Counsel To Counsel: A Law Firm GC's Data Protection Duties

Law360, New York (April 19, 2017, 12:09 PM EDT) –

Many law firms now have a designated general counsel, or a group of counsel, tasked with managing myriad legal matters for the firm. What are some top-of-mind priorities for these GCs today as they strive to keep their firms out of legal trouble?

Thomas White

For most companies and their lawyers, information security—and the consequences of data breaches—represents one of the biggest risks they face today. It's no different for law firms. Indeed, for a number of reasons law firms may face even greater risks. Clients entrust us with some of their most sensitive personal, legal or commercial information. We are bound by rules of professional conduct to maintain the confidentiality of client information, and the most recent revisions to the ABA model rules establish a specific duty to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. We risk reputational damage and potential professional liability exposure in the event client information is disclosed.

The threats are real. Last year, the FBI warned that law firms were the targets of hackers who sought to gain information as part of insider trading schemes. Subsequently, the government charged individuals with insider trading based on information obtained through penetration of the computer networks of two major international law firms. Other threats affecting law firms include email phishing attacks, social engineering by impersonation of key executives, and potential data loss and extortion from ransomware. These attacks can number in the millions — a day. WilmerHale's experience confirms the magnitude of the threats. Like other large businesses, we are subject to cyberattacks, including constant scans for vulnerabilities against our firewalls, infected email attachments, and web browser threats.

Clients are understandably focused on law firm compliance. Financial institution clients maintain particularly rigorous oversight of law firm data security practices, given the data protection regulations to which they themselves are subject. Increasingly, we see companies in all industries seeking to perform various levels of due diligence on our information security defenses. Client diligence can include written questionnaires, site visits, and other requests for backup evidence and attestations. Some clients even conduct their own penetration tests of our defenses. We received three times as many diligence requests from clients and prospective clients in 2016 as we did in 2015. Many clients ask the firm to adopt specific information security controls, including segregation of access to their information, encryption of data at rest and in transit, and continual review of contractor/outsourcing security measures.

In light of these developments, a law firm should proactively identify cybersecurity risks and implement strong defenses to data attacks and breaches. Many large law firms now participate in a legal information sharing and analysis coalition affiliated with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and incorporate multiple sources of cyber intelligence in daily operations.

Although data protection is sometimes thought of primarily as an "IT" matter, in light of the risk management implications, a firm's general counsel should be an active participant in the firm's data protection efforts. To use our firm as an example, our office of the general counsel (which consists of three partners, a deputy general counsel and a special counsel):

- In conjunction with the firm's cybersecurity and data privacy lawyers, advises management about applicable law and professional responsibility rules relevant to cybersecurity, including providing legal guidance with respect to matters such as appropriate security incident response procedures;

- Actively participates in the firm's Information Security Working Group, a group composed of members from the firm's information services, human resources, internal audit and general counsel functions, as well as the firm's cybersecurity and privacy lawyers, which reviews and recommends firm information risk initiatives, prioritizes resources to address those initiatives, and creates and recommends firm security policies to firm management;

- Assists in the development of technology- and information-related firm policies;

- Reviews terms of outside counsel guidelines and requests for proposal (RFPs) that address data security requirements;

- Assists management in developing the firm's crisis management strategy for responding to security incidents;

- Advises management about cybersecurity insurance.

While design and implementation of the data protection program may be others' responsibilities, the general counsel should understand the basic parameters of an effective program. Things that a law firm general counsel may wish to consider as part of his or her firm's data protection security program include:

Compliance with International Security Standards — Obtaining and maintaining appropriate certifications, such as ISO 27001:2013.

Privacy and Security Awareness — Providing security awareness training, including regular email phishing exercises against internal users and quizzes on training materials.

Policy and Procedures — Establishing policies governing matters such as uses of firm technology resources, use of social media, and protection of sensitive personal information.

Business Continuity — Maintaining a business continuity and disaster recovery program that includes governance, testing procedures, and system documentation to prepare for unforeseen events.

Cyber Defenses — Maintaining robust protections against cyber intrusions, such as through a defense-in-depth approach, which incorporates cyber intelligence feeds from multiple sources operating in conjunction with endpoint security agents, firewalls and internal intrusion detection sensors

Mobile Device Management — For mobile devices, implementing policies on encryption, password complexity, phone tracking, data loss prevention, and mobile lock and wipe.

Encryption — Requiring appropriate encryption of mobile data storage and processing devices such as laptops, mobile devices and removable storage media.

Vulnerability Management — Performing periodic vulnerability scans to detect new vulnerabilities with formal procedures to respond to immediate threats.

Physical Security — Maintaining physical security controls, including keycard access, security cameras and visitor ID requirements, to prevent unauthorized physical access to firm facilities or technology assets.

Access Management — Employing permissions management to ensure that every person in the firm maintains a level of system access that is appropriate for their work, enforcing strict password requirements that include industry best practices, and mandating settings for user account inactivity, session lockouts and account disabling

In sum, for GCs, data protection ranks right up there in the category of "What keeps you up at night?" Mitigating information security risks is a major risk management function for the firm, and involves ongoing attention and the investment of substantial resources. Given the ever-evolving nature of cybersecurity threats, and the stakes involved, these issues are unlikely to abate for a long time, if ever.

Thomas W. White is the general counsel of WilmerHale. He works out of the firm's Washington, D.C., office.