By DANIEL J. SIEGEL

Responsible Cybersecurity Response

Data Breaches, Security and Ethical Obligations . . . Online

Has your law firm experienced a data breach? If your answer is a knee-jerk "no," perhaps you should reconsider. According to the 2017 American Bar Association *Legal Technology Survey Report*, 22 percent of survey respondents reported that their firms had experienced a data breach, with 35 percent of the firms with 10 to 49 attorneys reporting a breach. One in every ten solo firms also reported a breach.Why?

According to Trend Micro[1], a data breach "is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. . . . Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security." The company noted that "based on the number of data breach incidents recorded between January 2005 and April 2015, personally identifiable information (PII) was the most stolen record type while financial data came in second."

Attorneys, of course, have an ethical obligation to protect confidential client information and other sensitive information. In 2018, the Pennsylvania Supreme Court emphasized this obligation when the Public Access Policy went into effect, requiring the redaction of sensitive and confidential information and documents in court filings. Even so, most attorneys, particularly those who practice in solo and small firms, do not expend much, if any, effort proactively protecting their firms against data breaches.

Not only do the statistics confirm this lack of concern, but when I ask attorneys how or if their firms prepare for a data breach, I get little response. Should such a breach occur, these firms will simply improvise and hope that they avoid problems.

The ABA Standing Committee on Ethics and Professional Responsibility recently addressed this issue in Formal Opinion 483 (October 17, 2018), "Lawyers' Obligations After an Electronic Data Breach or Cyberattack." In the Opinion, the Committee concluded that "[w]hen a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules."

The Opinion notes that lawyers and law firms are inviting targets for hackers because they are custodians of highly sensitive information. As a result, "[d]ata breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession."

The Opinion initially explains that it addressed data security in Formal Opinion 477R[2], which discussed an attorney's ethical responsibility to use reasonable efforts when communicating client confidental information using the Internet, noting that "this opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information."

The Committee's central conclusion is that an attorney's obligations under the Rules of Professional Conduct after a breach depend upon the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.

To reach its conclusion, the Opinion begins by analyzing Rule 1.1's requirement that an attorney's duty of competence includes understanding the technology relevant to his or her practice. This duty includes an obligation to monitor for a data breach, which it

defines as "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."

Next, the Opinion notes that:

> [L]awyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred, whether further action is warranted, whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties, and how and when the lawyer must take further action under other regulatory and legal provisions. Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information. (2018, p. 5)

Should a breach occur, or be suspected, Rule 1.1 requires a lawyer to act reasonably and promptly to stop the breach and to mitigate damage resulting from the breach. However, because breaches occur in many forms and their breadth differs dramatically, the Opinion offers no advice how to respond when one occurs. Rather, the Opinion suggests that a lawyer must make reasonable efforts to determine what occurred during the breach. In addition, the attorney, or the person investigating the breach on the attorney's behalf, should verify that the intrusion has ended and determine the extent of the data accessed or stolen.

The Opinion goes on to explain that an attorney's duty, even in the event of a data breach, is one of reasonable care, citing the ABA Cybersecurity Handbook, which states:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.

After making these assessments, attorneys should evaluate their obligations to provide notice to clients and potentially others. Under Rule 1.4, a lawyer must notify current clients about a data breach. The Opinion concludes, in a quote from 1995 Opinion 95-398 in which the Committee discussed the unauthorized release of confidential information, that "[w]here the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b)."

The Opinion then discusses an attorney's obligation to former clients. It recommends that lawyers reach agreements with clients before the conclusion, or at the termination, of a relationship about how to handle client information in the lawyer's possession. The Committee also notes that lawyers must consider data privacy laws, common law duties, and contractual arrangements with former clients when determining how to deal with those former clients.

In conclusion, data breaches are serious events and occur at an ever-increasing frequency. Law firms that ignore their duty to be proactive to avoid breaches and hacks are particularly vulnerable not only to the legal implications of a breach, but also the ethical ones. ■

---

[1] *https://www.trendmicro.com/vinfo/us/security/definition/data-breach*

[2] *See my Fall 2017 Ethics column.*

Daniel J. Siegel, a member of the Board of The Philadelphia Lawyer, is the principal of the Law Offices of Daniel J. Siegel, which provides appellate, writing and trial preparation services to other attorneys, as well as ethical and disciplinary guidance. He can be reached at dan@danieljsiegel.com.