Attorneys' Ethical Obligation in the Event of a Data Breach

By Deirdre R. Wheatley-Liss

The age of data protection is upon us. Data breach after data breach have screamed from the headlines in recent years—50 million, 100 million, 330 million, 1 billion records breached. However, many attorneys seem to have the sense that all the data protection hoopla doesn't apply to them. Who would want to breach the security of the law firm? It's not like we are a bank. And we are attorneys—we have always had the obligation to hold our clients' information confidential. Confidentiality is nothing new to us.

The reality is that law firms are often juicier targets than big-name businesses. Our clients are big-name businesses, many of which have million-dollar budgets to throw toward cyber security and data protection. As attorneys, we have key information of those clients in our systems and rarely have the same cyber security resources. The question is not *if* a law firm will be subject to a cyber attack, but *when*.

While we are law firms, we are also businesses. We are not exempt from laws such as the New Jersey Identity Prevention Act, the California Consumer Protection Act, the New York SHIELD Act, HIPAA and myriad other federal and state data protection regulations that require specific activities to both prevent data breaches and provide notice when personal information has been compromised.

Besides the patchwork of legislation, the American Bar Association has issued Formal Opinion 483 "Lawyers' Obligations After an Electronic Data Breach or Cyberattack"[1] outlining our ethical obligations to clients if a data breach occurs. However, none of the state, federal or ethical obligations are in lieu of each other; instead, attorneys have an ongoing obligation under all of those frameworks to both protect personally identifiable information within its systems and notify employees, clients and government agencies in the event of a breach.

The touchstone of the opinion states: "[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 obligation under these Model Rules." Unfortunately for attorneys, the opinion does not create a specific framework of "reasonable steps." This article unpacks some of the key points of the opinion with practical recommendations for attorneys to meet their ethical obligations.

While we are law firms, we are also businesses. We are not exempt from laws such as the New Jersey Identity Prevention Act, the California Consumer Protection Act, the New York SHIELD Act, HIPAA and myriad other federal and state data protection regulations that require specific activities to both prevent data breaches and provide notice when personal information has been compromised.

Competency. Model Rule 1.1 requires that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In 2012, the ABA modified Comment [8] to Rule 1.1 to speak directly to technology: "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…*" (emphasis added).

To satisfy our ethical obligations of competency, the opinion identifies three areas where an attorney must take reasonable steps to address the probability of a data breach:

1. *Obligation to Monitor for a Data Breach*. This requires that "lawyers 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." From a practical perspective, law firms should engage in penetration testing at least annually to assess the robustness of their information security and take steps to improve that security as a result of the assessment. When engaging vendors, the contract should detail the vendor's requirements to protect client information, and create notification mechanisms if the vendor experiences a data breach.
2. *Stopping the Breach and Restoring Systems*. The opinion advises that "lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach." The "2019 Cost of a Data Breach Report" issued by IBM Security and the Ponemon Institute finds that having an incident response plan in place is

DEIRDRE R. WHEATLEY-LISS *is principal at Porzio, Bromberg, and Newman, P.C. and leader of the Cybersecurity and Data Privacy Team. Wheatley-Liss co-chairs the New Jersey State Bar Association Computer and Internet Law Committee.*

the single most cost-effective measure in addressing a data breach. An incident response plan should identify who will be the incident response team—including both internal stakeholders and outside experts, and what specific steps are to be taken to triage, investigate and notify the required parties of the breach. To be most effective, the law firm should hold semiannual "tabletop exercises" where an incident fact pattern is given to the incident response team to work through, and the response plan is modified to address any gaps that become apparent in dealing with a fact pattern.

3. *Determining What Occurred*. The opinion makes clear that "[a] competent attorney must make reasonable efforts to determine what occurred during the data breach." As a practical matter, most law firms do not have sufficiently skilled internal resources to determine how the breach occurred and exactly what data was exposed. The law firm should consider a forensic technology expert as part of the incident response team to lead the investigation and provide a report of the affected records and information. Only armed with this information is the attorney able to meet their legal and ethical obligations to notify clients and government agencies.

Confidentiality. Model Rule 1.6(a) requires that "[a] lawyer shall not reveal information relating to the representation of a client." In 2012, the ABA added an affirmative duty to the attorney in Rule 1.6(c) that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."

The actions to be taken by a small or solo practice versus a multi-national law firm to make "reasonable efforts" to protect the confidentiality of client information will differ, given their resources. Comment [18] to Rule 1.6(c) includes nonexclusive factors to guide lawyers in identifying if "reasonable efforts" are being made, including:

- the sensitivity of the information,
- likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing 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).

Some security measures are standard these days, and a lawyer would be hard-pressed to argue that they were taking reasonable efforts without them, including firewalls, robust passwords policies, two-factor authentication, written information security policies (that are reviewed and enforced), and limiting access based on business purposes. However, the specific information security measures of one law firm will differ from another based on the nature of the clients, the practice, and the resources available.

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals[2] recommends "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." As a practical matter, lawyers should annually assess their technology, ensure all technology is up to date (e.g. patching and investing in new software versions), and shift away from technology with known security vulnerabilities. Unless the law firm has a robust information security resource in-house, consider retaining an outside technology expert to perform this assessment.

Breach Notification. When a breach occurs, lawyers are subject to a variety of breach notification requirements. All 50 states have a breach notification laws to consumers and government agencies. Certain federal laws such as HIPAA, Graham-Leach-Bliley and FERPA require vendors with access to confidential information to report the breach of that information to the consumer-facing organization. A lawyer may have a contractual obligation with a client to provide notice of any breach, whether the client's information is

impacted or not. From a practical perspective, a comprehensive incident response plan will identify the law firm's breach notification requirements before an incident occurs.

The opinion concludes that "an obligation exists for lawyers to communicate with current clients about a data breach" based on Model Rule 1.4(b) which provides "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." While the opinion does not provide a format for the breach notification, the law firm can look to the breach notification statutes of the jurisdictions in which they practice for reasonable guidance on the information to be shared with the impacted clients.

Notably, the opinion does not assert a similar notice obligation for former clients, stating "the Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice." However, federal and state statutory breach obligation provisions are likely to require notice to a former client if their protected personal information, as defined under the statute, has been subject to a data breach.

The key takeaway is that to meet their ethical obligations, a lawyer must be able to demonstrate that concrete efforts have been taken to protect the client information in their care from the risks of cyber-attack, that systems are in place to identify when a data breach has taken place, that there is a process to minimize exposure to data breaches in evaluating technology, and when a gap is exposed, specific steps are taken to reduce that gap. From a practical perspective, most lawyers are not technology experts, and law firms should consider retaining outside consultants with expertise in cyber security and data privacy to guide them in meeting their legal and ethical obligations. ⚖

Endnotes

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018).
2. ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, 124 (2d. ed 2018).