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: Balancing Act

By **Kristin Jones**

Law360, New York (August 10, 2017, 10:52 AM 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.


Kristin Jones

As the role of law firm chief privacy officer becomes more prevalent and expansive, many CPOs are finding themselves in the midst of a delicate balancing act, weighing compliance with government regulations and client requirements on one side with the needs of firm business on the other.

Full-service law firms are subject to multiple regulatory schemes by virtue of their multidisciplinary practices. Simultaneously, clients are increasingly demanding more comprehensive privacy programs. These obstacles leave a CPO with little opportunity to tailor a privacy program to the needs of the organization. The result can be a program that is largely reactive to client and government requirements, instead of the proactive approach that law firms themselves typically recommend to clients. In order to get a sense for how to resolve this balancing act, it helps to take a closer look at the issues and when they arise.

Maintaining Compliance With Industry-Specific Government Regulations

Law firms started appointing CPOs around 2013 after new regulations extended the Health Insurance Portability and Accountability Act of 1996 to business associates, including law firms. As other industries developed comparable regulatory schemes, the role of the CPO has expanded far beyond HIPAA. Consequently, CPOs — who may have been appointed due to their familiarity with health privacy regulations — have been left to educate themselves on other industry-specific regulations, such as the Gramm-Leach-Bliley Act (GLBA), the Federal Trade Commission Act and more.

Vendors, including law firms, are often subject to the same legally imposed compliance obligations as their clients. These industry-specific regulations often direct clients to contractually require their vendors to maintain the same strict privacy and security standards as the regulated entities and monitor their vendors' compliance with contracted terms. These regulations, including both HIPAA and the GLBA, direct covered organizations to implement "appropriate" administrative, technical and physical safeguards. As a result, implementing standards required for compliance with these regulations — such

as password requirements, encryption, and information backup and disposal criteria — will vary depending on certain characteristics of the client, such as its size and resources, its capabilities to implement safeguards and its access to nonpublic information. The law firm is then left to manage multiple security standards or protect information in accordance with their strictest client's requirements, regardless of the firm's own resources.

Responding to Client Requirements

Applicable government regulations are not the only reason clients expect outside counsel to have robust information security programs. Just like their clients, firms may face financial and reputational damage if private information is compromised. As the legal market becomes more competitive, clients have become more savvy consumers and are now using privacy and security programs as one way to whittle down the options. Clients regularly send law firms comprehensive questionnaires asking hundreds of questions about the firm's privacy and security practices, procedures and standards. No two questionnaires are the same; queries about similar content are typically asked in different ways. "Has your law firm suffered a data loss or security breach?" may be replaced with "Has anyone alleged that their personal information was compromised or have you notified any third parties that nonpublic personal information was compromised?" Each question requires a unique and carefully prepared response or the client may seek new outside counsel.

CPOs are faced not only with complex questionnaires, but also with client demands in other forms: outside counsel guidelines, requests for a proposal or other project bids or even informal email inquiries. These alternate means have the same potentially significant implications; the wrong response could cost the law firm a new engagement or existing client. Further, when new privacy or security concerns hit the headlines, a spurt of new client demands hit the CPO's inbox just as rapidly. Recently, news relating to ransomware and press releases on the use of Transport Layer Security sparked a slew of questions and requirements from clients inquiring about those issues.

With tight deadlines and important clients to please, law firms generally prioritize privacy and security initiatives in response to client demands. Even still, certain areas may be difficult for firm compliance. For example, information classification policies, which limit access to existing work product to those lawyers and staff members with a "need to access" the information, can impede the firm's ability to share information internally. Large law firms rely on institutional knowledge — templates and other forms of prior work — to efficiently develop new work products. These policies may receive institutional resistance. The CPO is then forced to evaluate whether the law firm should sacrifice traditional efficiencies, like templates, in order to add another layer of privacy protection.

Incorporating the Firm's Needs Into the Privacy Program

Privacy programs in a law firm setting may be primarily reactive — that is, built in response to requirements imposed by clients and regulators. New policies or safeguards may be rapidly implemented in order to check the box indicating that "Yes, the law firm does comply with this standard." However, in addition to satisfying clients by meeting their demands — essentially a requirement in the competitive legal market — a CPO is proactively building a privacy program that will reduce the firm's risk of a breach. These measures include revising and preparing policies and procedures, working with the chief information security officer to ensure that technical measures meet regulatory guidelines, monitoring the workforce's compliance with existing guidance, and incorporating privacy terms into contractual relationships.

Engaging the workforce in complying with the firm's privacy program can be particularly challenging. Security awareness training — whether in the form of a formal program or an informal question — is critical to ensuring that the firm's workforce has a clear understanding of their role in protecting the organization from privacy and security risks. The support of firm management can grease the wheels with reluctant attorneys and staff. Still, the CPO should remain cognizant of these issues when developing policies and procedures. Attorneys are trained to find gaps in guidance, and the firm's privacy and security policies are no exception. Further, if the CPO takes a position that is too burdensome on attorneys and staff, then they are less likely to follow the CPO's guidance.

Balancing Government and Client-Imposed Compliance Obligations and the Firm's Needs

The issues described above illustrate the ultimate challenge of a law firm CPO: balancing compliance with government regulations and client requirements against the business needs of the law firm. Clients — particularly those in the health care or financial services market — will not tolerate a material breach. A competitive legal market requires law firms to dedicate resources to satisfying existing clients and building a new client base. However, the CPO cannot ignore the firm's own business needs in order to meet the needs of its clients. Some privacy and security safeguards can be overly burdensome in an environment where law firms are pressured to reduce costs and increase quality.

The CPO should consider whether the privacy program is appropriate for the firm, evaluating whether the program ensures the firm's compliance with government regulation, satisfies the firm's clients and reduces the firm's risk of a breach. This analysis influences a CPO's strategy in completing daily tasks, like responding to client questionnaires and preparing new policies. Ultimately, a law firm CPO must incorporate appropriate protections and processes to shield sensitive data from unnecessary risk without unreasonably sacrificing firm resources and profitability in order to have a successful privacy program.

Kristin J. Jones is an associate in the Malvern, Pennsylvania, office of Stradley Ronon Stevens & Young LLP. She serves as chief privacy officer for the firm.