Client Data Security Obligations Begin With the Law Firm

No matter whether firms keep data in-house or work with third parties, certain cybersecurity controls should be in place.

Timothy Opsitnick, TCDI, Legaltech News

November 9, 2016 | 0 Comments

As if a lawyer's job were not tough enough, we now need to understand technology in addition to the law. ABA Model Rules of Professional Conduct 1.6 outlines a lawyer's obligation in securing client data: "(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Moreover, the lawyer's duty of competence starts with legal knowledge, skill, thoroughness and preparation, but as outlined in Comment 8, Model Rule 1.1, amended in 2012, extends to "the benefits and risks associated with relevant technology." Finally, in accordance with Model Rules 5.2 and 5.3, the lawyer supervising a matter must ensure that subordinate lawyers and nonlawyers associated with the matter, including consultants and vendors, act with technical competence.

Therefore, data breaches have ethical implications as well as the risk of loss to the client and damage to the firm's reputation. Cybersecurity begins with a top-down strategy, but the culture of security must include each and every person in the firm and its consultants and vendors. Indeed, the need for firmwide cultural alignment around data security is no different from the climate within the corporate clients that we represent. Lawyers must be

cybersecurity leaders if we are to change the evolving dynamic of the ever-increasing number and scale of incidents.

Lawyers are not immune, and law firms are in fact being increasingly targeted. Corporations deploy layers of defense against cyber incidents, but law firms are just now catching up not only with their own internal data, but also their clients' data. Law firms may be targeted for confidential data but also out of motivations ranging from business disruption, money, political sabotage or sheer sport.

A law firm has two options when controlling client data: maintain the data in-house or through a third-party provider. Often, a third-party provider in the business to provide access to and secure data can do so more effectively. Each option demands the supervising attorney provides diligence in oversight to ensure data is secure. The following basic cybersecurity controls should be in place:

Physical: Ensure that the data center has restricted access controls. The hardware that is storing the data should only be accessible to authorized personnel and constantly monitored.

Technical: Client data and hardware should be hard partitioned from any other network used to run the organization as a starting point, but all other processes should ensure that the data being accessed has layered security inclusive of defense in depth, outward- and inward-facing firewalls, data loss prevention technology, anomaly detection and encryption, among other elements, to ensure incoming traffic is restricted to those specifically given access.

Application: Software applications that touch the data should be regularly tested for vulnerabilities and following changes to applications. When vulnerabilities are discovered, they should be remediated in a reasonable amount of time. Supervising attorneys should work with the teams deploying the software to have confidence in the development, testing and deployment of the platforms. Though most platforms used today are subject to their own scrutiny before deployment, it is still advised to have the CISO or IT director sign off on their use.

Administrative: This is where firms are most vulnerable and the culture of security needs to be properly defined. Cybersecurity policies throughout the entire firm and at any third-party provider need to be rolled out and adhered to strictly.

A law firm must understand its own internal data and its clients. Cybersecurity controls demand that a firm knows the type of data it collects and where that data resides. Where does your organization stand today?

Ensuring cybersecurity is an iterative process that requires vigilance each and every day, not just in a snapshot of time. A firm should determine the stage of its cybersecurity controls as well as what it should aspire to achieve. The following stages of cybersecurity maturity help define where you are and where to focus next:

1. Ad Hoc: Lacking a formal process leads to continual reactivity to hard and soft breaches and will give inconsistent performance.

2. Developing: Initial repeatable processes on proactive and reactive situations will give some consistency, but need continual process discipline.

3. Practicing: Controls are defined with documented and enforceable standards among employees. This will create consistency throughout organizational performance.

4. Optimizing: Controls are effective and the culture accepts individual care and responsibility. Adding process metrics will allow for targeted improvement.

5. Leading: Fully integrated strategies will allow for innovative changes and seamless controls that will impact the firm's overall security, but also will have an influence on clients.

The ABA Rules of Professional Conduct are clear in stating that lawyers have an ethical obligation to keep client data confidential. Ramping up cybersecurity and then keeping it up to date needs to be a priority for firms. In fact, effective cybersecurity should be viewed as a key differentiator in the marketplace.

Timothy M. Opsitnick is the executive vice president and general counsel of TCDI.