CHAPTER 1

OVERVIEW OF CYBERSECURITY AND THE LAW FIRM

Daniel Garrie
“People have entrusted us with their most personal information. . . . We owe them nothing less than the best protections that we can possibly provide by harnessing the technology at our disposal. We must get this right. History has shown us that sacrificing our right to privacy can have dire consequences.”

—Tim Cook,
CEO of Apple, at the 2015 White House Cybersecurity Summit

1.1 Introduction: Law Firm Vulnerability to Cyber Breaches

No one is immune to a cybersecurity incident. Every industry and business sector—including the legal profession—is a target for hackers and cyber criminals. Law firms are especially appealing targets, given that, in the course of their business, they acquire highly sensitive and confidential information from clients. According to a report from cybersecurity firm Mandiant, at least 80% of the leading U.S. law firms already have seen their security compromised via a cyber breach.\(^1\) Even this is likely to be an underestimate, as firms are often unaware they have been breached.\(^2\)

Law firms thus face intense pressure to improve their cybersecurity. Clients are increasingly requesting that their lawyers be allowed to work remotely (often on personal, possibly unsecured devices), while at the same time law firms are being required to verify the integrity and security of their networks and information systems.\(^3\) Large banks are pressing outside law firms to demonstrate that they are using state-of-the-art technology to secure the information the banks are entrusting to the firms.\(^4\) Some financial institutions are asking law firms to fill out lengthy questionnaires detailing their cybersecurity measures, while others are doing on-site inspections.\(^5\) In some cases, banks and companies are threatening to withhold legal work from law firms that hesitate to comply with increased scrutiny, or requesting that firms add insurance coverage for data breaches to their malpractice policies.\(^6\)

---

1 Stuart Poole-Robb, *Law Firms Are a Hacker’s “Treasure Trove,”* ITProPortal, http://www.itproportal.com/2015/03/30/law-firms-hackers-treasure-trove/#ixzz3nFgP2mm0.
2 Id.
5 Id.
6 Id.
Moreover, regulators and government agencies are criticizing law firms as a group for the weak protection afforded to the personal data and client information they collect and store. As early as 2009, the FBI cited the legal industry as a group that could easily succumb to cyber incidents. In 2011, the FBI met with major U.S. law firms to discuss their cyber preparedness, and followed up with educational programs intended to help firms implement more secure systems.

Thus, at this point, cyber threats should feature prominently on most law firms’ threat radar, yet there is an ominous statistical dichotomy in the legal industry: Most law firms view cybersecurity as a major threat to their organizations, yet many of them say they are unprepared for a significant cyberattack. Marsh’s 2014 Global Law Firm Cyber Survey returned the following results regarding law firm cyber security:

- 79% of respondents viewed cyber/privacy security as one of the top 10 threats in their overall risk strategy.
- 72% said that their firms had not assessed and scaled the cost of a data breach based on the information they retain.
- 51% said that their law firms either had not taken measures to insure against cyber threats (41%), or did not know if their firms had taken such measures (10%).
- 62% had not calculated the effective revenue lost or extra expenses incurred following a cyberattack.

As shown by these results, the majority of firms surveyed had not taken into account what kind of financial impact their organization could experience following a cyber incident. More than 60% said their firms had not calculated the effective revenue that could be lost following a cyberattack. Even more (72%) said their firms had not assessed how much a data breach could cost them based on the kind of information the firm retains.

The preceding statistics demonstrate that the legal profession generally lags behind other industries when it comes to preparing for and responding to cyber threats. Although a limited number of law firms have developed satisfactory cybersecurity programs, many law firm programs lack essential elements that are common in cybersecurity programs of companies in other industries. For example, some law firms now have a chief information officer (CIO) and/or chief information security officer (CISO), as is common with companies in other sectors, but it
is hardly the norm; many law firms still lack any kind of substantial cybersecurity program or dedicated cybersecurity personnel.\textsuperscript{13}

Effective cybersecurity programs involve privacy and data security training. The legal industry has been slow to adopt training concerning data protection.\textsuperscript{14} One of the difficulties in implementing cybersecurity training at law firms is that lawyer time is so valuable: Time spent training is time not spent on billables.\textsuperscript{15} Nevertheless, training is an essential component of good privacy and security protection.\textsuperscript{16} According to information technology (IT) executives quoted in a recent ABA Journal article, untrained lawyers and office personnel constitute the biggest weakness in a law firm’s cyber defense.\textsuperscript{17}

