New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 111
WEDNESDAY, DECEMBER 10, 2014

Outside Counsel

Cybersecurity: Business Imperative for Law Firms

BY KENNETH N. RASHBAUM,
JASON M. TENENBAUM
AND LIBERTY MCATEER

Banks and other financial institutions are auditing their law firms for cybersecurity safeguards. Hospitals and hospital systems have, as required by federal law, been demanding and examining law firm policies and procedures for compliance with security provisions under the Health Insurance Portability and Accountability Act (HIPAA) for several years. There is a basis for concern: A number of law firms, including some of the largest firms in the United States and Canada, have been hacked in the past two years, and a firm in Virginia was forced to cease operations for a time following a breach of three gigabytes of client data.[1]

It is not difficult, then, as the late Rod Serling, host of the long-running television show "The Twilight Zone" asked viewers at the beginning of each episode, to "imagine, if you will" the following scene:

A law firm's managing partner answers her phone on the first ring. It is 3 p.m. on the Wednesday before Thanksgiving and her husband wants to know when she'll be home to help him with dinner preparations for the 18 people expected to arrive within the next 24 hours. As she gathers her things and prepares to leave, her computer's email notification alarm chimes twice. She clicks on the first email. It's from the chief technical officer of the bank that is the firm's biggest client.

He is writing to advise that, due to increased cybersecurity scrutiny from New York State's Department of Finance and the Securities and Exchange Commission (SEC), he will be auditing the information security protocols of all of the bank's law firms. He needs access to the firm's network and copies of all information security policies and procedures, along with materials used to train the attorneys and staff—current, of course—by the following Monday morning. The managing partner swallows hard: There are policies, but they haven't been updated since BlackBerrys were the only smartphone allowed for firm business, five years ago. She clicks on the second email. This one is from the chief information officer of a 100-hospital system that shortlisted the firm for its national litigation counsel. His email says that the board has decided to review the information management policies of all the finalists. He apologizes but, he writes, after a recent incident in which another hospital system law firm inadvertently disclosed the information of 400 patients to Google, the board has decided not to award an engagement to any firm unless it can show that patient information will be adequately protected.

> Stories of breaches of cybersecurity are viral, and the virus has spread to law firms.

The managing partner picks up the phone, tells her husband she'll be working through the night and will also be leaving for the office right after the Thanksgiving meal, and offers that maybe one of the kids could help him cook.

Third-Party Vendors

Truth can be stranger than fiction, and life frequently follows art. Stories of breaches of cybersecurity are viral, and the virus has spread to law firms. While banks have been auditing law firms' information safeguards for some time on a sporadic basis, review initiatives have gained significant urgency as a result of a letter sent to New York financial institution chief executives, general counsel and chief information officers by New York State Department of Financial Services Superintendent Benjamin Lawsky on Oct. 21, 2014. Lawsky's letter required banks to provide information about the cybersecurity protections employed by their "third-party service providers." Lawsky stated the rationale of the inquiry in the first paragraph:

> [i]t is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors…It is important that financial institutions are able to identify, monitor and mitigate any security risks posed by third-party relationships, *including but not limited to law firms* and accounting firms.[2]

The letter also noted that the department is "considering a requirement that financial institutions obtain representations and warranties from third-party vendors with respect to the third parties' cyber security standards and policies." This requirement, of course, would obligate law firms to maintain policies and procedures on information security, conduct periodic evaluations of their information systems safeguards and document training on cybersecurity safeguards, much like hospitals and many banks currently require of their work forces.

It would, however, also require law firms to warrant to financial services clients, and perhaps the state, that their information systems and internal procedures are compliant with relevant security rules and regulations, creating the risk of a professional liability claim if there were a breach. One must question how many law firms representing financial services clients currently perform such audits and reviews and would be willing to make the representations Lawsky envisions.

In the event of a breach by the firm the risk would be considerable for the client, too, because Lawsky's letter asked the organizations to respond by Nov. 4 to five inquiries including, as question one, "any due diligence processes used to evaluate the adequacy of information security practices of third-party providers."

The danger would then rebound to the firm. If the due diligence processes of the clients were called into question, through proceedings by the Department of Financial Services, with regard to the hiring of law firms, it is a good bet that the clients would seek to implicate the law firms whose lax security practices were not discovered in vetting by the client. That spiral of recrimination could be a law firm's worst nightmare.

KENNETH N. RASHBAUM *is a partner at Barton and an adjunct professor at the Maurice A. Deane School of Law at Hofstra University.* JASON M. TENENBAUM *and* LIBERTY MCATEER *are associates at Barton.*

Regulatory Requirements

Additional cybersecurity standards required of law firms arise from myriad federal regulations. For example, following high-profile data breaches at such public companies as Target, Home Depot, JP Morgan Chase and CitiGroup, the Securities and Exchange Commission (SEC) has become more aggressive in recent months in enforcing its regulations on information security. On April 15, 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued its "OCIE Cyber Security Initiative," in which it indicated that it would be conducting examinations of registered broker-dealers and registered investment advisers, "focusing on areas related to cybersecurity."[3]

The document contained an appendix with a list of sample audit questions. The section of that appendix titled "Risks Associated with Vendors and Other Third Parties" included questions regarding whether the audited organization "conducts cyber security risk assessments of vendors and business partners," the latter term including law firms, and "whether the organization regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors and business partners."

