual property from a patent filing. As a result, attorneys have both an ethical and legal duty to take reasonable steps to protect their clients' personal sensitive data against a cyberattack, or face serious ramifications.

Why Law Firms Are Prime Targets

Law firms are a soft target to hackers as they possess a large volume of critical data. For example, an attorney involved in a highly sensitive business transaction has access to information ranging from a client's personally identifiable information (PII), to details of a business' confidential transactions. Moreover, through discovery and the litigation process, law firms gain access to, among other items, their clients' as well as adversaries' PII, personal health information (PHI), and confidential financial information. Everything from trade secrets, to sensitive market-moving information about a company's finances, to a client's PHI occupies a law firm's files and servers. Additionally, because attorneys tend to identify and isolate this information, hackers are able to quickly and efficiently locate this highly sensitive data. As such, by targeting law firms, cyber criminals have the ability to access a plethora of valuable information located in one place.

Moreover, law firms tend to employ fewer resources toward implementing strong cybersecurity controls, making them more susceptible to an attack. According to the American Bar Association Legal Technology Resource Center's 2019 Legal Technology Survey Report, 26% of respondents report that their firms have experienced some sort of security breach (ranging from hacker activity and website exploits, to more mundane incidents such as lost or stolen laptops). Although the 26% figure is notable, also eye-catching is the 19% of respondents who reported that they do not know whether their firm has ever experienced a security breach. Moreover, the survey found that only 31% of the respondents had an incident response plan. Additionally, only 44% of the respondents use file encryption, 38% use email encryption, and 22% use whole/full disk encryption.

It is evident that heading into the new decade, law firms will continue to be ripe targets for a cyberattack, and must take steps to add additional layers of protection to safeguard their clients' information, and to reduce the possibility of a malpractice claim.

Legal and Ethical Consequences of a Breach

The ethics rules require attorneys to be competent and take reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and comments). The comments to ABA Model Rule 1.1 state that "[t]o 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." In June 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R on the subject of a lawyer's ethical obligations to secure communication of protected client

Karen Painter Randall is the Chair of the Cybersecurity and Data Privacy Group, and Steven A. Kroll is an Associate in the Group, at Connell Foley LLP in Roseland, NJ. This article also appeared in the New Jersey Law Journal, an ALM sibling of Cybersecurity Law & Strategy.

information. The Opinion took a fresh look at advances in technology and ever-increasing cybersecurity threats, and provided guidance as to when enhanced security measures are appropriate when transmitting protected client information. The Opinion stated that it is not always reasonable to rely on the use of unencrypted email, thus, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters to determine what effort is reasonable.

The Committee recommended the following steps lawyers should take to guard against disclosures, including: understanding the nature of the threat; understanding how client confidential information is transmitted and where it is stored; understanding and using reasonable electronic security measures; determining how electronic communications about clients' matters should be protected; labeling client confidential information; training lawyers and non-lawyer assistants in technology and information security; and conducting due diligence on vendors providing communication technology.

Over a year later, on Oct. 17, 2018, the American Bar Association Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 483, detailing a lawyer's obligations after an electronic data breach or cyberattack. The ABA Committee recognized that "[a]s custodians of highly sensitive information, law firms are inviting targets for hackers." The Opinion outlined certain reasonable steps that the Committee believed lawyers should take in the event that a data breach occurs. In doing so, the Committee addressed an attorney's obligation to monitor for a breach, to stop a discovered breach and restore systems, to determine what information was compromised, to evaluate notice obligations, and to determine what information must be provided to clients and former clients in the event of a breach. The ABA Committee further recognized that an attorney's obligation in the event of a data breach or cyber-attack necessarily touches upon Model Rules 1.1, 1.4, 1.6, 5.1, and 5.2, which address, among other things, an attorney's duty to his or her client while using technology.

Accordingly, attorneys have an ethical duty not only to be competent when it comes to the use of technology, but to have reasonable safeguards in place to protect and respond to a data breach. The failure to do so has resulted in lawsuits being filed, sounding in professional malpractice. For example, in Millard v. Doran, No. 153262/2016 (Sup. Ct. N.Y. Cty.), a malpractice suit was brought against an attorney for allegedly permitting cybercriminals to hack into the firm's email system and to read and intercept communications held within. This resulted in the plaintiff fraudulently wiring $1.9 million to the cybercriminals. An example on a larger scale occurred in 2017, when a class action was commenced against the law firm Johnson & Bell not for any actual breach, but rather for having inadequate data security measures in place. As to damages, the class sought injunctive relief, the requirement that the firm inform its clients that its computer systems are not secure and undergo a security audit, the forfeit of fees and profits the firm allegedly diverted from having been spent on cybersecurity, attorney fees and expenses, and pre- and post-judgment interest.

To the extent law firms continue to ignore their ethical and legal obligations to guard against a cyberattack, it is expected that even more professional malpractice lawsuits will be filed.

Avoiding Malpractice Claims

Cybersecurity is everyone's responsibility in a law firm. Buy-in must flow from the top down to ensure a culture of security in the organization. Law firms should create a cross-organizational committee, which includes not only management but human resources, procurement, finance and 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 that the policies and procedures are consistent with the security plan and technology. Using resources like the National Institute of Standards and Technology (NIST) as guidance for implementing a data security program is a good start. It is a comprehensive and flexible template for managing risk. The five pillars of NIST include: Identify, Protect, Detect, Respond and Remediate. Thirty percent of U.S. companies currently use the NIST framework to manage their cyber risk. By 2020, the number of companies is expected to increase to 50%.

In addition, a law firm should conduct an inventory of its 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 or an outside vendor should conduct third-party vulnerability scans, penetration tests, and malware scans to protect against potential breaches. The use of antivirus software is simply not enough to detect sophisticated attacks that sometimes go undetected for an average of 300 days.

Most importantly, after setting the tone from the top, law firms must train employees so that they are aware of the company's security protocol, and 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 are very easy to use and protect clients' data and privacy when sending sensitive emails and attachments.

The new digital age imposes a greater ethical and legal responsibility on the legal

profession to protect the confidentiality, integrity and availability of a client's data. With the increased threat of cybersecurity-related malpractice claims, it is imperative that attorneys comport their practice to evolve with today's changes in technology.