As published in the New York Law Journal – SPECIAL REPORT, March 6, 2017

Cybersecurity for Law Firms: Business Imperatives Update 2017

By

Kenneth N. Rashbaum, Esq.[1]

The cyberattacks on the Democratic National Committee and the breaches at Yahoo have brought cybersecurity concerns into sharp focus, and law firm clients are taking a new look at how firms safeguard client information. Those who would attack law firms for client or firm information have found new and more efficient ways to invade firms' information systems. Clients in highly regulated areas are increasingly auditing law firms to assess the strength of the firms' information safeguards and have pulled work from or denied work to firms that haven't met applicable cybersecurity regulation standards, or the client's vendor management guidelines (yes, they still consider lawyers "vendors"). On March 1, 2017, the New York State Department of Financial Services cybersecurity regulations (23 NYCRR 500 *et. seq.,* (Dec. 28, 2016). will impose even greater information safeguard regulations on lawyers through the regulations' requirement for due diligence into the security infrastructure of firms that access Nonpublic Information of their Covered Entity Clients. To put a fine point on it, those firms that can meet the regulatory and client expectations for cybersecurity will get or retain the business, and those who don't, won't.

And these are just the business considerations. Law firms are increasingly subject to regulatory proceedings, professional liability claims and other litigation if they fail to adequately protect client or firm information. In December, 2014 we wrote about the business, ethical and legal challenges faced by law firms in their role as stewards of client electronic information[2]. Events such as the attacks on the law firms Weil Gotshal & Manges LLP LLP and Cravath, Swaine & Moore[3] and the attack on the "Panama Papers" law firm Mossack Fonseca[4] have placed the issue of law firm cybersecurity squarely in the eye of the public but also the eyes of state bar associations with regard to ethics opinions and attorney disciplinary rules and regulators in

[1] Kenneth N. Rashbaum is a partner at Barton LLP where he heads the Privacy and Cybersecurity Practice Group.
[2] Rashbaum, Kenneth N., Tenenbaum, Jason M. and McAteeer, Liberty, "Cybersecurity: Business Imperatives for Law Firms," New York Law Journal December 10, 2014
[3] Masters, Brooke, "Lawyers and Accountants are Prime Targets for Cyber Attacks," *Financial Times* December 30, 2016, available at https://www.ft.com/content/f52f6fee-ccf4-11e6-864f-20dcb35cede2?ftcamp=published_links%2Frss%2Fcompanies_technology%2Ffeed%2F%2Fproduct (last visited January 6, 2017)
[4] Bilton, Richard, "Panama Papers" Mossack Fonsecca Leak Reveals Elite's Tax Havens," BBC News April 4, 2016, available at http://www.bbc.com/news/world-35918844 (last visited January 6, 2017)

financial services and healthcare. In this update to our December 2014 article, we explore new threats to law firms from increased regulatory scrutiny and risk exposure (at the federal and state levels), professional liability litigation stemming from data breaches by the firm or its third-party vendors and inadvertent disclosure of protected and privileged information. Following the maxim that it's better to light a candle than to curse the darkness, we will also suggest practices for law firms to mitigate these risks.

New York Law Firms in the Regulatory Crosshairs

The New York Department of Financial Service supervises banks, insurers, lenders, holding companies, investment companies and service contract providers (including technical services contract providers), among other financial services entities (http://www.dfs.ny.gov/about/whowesupervise.htm. Last visited January 6, 2017). Its Cybersecurity Regulations will impact law firms in that the organizations covered by these regulations ("Covered Entities") must implement a Cybersecurity Policy that comprises "vendor and Third Party Service Provider Management" (23 NYCRR 500.03). Law firms are Third Party Service Providers in that they "maintain, process or (are) otherwise permitted to access Nonpublic Information" (23 NYCRR 500.01(n)). This means, in essence that Covered Entities must show that they have assessed the information safeguards of their law firms. Banks will continue to audit law firms on cybersecurity, and other Covered Entity clients will do so as well.

The Regulations also require that agreements with law firms contain representations that the firm has cybersecurity policies and procedures regarding access to and encryption of Nonpublic Information and notification to the Covered Entity in the event of a Cybersecurity Event (defined as a successful *or attempted* attempt "to gain access to Nonpublic Information or "disrupt or misuse an Information System") (23 NYCRR 500.01(d)(g); 500.11(b). This will entail some heavy lifting in revision of law firm protocols and in negotiation of engagement letters.

