Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Notes From A Law Firm Chief Privacy Officer: New Demands

By **Phyllis Sumner**

Law360, New York (August 14, 2017, 1:13 PM EDT) -- As more law firms become the targets of major cyberattacks, more firms may consider appointing a chief privacy officer. In this Expert Analysis series, CPOs at four firms discuss various aspects of this new role.

Privacy and cybersecurity are increasingly on the minds of law firm management and are impacting how law firms manage data. While distinct concepts, they intersect as lawyers balance professional obligations and increasing client expectations to maintain and protect sensitive and confidential information with the demands of a very competitive legal services industry.


Phyllis Sumner

On the privacy front, firms are faced with considering the privacy interests of their clients' customers and employees, in addition to the privacy interests of their own lawyers and staff. And although privacy and confidentiality concerns go beyond cybersecurity, the appropriate protection of computer systems and the data contained on those systems has become a significant concern for law firms and their clients. At the same time, outside counsel are expected to quickly and readily analyze information and provide advice to their clients at any time and from any place. Oftentimes, efficiency and responsiveness collide with security measures as clients are increasingly requiring their outside law firms to comply with third-party risk management programs. As clients become more sophisticated about data privacy and security, the challenges of balancing these interests with effectively and efficiently delivering legal services will continue to grow. To meet those challenges, law firms are focusing more on the need for and the roles of chief privacy officers and chief information security officers.

Increasing Cybersecurity Risks

Many commentators view cybersecurity, or cyberrisk, to be one of the biggest risks that law firms face today. Cybercriminals have targeted law firms because of the large quantities of client information available to law firms. Many top cyber incident headlines during 2016 involved the legal industry. For

example, in March 2016, the FBI notified the legal industry of a criminal actor seeking hackers to assist in obtaining insider information, including merger and share purchase agreements, and reportedly targeted nearly 50 elite law firms.[1] Media coverage in March 2016 revealed that several top firms representing Wall Street banks and Fortune 500 companies experienced breaches.[2] In April 2016, an anonymous source leaked the infamous "Panama Papers," 11.5 million files, including confidential client information obtained from Mossack Fonseca, a Panamanian-based law firm specializing in incorporating companies offshore.[3] 2016 also brought the first class action to publicly name a law firm for failing to protect client information when a federal judge unsealed a case in the Northern District of Illinois brought by former clients of Johnson & Bell.[4] The trend continued in 2017. Most recently, the law firm DLA Piper was hit by a ransomware attack that took down phones and computers in offices across the world.[5]

Given these mounting risks, law firms must focus on data privacy and security and follow their own advice to their clients to be vigilant in these areas. This requires firm management to be willing to invest the resources (costs that cannot be passed onto clients) to develop and maintain privacy and cybersecurity programs that meet the needs of their clients. For many firms, this means including chief privacy officers and chief information security officers on their firm management teams. Both roles focus on protecting information from unauthorized access, but the CPO also must focus on legal compliance with privacy laws, often across multiple jurisdictions, including whether information is being collected, transferred and maintained in an appropriate and legally compliant manner.

While law firms work to enhance privacy and security programs, they face the very real challenge of changing the work habits of lawyers who must meet high client service demands. Ensuring lawyers are focused on the security of emails, texts, laptops, tablets and wireless environments, particularly when traveling, can be difficult. An emphasis in recent years on efficiency and convenience for lawyers to work remotely whenever and wherever needed, creates a tension with the demands to maintain appropriate security measures. These risks no longer should be relegated to the information technology department, but need to be addressed through global privacy and security policies and procedures and training and awareness programs.

Evolving Professional Obligations

Lawyers understand and appreciate their obligations to maintain the confidentiality of client information. How to meet those obligations in an ever changing cyberrisk landscape, however, is a much more difficult question. Just as data breach laws have developed slower than cybersecurity risks, so has guidance for law firms concerning data privacy and security. Recent guidance has helped crystallize the responsibility of lawyers.

The American Bar Association Model Rules of Professional Conduct outline the basic obligations of an attorney to protect confidential client information, including staying up to date on relevant technology. Rule 1.1 requires that an attorney provide "competent representation" to a client, which includes "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Model Rule 1.6 states that an attorney is required "not to reveal information relating to the representation of the client" outside of exigent circumstances, and also to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, [client] information." The comments to Model Rule 1.6 discuss in detail precautions attorneys should take in storing and transmitting client information, while making clear that an attorney who takes "reasonable efforts to prevent access or disclosure" will not be found in violation of the Rule. Factors that are considered in determining the reasonableness of the lawyer's efforts include, but are not

limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

In May 2017, the ABA issued Formal Opinion 477, a new ethics opinion stating that under the professional rules of conduct, attorneys have a confidentiality obligation to take reasonable measures to ensure that unencrypted emails containing client information are safe from cyberthreats. The opinion noted the explosion in attorneys' use of tablets, smartphones, and other devices, as well as the adoption of email to relay sensitive information, were driving factors in the issuance of this new guidance. The opinion states that routine communications may still be conducted via unencrypted email, but attorneys must have implemented reasonable electronic security measures, and urges lawyers to develop a process to address cybersecurity needs on a case-by-case basis that may require encryption depending on the sensitivity of the client emails or files.

Additionally, many states have released formal ethics opinions addressing specific issues relating to the interplay between technology and the practice of law. See, e.g., Cal. Ethics Op. 2012-184 (2012) (discussing ethical obligations of attorney practicing law via "virtual office"); Conn. Ethics Op. 2013-07 (2013) (addressing cloud computing in practice of law).

