Protect Your Firm from Collateral Damage

Understand Your Ethical Duties in the Event of a Data Breach

By Alyssa A. Johnson and Mollie T. Kugler

Seven years ago, former FBI Director Robert Mueller warned about the proliferation and ubiquity of cyber warfare: "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Robert Mueller, Director, FBI, Remarks at the 2012 RSA Cyber Security Conference (Mar. 1, 2012).

This principal is even truer now, with no changes in the foreseeable future. We have seen that industries are vulnerable, and most especially the legal industry. Law firms are the secret-keepers for wide-ranging clients; they are natural targets of cyberattacks. Law firms should understand their cyber liability exposure, especially given the "sharp increase" in the number and cost of cyberattacks in 2018. Najiyya Budaly, *Cyberattack Reports Surge to 61 percent in 2018, Insurer Reveals*, Law360 (Apr. 23, 2019).

Growing concerns surrounding data vulnerabilities affect lawyers' duties under the American Bar Association (ABA) Model Rules of Professional Conduct or the attorneys' states' ethics rules. Lawyers have a duty to keep up with "changes in the law and its practice." Model Rules of Prof'l Conduct R. 1.1 cmt. 8. Further, recent amendments to the Model Rules and their comments demonstrate the ABA's increasing concern about the ethical implications of a data breach. Comment 8 to Model Rule 1.1 indicates that a lawyer has a duty to stay up-to-date on "the benefits and risks associated with… technology." *Id*. Not only should lawyers know how to use technology to handle client matters efficiently, they should also know how technology can subject a client's information to attack.

Model Rule 1.6, which details a lawyer's duty to keep client confidences, is also implicated in the event of a data breach. Model Rules of Prof'l Conduct R. 1.6. Lawyers are required to take reasonable steps to "prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Model Rules of Prof'l Conduct R. 1.6(c). The level of effort that qualifies as "reasonable" under this standard varies, especially as lawyers become more aware of the specific threats their clients face. Client information is especially attractive to hackers (particularly large business or government entity clients), so it is important that lawyers and law firms analyze the data protection measures they currently take and evaluate other protection or mitigation resources that are available, including cyber insurance.

Within the last year, the ABA issued Formal Opinion 483, which makes clear that "when 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." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018). What most people don't think about until it happens is how costly a data breach can be for a lawyer or a firm. Formal Opinion 483 suggests having an "incident response plan" for a data breach, which could include calling the insurance company, hiring a data breach lawyer or a digital forensics company, or both, and performing further recovery and repair efforts. Putting an incident response plan in motion may potentially take away billable hours from those who would have to manage the mitigation efforts after a breach. In short, an emergency breach-response plan will have expenses. Not to mention, if the breach is serious, and you are required under the ethics rules to notify your clients, it may also cost you your clients.

This is why law firms might consider whether having a cyber insurance policy could help meet ethical duties after a breach, which will grow increasingly significant as hackers target law firms' wealth of confidential client information. In a 2018 poll conducted by the ABA, almost one quarter of law firms responded that they had

■ Alyssa A. Johnson is an associate in Hinshaw & Culbertson LLP's Milwaukee office. She represents a wide range of professionals in liability matters. Among others, Ms. Johnson defends lawyers and law firms in legal malpractice cases. She serves as the DRI Lawyers' Professionalism and Ethics Committee Young Lawyer Liaison. Mollie T. Kugler is a partner in Hinshaw's Milwaukee office. She focuses her practice on insurance services, with an emphasis on insurance coverage issues. She also litigates many types of insurance defense and other civil and commercial cases, including professional liability matters. She is a DRI member.
The authors wish to acknowledge the assistance of Claudia Verba, a law clerk at Hinshaw & Culbertson LLP, in drafting this article.

experienced a data breach. David G. Ries, 2018 Cybersecurity Tech Report, ABA Law Practice Div. (Jan. 28, 2019). The percentage of firms experiencing a breach increased with the size of the firm. *Id*. In an environment in which legal malpractice payouts are surging, it is important for lawyers to understand the ethical implications of technology and to consider cyber insurance's role in preventing and mitigating ethical problems in the wake of a data breach.

Also be aware that general and lawyers' professional liability (LPL) policies may not adequately cover cyber losses. To put it simply, general liability policies typically cover losses from bodily injury, property damage, and personal and advertising injury. And many general liability policies contain some sort of cyber exclusion. On the other hand, LPL policies generally cover claims arising out of the provision of professional services. Most commonly, LPL coverage protects against malpractice, human error, acts of omission, acts deemed wrongful, and breaches of fiduciary duty or contract. But an LPL policy may not cover claims for fines and penalties, losses incurred by threats of a data breach, and emergency breach-response expenses. These losses become especially important (and costly) when a lawyer's ethical duties to inform clients and protect client confidences are concerned. Cyber liability insurance may be purchased to fill this gap.

Nevertheless, few attorneys recognize this exposure. According to the 2018 ABA survey, mentioned above, only 34 percent of responding lawyers had cyber coverage, with the largest proportion attributable to mid-size firms, which was up 7 percent from the previous year. Ries, *supra*. Firms of 500 attorneys or more reported carrying cyber insurance at a smaller percentage than any other size firm, including solos. *Id*.

Lawyers and law firms are charged with the almost Herculean obligation of protecting their clients' sensitive and confidential data. Cyber breaches will happen. As Mr. Mueller warned, it is not a matter of if, but when. Therefore, as part of your duty under your state's ethics rules, you might consider Formal Opinion 483, creating an incident response plan, and investigating whether cyber insurance is right for your firm. FD