Law firms who work with financial services or healthcare clients face regulatory risks on other fronts. In November, 2016 FINRA settled a penalty proceeding with Lincoln Financial Securities for $650,000 stemming from a breach by Lincoln's cloud services provider. Among the grounds for the penalty were findings that Lincoln did not include a representation of security practices in its service level agreement with its cloud services provider and did not monitor its compliance with security metrics.[5] The FINRA rules cited in this proceeding would also apply to a breach by a broker-dealer's law firm where the broker-dealer didn't get security representations from its law firm or failed to monitor the firm's security practices.

The Office of Civil Rights ("OCR") to the U.S. Department of Health and Human Services has also been active in enforcing HIPAA provisions regarding third-parties. Attorneys, as HIPAA

[5] Financial Industry Regulatory Authority Letter of Acceptance, Waiver and Consent No.: 2013035036601, Pubic Document No.: 66846, October 21, 2016, available at http://disciplinaryactions.finra.org/Search/ViewDocument/66846 (last visited January 6, 2017.

Business Associates, are directly covered by HIPAA are subject to penalties for violation of HIPAA Rules.[6] In July 2016, OCR settled a penalty proceeding against a Business Associate (in this case a management organization), stemming from a data breach, for $650,000.[7] That amount would pale, though, if a Covered client that generated millions of dollars in fees per year, were lost through such a breach.

Professional Liability

Two recent claims highlight the exposure to law firms from outdated or lax information security protections. In *Millard v. Doran*, filed in Supreme Court, New York County, a "spoofing attack" led to the plaintiffs' wiring $1.938 million to hackers, instead of their counsel. They alleged that the attorney's maintenance of her law firm email account on America Online ("AOL"), given that AOL was "notoriously vulnerable to 'hacking' by cybercriminals," and the failure to "install basic cybersecurity protection" on the subject computer was professional negligence and a breach of her fiduciary duties to her clients (*Robert Millard and Bethany Millard v. Patricia L. Doran*, Supreme Court of the State of New York, County of New York, Index No.: 153262/2016, filed April 18, 2016).

Yet, an actual breach may not be required for a claim against a law firm. A class action was brought against Chicago law firm Johnson & Bell, alleging that the firm's billing and other information systems contained such severe weaknesses client were damaged because a breach of their information "is inevitable" (*Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd.*, Docket No.: 1:16-cv-or04363 MIS/SES , N.D. Il., filed April 15, 2016). There was no actual breach and the firm brought a motion to dismiss for, among other things, lack of a concrete injury. The case is currently in arbitration but the firm has sustained significant reputational damage and it is unclear how much money it spent in legal fees out of pocket. Appearances, in cybersecurity, matter greatly and can result in significant costs.

Moving Forward

The operable metric for cybersecurity is reasonable steps, not perfection. "Reasonable steps" requires documentation of security practices, and controls to instill a culture of security. I 2017, security is everyone's job. Suggestions include:

- Learn the federal and state cybersecurity requirements that apply to your practice and your clients' counsel guidelines on security.
- Prepare documented information security policies and procedures that meet those standards and prepare and conduct training (including reminder training) on those

[6] 45 C.F.R. Secs. 160.103, 160.105, 160.310, 164.302, 164.306, 164.308, 164.312, 164.314

[7] OCR Resolution Agreement July 1, 2016, available at https://www.hhs.gov/sites/default/files/chcs-racap-final.pd (last visited January 6, 2017).

standards. Get experienced counsel or consultants if your firm does not have in-house expertise.

- Regularly assess security protocols and remain current on malware mitigation techniques and security patches.
- Protect client and sensitive firm information in transit and in storage through encryption and Virtual Private Networks ("VPNs").
- Inventory mobile devices used for firm business (smartphones, tablets, laptops, USB "thumb" drives) and prepare a mobile device management protocol.
- Review your firm's insurance policies to ascertain whether they cover cyber risk. Most malpractice and general liability policies exclude cyber events. Clients may require that the firm carry cyber insurance naming the client as an additional insured. Cyber policies vary widely and contain many exclusions, so have counsel at the firm or outside review it carefully.

Clients will drive law firms to cybersecurity, but the regulators are right behind them. Firms should take advantage of the defenses good cyber practices can provide.