Increasing Cybersecurity Requirements for Lawyers

Stephen Treglia, New York Law Journal

May 30, 2017

Say the words "data breach," and a legal practice might not be the first enterprise that comes to mind when imagining the likely victim. A health care provider, a financial institution, an educational facility, a government agency, perhaps, but not a law firm.

Major Law Firm Data Breaches

Not if you listened to former U.S. Attorney for the Southern District of New York, Preet Bharara, whose office, prior to his dismissal, indicted three Chinese nationals this past December for hacking into the servers of two separate law firms to secure confidential information regarding merger and acquisitions deals. According to one report, the hackers secured confidential information between April 2014 until the end of 2015, regarding 13 individual deals, thereby providing insider information resulting in trading losses in excess of $4 million.

At the press conference announcing the indictment, Bharara put law firms on notice of their immense cyber vulnerability. He said that the incident "should serve as a wakeup call for law firms around the world … . [Y]ou are and will be targets of cyberhacking because you have information that would be valuable to would-be criminals." In other words, to paraphrase the infamous bank thief Willie Sutton and upgrade his oft-quoted saying to 21st Century reality, cyber criminals are targeting law firms because that's where the greatest digital gold is located.

It also should not be overlooked that prior to the indictment, two major law firms announced their respective networks had been breached, leading to speculation that these events are all connected. Regardless, the increased cybercrime activity perpetrated worldwide upon all kinds of businesses and government agencies, including the current ongoing ransomware attack that began on May 12, 2017, known by the name WannaCry and described as the greatest cyberattack ever, dictates law firms should immediately reassess the potential exposure of their critical data.

Expanding Requirements

More importantly, practicing good cyber-hygiene is becoming less and less a voluntary activity to be undertaken by law firms. For a variety of reasons, it is becoming legally and otherwise mandated. The severity of these requirements is gradually approaching even standards of legal ethics.
In 2012, the American Bar Association's Commission on Ethics 20/20 amended footnote [6] to Rule 1.1 of the Model Rules of Professional Responsibility regarding an attorney's level of competence to represent clients. The amendment, shown here in italics, specifically instructs:

[6] 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

While New York has yet to adopt the Model Rules, they are increasingly becoming the standard in other states, making it almost certainly a harbinger of guidelines to be required nationwide in the near future. Even if not formally codified in New York at this time, still the basic ethical precepts of maintaining the confidentiality of sensitive client information require lawyers in this state to prevent ethics violations caused by the unauthorized access to privileged client information such as intellectual property, pending commercial transactions, attorney-client communications, etc., even when such information is transmitted via email.

Beyond an attorney's ethical requirements, certain statutes or regulations may impose additional cybersecurity obligations upon a lawyer based upon the kind of business conducted by the client.

**Covered Entities and Downstream**

For example, in the health care environment, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) extended the applicability of the Health Insurance Portability and Accountability Act (HIPAA) to "Business Associates" of "Covered Entities." (A "Covered Entity" is defined as: "a health plan, a health care clearing house, or a health care provider who transmits any health information in electronic form in connection with" a HIPAA-HITECH-covered transaction, 45 CFR §160.103.) A Business Associate is defined, in part, by the kind of services performed on the behalf of a Covered Entity, and specifically includes legal assistance. 45 CFR §160.103(1). Moreover, the information security and privacy rules applicable to Covered Entities under HIPAA-HITECH are equally applicable to all Business Associates (45 CFR §164.302) as well as all subcontractors of Business Associates (45 CFR §160.103(3)(ii)). Hence, a lawyer or firm who represents a health care Covered Entity and possesses, in any way, what is called "Protected Health Information" (PHI) is just as subject to HIPAA-HITECH compliance as the Covered Entity it represents.

It appears that New York recently further expanded the categories of clients for whom a lawyer must impose its own internal cybersecurity requirements. On March 1st, 2017, the Department of Financial Services (DFS) enacted new regulations applicable to a wide range of financial institutions which become enforceable on August 28th. These regulations have been described as among the harshest cybersecurity requirements yet to be required anywhere in the United States.

Here, the term "Covered Entity" is similarly used to identify the primary organizations responsible for compliance, but is defined as

any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

23 NYC §500.01(c).

In place of the term "Business Associate" in the HIPAA-HITECH realm, the new DFS regulations employ the term "Third-Party Provider," which applies to any person providing services to the Covered Entity and possessing certain forms of non-public personal information. 23 NYC §500.01(n). There
seems to be little doubt this would also apply to law firms providing legal services to covered financial institutions.

The DFS regulations mandate certain cybersecurity activities be performed by every Third-Party Provider regarding the critical digital information it possesses, such as: the implementation of written policies and procedures, the use of in-transit and at-rest encryption, notification of any cybersecurity events to the Covered Entity, and the Third Party's making of warranties and assurances to its Covered Entity of its cybersecurity practices. 23 NYC §500.11(b). It is also required that the Covered Entity adopt written policies and procedures ensuring that the Third-Party comply with the latter's duties. 23 NYC §500.11(a).

**Accretive Health Story**

There already exists a devastating case study regarding the consequences for mishandling critical personal data in this Covered Entity-downstream relationship. In July 2011, Accretive Health, a Chicago-based hospital revenue-cycle management company (hence, a Business Associate) suffered a data-breach when an unencrypted laptop containing PHI of as many as 23,500 patients of two Minnesota hospitals (its Covered Entities) was stolen from the trunk of an Accretive employee's rental car parked in an airport lot.

The HITECH Act expanded the jurisdiction of enforcement agencies empowered to institute HIPAA actions to state attorneys general, and one was instituted in the Accretive case by the Minnesota AG, Lori Swanson. In July 2012, Accretive reached a settlement with the AG, agreeing to a $2.5 million penalty. More devastating was the requirement that Accretive not do business in Minnesota from between two to six years, solely at the discretion of the AG.

In its first public filing following the AG settlement, Accretive acknowledge that the loss of its Minnesota clients would cost it between $23 and 25 million per year in revenue. Add on a subsequent $14 million settlement with Accretive's shareholders over its involvement in the HIPAA proceeding and a 20-year settlement with the Federal Trade Commission to follow industry-recognized cybersecurity practices in the future, to be verified by an independent auditor at Accretive's expense, and the total cost to the company for the loss of a single unencrypted laptop has been in excess of $100 million.

And that is not the end of the story. In March, 2016, one of Accretive's Covered Entities in this incident, North American Health Care of Minnesota, suffered a $1.55 million HIPAA penalty at the hands of the Office for Civil Rights of the U.S. Department of Health and Human Services for its acts of omission regarding Accretive. The health care provider failed to secure a written agreement with Accretive governing its use of the Entity's data and also failed to oversee Accretive's use of its data.

**Conclusion**

Granted, the future regarding how these various cybersecurity laws and regulations will be enforced against lawyers and law firms is not yet completely certain. But if this early history is any indication, the legal profession must awaken and start taking notice and action before it becomes too late. No lawyer or law firm can become cybersecure at the mere snap of the fingers. Careful thought, written policies and procedures, encryption deployment, risk assessment and regular review, staff training, and numerous other steps must be taken in advance to satisfy regulators when they come knocking at the door.

And this article has not even touched on the issues of how the practice of law can come within the demands of state breach notification laws or the impending European Union's General Data Protection Regulation, which becomes effective May 25, 2018. Topics to be covered in future articles.
Stephen Treglia is the former head of the cyber crime unit at the Nassau County district attorney’s office and currently consults with data protection companies and law firms.