\section*{1.2 Potential Consequences and Liability for Law Firms from a Data Breach}

A cybersecurity incident can cause serious trouble for a law firm, including lawsuits, ethical violations, negative publicity, reputational damage, regulatory fines, and/or disgruntled clients. On top of that, there is the cost of any necessary forensic investigation and breach notification, as well as the potentially tremendous amount of valuable attorney time lost. This section surveys some potential consequences and sources of liability when a law firm is the victim of a data breach.

\subsection*{1.2.1 Ethical Violations May Result from a Cyber Breach}

\subsubsection*{1.2.a Privilege and Confidentiality}

Inadequate data security or protection of privacy arguably constitutes a failure to fulfill a law firm’s duty of confidentiality. Under Rule 1.6 of the ABA Model Rules of Professional Conduct, “a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.”\textsuperscript{18} Lawyers must “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”\textsuperscript{19}

\begin{thebibliography}{99}
\bibitem{13} Id.
\bibitem{14} Id.
\bibitem{15} Id.
\bibitem{16} Id.
\bibitem{17} Id.
\bibitem{19} \textit{Model Rules of Prof’l Conduct} R. 1.6 (Am. Bar Ass’n 2015) (hereafter “Rule”).
\bibitem{20} Id., Rule 1.6(c).
\end{thebibliography}
Rule 1.6(c), however, does not address whether attorneys have to tell their clients about a data breach. The law governing lawyers suggests that lawyers must self-report a breach in which client data is exposed if the breach results from the lawyers’ negligence. Professor Benjamin Cooper, in discussing Rule 1.6, Rule 1.4 (communications with the client), and the fiduciary law governing the lawyer–client relationship, states: “If the lawyer’s conduct of the matter gives the client a substantial malpractice claim against the lawyer, the lawyer must disclose that to the client.”

Indeed, the ABA Model Rule is written broadly enough that it likely requires disclosure of a breach even if the lawyer did not personally act negligently in exposing the data. Further, various doctrines of secondary liability mean attorneys can be held liable for malpractice due to negligent defects in information security systems caused by subordinate employees. Thus, even if an IT employee at a law firm negligently caused or allowed a security breach through which a client was harmed, the client could have a viable malpractice claim against the lawyers and firm responsible for managing that IT employee, such that the lawyers likely would be required to disclose the breach to the client.

In this regard, Model Rule 5.3, governing law firm responsibilities related to nonlawyers, suggests that attorneys may be liable for ethical violations by their subordinate IT personnel:

A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

1. the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
2. the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Ignorance of IT personnel’s negligent actions likely will not be a successful defense against a claim for failing to disclose a law firm data breach, given the requirements of Rule 1.6 discussed earlier, as well as the further requirement of Rule 5.3 that “a lawyer having direct supervisory authority over the non-lawyer...
shall make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer.”

Examining these two rules in conjunction, it is clear that lawyers in a managerial position at a law firm must oversee IT personnel action regarding client data, and make sure those actions are compatible with the professional obligations of the lawyer, to avoid possible ethics violations. As Professor Cooper has observed, “firms have a duty under Rules 1.1 and 1.6 to effectively protect their clients’ information. If a firm is negligent in carrying out that duty because it has been lax with its security, and that resulted in client files being disclosed, it is potentially a problem.” Even if a firm has a very good security system, he states, “the attorney absolutely has a duty to inform clients under 1.4 that their confidential information has been compromised.”

Accordingly, a strong security program may help shield a firm from an ethics violation caused by not appropriately protecting client data, and it may help them defend against a negligence charge, but it has no impact on an attorney’s ethical requirement to inform clients of security incidents. A good security program does, however, reduce the likelihood that such a painful conversation will have to take place.

1.2.b Competence

Inadequate cybersecurity systems can also raise competence issues. Model Rule 1.1 requires that a “lawyer shall provide competent representation to a client.” “Competent representation” means “the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” The ABA recently amended Comment 8 to Model Rule 1.1 to emphasize that “a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology” (added language indicated by italics).