In addition, lawyers who provide advice to clients that are public companies where the advice may be filed with or submitted to the SEC (such as an opinion on the potential financial exposure of litigation) are considered to be practicing before the commission, and subject to certain SEC regulations. A breach by a law firm, then, may subject the firm to an investigation by the SEC.[4]

Protected Health Information

Law firms that access individually identifiable health information (protected health information, or PHI) in the course of their representation of health care providers or health insurance plans (considered "business associates" under HIPAA) are required by the HIPAA Final Omnibus Rule[5] to prepare and implement safeguards for the PHI they use, disclose and store. The HIPAA security rule requires such law firms to employ administrative (i.e., policies and procedures), technical (i.e., access controls and authorization controls, malware protection and encryption), and physical (i.e., secured enclosures for equipment) safeguards to ensure and protect the confidentiality of PHI.

The security rule also requires training of the firm's work force on security protocols, and documentation of that training. In addition, HIPAA's privacy and security rules mandate that these law firms sign a business associate agreement with their provider and health plan clients, in which the firm agrees to maintain PHI in accordance with the requirements of the HIPAA rules. These mandates have teeth. The omnibus rule provides for direct jurisdiction over law firms, as business associates, by the U.S. Department of Health and Human Services.[6]

If there is a breach of PHI by a law firm, then, the U.S. government may commence proceedings for civil monetary penalties against the firm. In addition, where a law firm fails to adequately protect information, it can face a breach of contract action by the client—not to mention probable loss of the client's business.

Law firms that access individually identifiable health information (protected health information, or PHI) in the course of their representation of health care providers or health insurance plans are required by the HIPAA Final Omnibus Rule to prepare and implement safeguards for the PHI they use, disclose and store.

Ethical Obligations

Perhaps of equal or even greater significance, lawyers are also subject to ethical requirements to safeguard client information, regardless of the industries of their clients, including New York's Rules of Professional Conduct.[7] In 2014, when most client and law firm documents are in electronic format, this is more difficult than it may first appear. Electronic information differs fundamentally from paper documents in two ways: there is more of it, and it is more difficult to inventory because it may reside in many places (not all of them secure), such as laptops, smartphones, tablets, USB drives, the cloud, etc. The regulatory and business imperatives of law firm cybersecurity cannot be separated, practically, from the ethics rules with regard to confidentiality.

The reputed technophobia of many lawyers notwithstanding, there is also a clear ethical obligation to be aware of cybersecurity obligations and risks and lawyers must learn and implement the relevant technology. In 2012, the ABA amended Model 1.1 on the duty of competent representation with Comment 8, requiring 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."[8]

Federal and state case law has also demonstrated that there are obligations on law firms to prevent inadvertent disclosures of electronic communications that can imperil privilege.[9] Finally, understanding technology, including cybersecurity, is a requirement of engaging in electronic discovery.[10]

Cybersecurity is a regulatory requirement, an ethical obligation and business imperative. In today's business climate, few multinational corporations will retain law firms that cannot control and safeguard its flow of critical information. The paper era has given way to the digital age in business.

With developments such as the requirements upon lawyers in the HIPAA omnibus rule and Superintendent Lawsky's letter requiring financial institutions to provide information about their law firms' information safeguards, the legal, ethical and business obligations come together. The question for law firms is not whether to become cybersecurity literate, but how quickly they can do so, in-house or with the assistance of outside experts and counsel, to the satisfaction of their clients and the clients' regulators.

1 Sam Biddle, "Anonymous Leaks Marine Corps Massacre Case" (Updated), GIZMODO, Feb. 3, 2012, http://gizmodo.com/5882057/anonymous-leaks-marine-corps-massacre-case; Jett Hanna, "The Risk of Data Breaches in Law Firms," TLIE Newsletter (Texas Lawyers' Insurance Exchange, Austin, Texas), November 2013, available at http://www.tlie.org/newsletter/articles/view/200; Andrew Conte, "Unprepared Law Firms Vulnerable to Hackers," Pittsburgh Tribune, Sept. 13, 2014, available at http://triblive.com/news/allegheny/6721544-74/law-firms-information#axzz3Ji9kuMrl.

2. Letter from Benjamin M. Lawsky, Superintendent, N.Y. State Dep't Fin. Servs. to Chief Executive, General Counsel and Chief Information Officer (Oct. 21, 2014) (emphasis added).

3. SEC National Exam Program Risk Alert, OCIE Cybersecurity Initiative, April 15, 2014, available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%26+Appendix+-+4.15.14.pdf

4. See Implementation of Standards of Professional Conduct for Attorneys (Final Rule), Securities Act Release No. 33-8185, Exchange Act Release No. 34-47276 (Jan. 29, 2003), available at http://www.sec.gov/rules/final/33-8185.htm.

5. Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (amending 45 C.F.R. Parts 160 and 164).

6. See id.

7. See New York Rules of Prof'l Conduct R. 1.15; See also N.Y.C. Bar Ass'n, Comm. On Small Law Firms, The Cloud And The Small Law Firm: Business, Ethics And Privilege Considerations 11 n.13 (2013), available at http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf (citing New York Rules of Prof'l Conduct R.1.6 cmt. 17).

8. Model Code Of Prof'l Conduct R. 1.1 cmt. 8 (2012) (emphasis added); N.Y. State Bar Assoc. Comm. on Prof'l Ethics, Opinion No. 842 (2010) ("The same duty to stay current with the technological advances applies to a lawyer's contemplated use of an online data storage system.").

9. *U.S. v. Finazzo*, No. 10-CR-457 (RRM) (RML), 2013 WL 619572 (E.D.N.Y. Feb. 19, 2013) (holding that the lawyer waived privilege by sending an email to his client on an accessed and monitored network); see *Scott v. Beth Israel Med. Ctr.*, 17 Misc.3d 934, 847 N.Y.S.2d 436 (S. Ct. N.Y. 2007) (holding that the client waived privilege by sending his attorney an email over a network he knew to be accessed and monitored by his employer, a potentially adverse party).

10. *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("…counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture."); see also *Voom v. Echostar,* 93 A.D.3d 33 (1st Dept. 2012) (adopting the Zubulake standards).