Indeed, recognizing this increasing risk, the ABA in February 2017 added cybersecurity to its list of insurance offerings for attorneys and law firms, providing coverage for data incidents and breaches and possible network threats. The offering includes coverage for expenses, income loss, forensics, and third-party claims and losses. Citing the 2016 threats of insider trading schemes targeted at law firms, ABA President Linda A. Klein stated that "as the number of cyber breaches increases everywhere and throughout all industries, it is critical that lawyers and law firms that rely on vast amounts of electronic data are protected."[6]

Meeting Increasing Client Expectations

Aside from applicable professional rules, a law firm's practices related to privacy and cybersecurity may be implicated by an engagement letter or outside counsel guidelines, thereby potentially creating a contractual duty to the client regarding the handling, storage, and protection of electronic data. Indeed, clients are demanding more of law firms with regard to protecting the confidentiality of their information, some going so far as to include certifications and indemnity clauses in their engagement letters. According to a 2016 ABA Legal Technology Survey Report, 30.7 percent of all law firms and 62.8 percent of firms of 500 lawyers or more reported that current or potential clients provided them with security requirements.

It is becoming more commonplace for clients across many industries to require various levels of due diligence, including exhaustive written data security and privacy questionnaires, review of privacy and security policies, site visits by due diligence teams to inspect technology and physical security, and requests for backup evidence and attestations. Clients also are more frequently seeking certifications and requirements from vendors, which law firms engage to assist with client data, including the routine use of electronically stored information vendors during litigation. As a result, firms are faced with developing and implementing processes involving appropriate law firm stakeholders to respond to these client demands in an appropriate and consistent way. This is particularly challenging when a law firm has multiple offices across the globe, and faces varying levels of client requests to handle data in a constantly changing landscape of data protection and privacy laws across many different jurisdictions

and regulated by a variety of governing bodies and regulatory agencies. As law firms face these challenges more frequently, the roles of CPO and CISO become more integral to managing those issues.

Looking Forward

While the guidance and specific steps law firms should take to protect data will continue to evolve, it is clear that, regardless of size or geographic reach, law firms must take affirmative steps to address privacy and data security risks, including regularly reviewing and updating policies and procedures to protect the confidentiality of client information.

According to an ABA study in 2016, only 17.1 percent of all law firms had an incident response plan in place to address a security breach, and only 50 percent of firms of 500 lawyers or more had such a plan in place. The ABA further found that only 56 percent of firms reported having document records management and retention policies, 49 percent reported having email use policies, 41 percent reported having internet use or computer use policies, and 34 percent reported having social media policies in place.

Privacy and security risks are on the rise and law firms should address these issues with the same level of sophistication as the practice of law. Fortunately, resources available to law firms in this space are growing. The ABA is set to publish its second edition of "ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals" this year, which will include a particular focus on resources available for small firms, as well as the legal and ethical obligations and cultural challenges faced by firms. Law firms also can look to industry standards for cybersecurity benchmarks, including ISO data security certifications and guidance from the National Institute of Standards and Technology. In addition, consulting firms and other major players in this space are developing programs and services for law firms to manage cyberrisk. The Association of Corporate Counsel recently issued guidelines titled “Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information” in March of this year to serve as a benchmark for law firm cybersecurity practices.

Given the increasing risks, client demands, and developing laws and guidance, law firm management, including the general counsel, chief information officer, CPO and CISO, should band together to actively analyze and affirmatively address privacy and cybersecurity issues, taking into consideration risk management and insurance implications. Such team efforts across the firm are critical in developing a culture in which lawyers and law firm staff protect the confidentiality of client and employee information, while still meeting client demands for effective and efficient legal services.

Phyllis Sumner is a partner in the Atlanta office of King & Spalding LLP and the firm’s chief privacy officer. She leads the firm's data, privacy and security practice and is a former assistant U.S. attorney for the Northern District of Illinois and the Northern District of Georga.

[1] “Criminal-Seeking-Hacker” Requests Network Breach for Insider Trading Operation, Federal Bureau of Investigation, Cyber Division, Alert No. 160304-001 (March 4, 2016).

[2] Claire Bushey, Russian cyber criminal targets Elite Chicago law firms, Crain's Chicago Business (March 29, 2016), http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms; see also Nicole Hong & Robin Sidel, Hackers Breach Law Firms, Including Cravath and Weil Gotshal, Wall Street Journal (Mar. 29, 2016), http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[3] Luke Harding, What are the Panama Papers? A guide to history's biggest data leak, The Guardian (Apr. 5, 2016), https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers; see also Mossack Fonseca, Mossack Fonseca's response to the Panama Papers, The Guardian (Apr. 3, 2016), https://www.theguardian.com/news/2016/apr/03/mossack-fonsecas-response-to-the-panama-papers.

[4] Roy Strom, Chicago's Johnson & Bell First US Firm Publicly Named in Data Security Class Action, The American Lawyer (Dec. 9, 2016), http://www.americanlawyer.com/id=1202774361560/Chicagos-Johnson--Bell-First-US-Firm-Publicly-Named-in-Data-Security-Class-Action?slreturn=20170011171830.

[5] Debra Cassens Weiss, DLA Piper hit by 'major cyber attack' amid larger hack spreading to US, The ABA Journal (June 27, 2017), http://www.abajournal.com/news/article/dla_piper_is_hit_by_major_cyber_attack_amid_larger_hack_spreading_to_us

[6] https://www.americanbar.org/news/abanews/aba-news-archives/2017/02/aba_begins_offering.html

---