Furthermore, the ABA published Resolution 109 in 2015, calling for firms to “develop, implement, and maintain an appropriate cybersecurity program.” The ABA’s adopted resolution encourages firms to “create cybersecurity programs that are tailored to the nature and scope of the [firm] and the information to be protected.” The resolution also encourages firms to regularly conduct threat assessments, “create controls based upon these assessments, create response plans for possible cyber-attacks, and establish relationships and share information with...
external organizations, where appropriate, as a method of addressing the problem of cyber-attacks.”

Based on Comment 8 and Resolution 109, adequate cybersecurity protection now appears to be a material part of the “skill, thoroughness and preparation” expected from competent legal counsel. Thus, in the event of a data breach, law firms may face liability and sanction for breach of the ethical duty of competence, in addition to any other ethical violations or legal claims against the law firm related to the disclosure of confidential information.

1.2.2 Lawsuits Brought by Clients

Law firms that are victims of cyber breaches can be held liable for a number of common law claims brought by clients whose data was exposed. Possible causes of action include malpractice, negligence, breach of fiduciary duty, and fraud. Although case law regarding law firm data breaches is sparse, attorneys now may have a greater duty of care with respect to information security than in the past, in light of the abundance of recent data breaches and the ABA’s recent comments and resolutions.

Since the late 19th century, attorneys have been held to what courts have described as an “ordinary” standard of care in representing their clients. In other words, as it is frequently expressed, an attorney must exercise that degree of care, skill, and diligence which is commonly possessed and exercised by attorneys in practice in the jurisdiction. As the recent comments to the ABA Model Rules and Resolution 109 suggest, “ordinary care” for attorneys now seems to include some degree of care with respect to information security. Attorneys should proceed accordingly.

Negligence claims arising from data breaches in other sectors may shed some light on what “ordinary care” means for attorneys with respect to information security in this age of increased cyber threats. Following the highly publicized 2014 Target data breach, customers and financial institutions affected by the breach brought a number of lawsuits against Target, primarily asserting claims of general negligence in Target’s implementation and maintenance of its information security systems. The District Court of Minnesota’s order identified three distinct duties

---

36 Id.
37 To establish a cause of action for legal malpractice, a plaintiff must demonstrate that its attorney was negligent in representation and that such negligence proximately caused actual and ascertainable damages (see Bixby v. Somerville, 62 A.D.3d 1137, 880 N.Y.S.2d 205 [3d Dep't. 2009]; see also Comment 8 to Rule 1.1.
38 For example, in Babbitt v. Bumpus, 41 N.W. 417 (Mich. 1889), the Supreme Court of Michigan held that attorneys must be held to a standard of “ordinary care and diligence”; in Hill v. Mynatt, 59 S.W. 163 (Tenn. 1900), the Court of Chancery Appeals of Tennessee held that an attorney should be liable for injuries caused when the attorney fails to exercise “reasonable diligence” or ordinary care.
40 A court may conclude that a negligence suit is appropriate where a business failed to take reasonable steps—as defined by statutes, regulations, industry practices or even retroactively applied standards determined by a judge—to secure its network, resulting in a data breach involving client data. See Sulkowski, supra note 24.
that Target (and now other companies) have in the data breach context: (1) a duty to safeguard its and its business associates’ customers’ data; (2) a duty not to disable security features that would prevent a data breach; and (3) a duty to heed the warning signs of an attack and respond appropriately. Though nothing is set in stone as of this writing, since the Target case is ongoing, the initial phases of the litigation indicate that the court is willing to consider recognizing what some see as a new species of tort: negligent data security.

To date, data breach victims have been only marginally successful in breach lawsuits, but the field is developing rapidly. Recent filings have sought to broaden plaintiffs’ arsenal of weapons by alleging negligent misrepresentation and applying products liability theories. For example, class action plaintiffs suing Ashley Madison claimed that its duty of care stems from the availability of commercially reasonable safeguards against breaches. These plaintiffs claimed that Ashley Madison failed to follow industry standards, citing the Data Security Standards for the payment card industry to demonstrate the kind of steps that plaintiffs assert would have been sufficient to protect data. The theory behind this claim is that, had Ashley Madison adhered to industry standards, the breach could have been avoided. This approach is much closer to a products liability claim, alleging that a defendant’s failure to take commercially reasonable and viable steps to protect consumers led to harm, than to a general negligence claim.

