CHICAGO LAWYER

An ounce of prevention: Attorneys need to be on guard in new cyber world

September 01, 2015

By Nicholas A. Gowen
Nicholas A. Gowen is a partner at Honigman Miller Schwartz and Cohn, where he has broad national practice representing businesses and individuals in a range of disputes.

Imagine the following scenario:

Your law firm's managing partner told you that the firm recently hired a consultant to conduct a test to determine the effectiveness of the firm's network security.

The consultant simulated a data breach resulting in a virus infiltrating the firm's document database.

The consultant determined that the firm's network security was inadequate and needed to be upgraded.

The firm is now refocusing its efforts to secure its network, enhance its internal policies and determine its ethical obligations to secure client data from cyber breaches.

You have been tasked with determining the firm's ethical obligations to secure client data stored on the firm's network.

Although data breaches affecting large businesses seem to be in the news all of the time, you have not previously considered how such an event implicates a law firm's ethical responsibilities to its clients.

This scenario is becoming more common as law firms have become targets of hackers seeking valuable electronic data. Although a law firm's network may not store the same type of information as those of financial institutions or retailers, law firms have access to valuable, sensitive client information that is a treasure to hackers, including:

- clients' strategic business and financial information,
- clients' trade secrets,
- litigation-specific confidential client documents,
- attorney-client privileged communications and work product, and
- personally identifiable information for clients and third parties, such as Social Security numbers, personal health information and financial data.

Unlike other industries and professions, lawyers are bound by the rules of professional conduct to protect client confidential information in addition to the myriad statutory, regulatory and contractual obligations that also exist. In particular, the Illinois Rules of Professional Conduct of 2010 require lawyers to keep clients abreast of any developments in their case and to keep client information confidential. Both rules are implicated if a data breach involves client information.

Rule 1.4 requires lawyers to keep clients "reasonably informed" about any material developments in their case, an obligation that arguably applies to the unauthorized disclosure of a client's data.

If a client's private confidential information has been improperly compromised that is certainly a material development in their representation.

Although not every loss of data may be considered significant, clients expect that their confidential information is being kept secure, so the firm should notify its affected clients of any security incident affecting their information.

Additionally, Rule 1.6 requires lawyers maintain confidentiality of all information relating to the representation of a client.

A lawyer "shall not reveal information relating to the representation of a client unless the client gives informed consent."

Comment 16 dictates that "a lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure."

Comment 17 further explains that when transmitting information relating to the representation of a client, "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

Lawyers must take "reasonable precautions" to protect the confidentiality of electronic data. The lawyer's duty, however, does not require that special security measures be implemented if the communication affords a reasonable expectation of privacy.

Although lawyers are not required to store and transmit all client data using heightened technology such as encryption, some situations may require that "reasonable precautions" include being more sensitive to where and how client data is accessed and transmitted.

Thus, lawyers should be aware to store, access and transmit certain confidential data in a manner that ensures heightened protection. For example, lawyers should not use public wireless networks to access certain types of highly confidential documents on the firm's network. Lawyers should also avoid storing confidential data on unencrypted portable USB drives.

Lawyers have ethical obligations to take reasonable measures to ensure that clients' confidential information is protected from cyber breaches and to disclose to clients in a reasonable time period in the event that a breach has occurred.

Some reasonable measures that lawyers can take to protect clients' data include the following steps:

- Ensure that the law firm maintains computer-use policies requiring employees to use and routinely update passwords for e-mail, document management systems, laptops and mobile devices.

- Require laptops and mobile devices be installed with full-disk encryption software.

- Require employees using personal devices to work outside of the office to install anti-virus protection.

- Encrypt content-based e-mail.

- Install laptop tracking technology.

- Limit the number of employees who may remotely access particular databases.