Should the “commercially reasonable options” approach prevail, the consequences would be substantial; under this analysis, the burden shifts to the defendant, who must demonstrate that it kept up with, and abided by, industry standards on data security. Such a standard would put significant pressure on many businesses to identify applicable industry standards and raise their information security to that level. However, this rule could also allow defendants in industries with low information security standards to get claims dismissed on the grounds that their security—however poor it is—meets those industry standards.

44 Under the Rule 12(b)(6) paradigm, data breach plaintiffs face difficulties overcoming defenses such as lack of standing and failure to demonstrate a cognizable injury. In 2011, a class of data breach victims in Whitaker et al. v. Health Net of Cal., Inc. filed suit for a data breach that occurred when IBM lost nine servers containing 800,000 Health Net customers’ confidential information. The plaintiffs contended that they had standing to sue because of the threat of loss. The judge rejected plaintiffs’ argument, and dismissed the lawsuit because “the threat plaintiffs allege [was] wholly conjectural and hypothetical.” See The Typical Data Breach Lawsuit and How to Protect Your Company, InsideCounsel (Oct. 2014), http://www.mvalaw.com/news-publications-347.html.
45 In the wake of the Ashley Madison breach, in which self-proclaimed hacktivists released the personal, financial, and social information of about 30 million users of the website, various class actions have been filed against Ashley Madison alleging more than $500 million in damages. See Kim Zetter, Ashley Madison Hit with $500 Million in Lawsuits (Aug. 23, 2015, 3:30 PM), http://www.wired.com/2015/08/ashley-madison-hit-500-million-lawsuits/.
47 Stein, supra note 43.
48 Id.
49 Id.
At the time of this writing, the Target and Ashley Madison lawsuits are ongoing, and there remains significant uncertainty on this issue. In opposition to this new type of tort, a Pennsylvania trial court recently dismissed a class action lawsuit brought on behalf of more than 62,000 employees and former employees of the University of Pittsburgh Medical Center (UPMC), whose confidential personal identifying information was stolen from UPMC’s computer system.\(^{50}\) The court refused to find “that the courts should impose a new affirmative duty of care that would allow data breach actions to recover damages recognized in common law negligence actions.”\(^{51}\) Moreover, the UMPC court not only found that there are no generally accepted reasonable care standards concerning data protection obligations, but also held that the use of “‘expert’ testimony and jury findings” is not a “viable method for resolving the difficult issue of the minimum requirements of care that should be imposed in data breach litigation, assuming that any minimum requirements should be imposed.”\(^{52}\)

Although the Target, Ashley Madison, and UPMC lawsuits are not directly related to the legal profession, their outcomes could significantly impact the standard of care expected of law firms with respect to information security. These decisions are likely to be invoked soon, as it is only a matter of time before some court is faced with a precedent-setting legal malpractice claim involving a data breach.

A 2014 study by insurance broker Ames & Gough found that half of the leading legal malpractice insurers surveyed have had a lawyers’ professional liability insurance claim arising from a cyber or network security event.\(^{53}\) Of the insurers with these claims, the majority traced the breach to a lost or stolen laptop.\(^{54}\) For the remainder, a combination of employee error, hackers, and disgruntled employees led to a breach.\(^{55}\) These security breach claims can be extremely costly, and may not always be covered by the traditional professional liability policies held by law firms. In the face of all the uncertainty concerning limits of liability for data breaches, and the potentially massive dollar amounts involved, client lawsuits pose a significant risk to law firms that have inadequate information security.

### 1.2.3 Clients Can Be Liable for Their Law Firm’s Inadequate Security

When a breach or incident at a law firm involves a client’s data, the client may also be liable to third parties affected by the breach. This client liability may be via vicarious liability, or via direct liability for failure to exercise due diligence in

---


\(^{51}\) Dittman, supra note 50.

\(^{52}\) Id.


\(^{54}\) Id.

\(^{55}\) Id.